

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

Brussels, 21 September 2015 (OR. en)

12034/15

**LIMITE** 

**DATAPROTECT 141 JAI 660** MI 565 DIGIT 65 **DAPIX 151 FREMP 185 COMIX 408 CODEC 1191** 

#### **NOTE**

From:	Presidency	
To:	Delegations	
No. Cion doc.:	.: 5853/12	
Subject:	Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)	
	- Chapter IV, preparation for trilogue	

### Introduction

- At the Friends of Presidency DAPIX meeting of 15<sup>th</sup> September 2015 and at the JHA 1. Counsellors meeting of 18<sup>th</sup> September 2015, and with a view to the next trilogue, the Presidency invited delegations to discuss, on the basis of document 11784/15,
  - Chapter IV Controller and Processor
  - Relevant definitions in Article 4, in particular definitions (9) and (15)
  - Relevant recitals: 60, 60a, 60b, 60c, 61, 62, 63, 63a, 64, 65, 66, 66a, 67, 68, 68a, 69, 70, 70a, 71, 71a (EP), 71b (EP) 72, 73, 74, 74a (EP), 74a (Council), 74b, 75, 75a (EP), 76, 76a, 77

12034/15 VH/tt EN

DGD<sub>2</sub>C **LIMITE** 

- 2. Taking into account the General Approach reached on 15<sup>th</sup> June 2015 which constitutes the basis of the negotiation mandate for the Presidency, taking into account the discussions at the Friends of Presidency DAPIX meeting of 15<sup>th</sup> September 2015, as well as considering the European Parliament's position on Chapter IV, the Presidency has put together compromise suggestions in the 4<sup>th</sup> column of the document in annex with a view to the next trilogue. The Presidency invites delegations to share their views on these suggestions.
- 3. Delegations are reminded that the next trilogue will not address issues related to flexibility for the Member States' public sector which the Presidency proposes to discuss comprehensively when addressing Articles 1(2a), 2, 6(3) and 21.

The Presidency has also endeavoured to increase clarity and readability of the text in terms of structure and consistency, both as regards the alignment between recitals and articles, as well as articulation between different provisions.

4. In order to ensure an efficient discussion process, as well as to maximise its clarity, the Presidency chose to divide the different provisions into two categories.

The first category (points 5 and 6) relates either to provisions on which the co-legislators have a consensual view or to provisions where the Presidency intends to maintain the Council's General Approach. With regard to this category, the Presidency takes the view that no further discussion is needed. However, in case delegations wish to raise any crucial point or to provide further input relating to these articles, they may do so under point 8.

The second category (point 7) relates either to provisions where the Presidency suggests maintaining the Council's General Approach, while remaining flexible with regard to minor modifications suggested by the European Parliament or to provisions by the Parliament that differ from the provisions of the Council's General Approach.

For this last category, the Presidency invites delegations to give their views on the compromise suggestions made by the Presidency in the 4<sup>th</sup> column.

12034/15 VH/tt 2
DGD 2C **LIMITE EN** 

## Preparation for trilogue

- 5. Considering the position of the European Parliament and the Council's General Approach, delegations will note that there is a consensus on:
  - Article 22 (2) chapeau, (2(a)), (2(b)), (2(c)), (2(d)), (2(e)), (4)
  - Article 23 (3), (4)
  - Article 25 (2) chapeau, (2(c))
  - Article 26 (5)
  - Article 28 (5), (6)
  - Article 30 (4)
  - Article 31 (3) chapeau, (3(b)), (6)
  - Article 32 (6)
  - Article 33 (2(d)), (2(e)), (6), (7)
  - Article 34 (1), (5), (8), (9)
  - Article 35 (11)
  - Article 36 (1)
  - Article 37 (2)
  - Article 38 (1a(a)), (1a(b)), (1a(c))
  - Article 39 (3)

The Presidency takes the view that no additional discussion is necessary on these provisions. However, in case delegations wish to raise any crucial point or to provide further input relating to these articles, they may do so under point 8.

- 6. The Presidency suggests to maintain the Council's General Approach as regards:
  - Article 4 (9), (15)
  - Article 22 (2(b)), (3a) (EP)
  - Article 23 (2a)
  - Article 24 (2)
  - Article 25 (1), (2(a)), (2(d)), (3), (3a), (4) while taking the outcome of the trilogue on Chapter V into account
  - Article 26 (1a), (2), (2(a)), (2(c)), (2(d)), (2(e)), (2(h)), (2a), (2aa), (2ab), (2b), (2c), (3a) EP
  - Article 28 (1) chapeau, (1(a)), (1(b)), (1(c)), (1(d)), (1(e)), (1(f)), (1(g)), (2a) chapeau, (2a(a)), (2a(b)), (2a(c)), (2a(d)), (3), (4), (4(b))
  - Article 29 (2)
  - Article 30 (1), (2), (2a), (2(b)) EP, (2b), (2(c)) EP
  - Article 31 (2), (3(a)), (3(b)), (3(c)), (3(d)), (4),
  - Article 32a EP (as a whole)
  - Article 33 (2) chapeau, (2(a)), (2(b)), (3(e)) EP, (3(f)) EP, (3(g)) EP, (3(h)) EP, (3(i)) EP, (3(j)) EP, (3a) EP, (3b) EP, (3a), (4)
  - Article 33a (new) EP (as a whole)
  - Article 34 (2), (2(a)), (2(b)), (3), (4), (6), (7), (7a)
  - Article 35 (2), (3), (4), (5), (6), (7), (8), (9)
  - Article 36 (2), (3), (4)
  - Article 37 (1(a)), (1(b)), (1(c)), (1(d)), (1(e)), (1(f)), (1(g)), (1(h)), (1(i)) EP, (2a)
  - Article 38 (1a) chapeau, (1a(aa)) EP, (1a(aa)), (1a(bb)), (1a(d)), (1a(e)), (1a(ee)), (1a(ef)), (1ab), (1b), (2), (2a), (2b), (3), (4), (5), (5a)
  - Article 38a (as a whole)
  - Article 39 (1a), (1a) EP, (1c) EP, (1d) EP, (1g) EP, (1h) EP, (2) EP, (2), (2a), (3), (4), (5)
  - Article 39a (as a whole)

The Presidency takes the view that no additional discussion is necessary on these articles. However, in case delegations wish to raise any crucial point or to provide further input relating to these provisions, they may do so under point 8. Where the text from the European Parliament has not been taken on board by the Presidency, the 4<sup>th</sup> column is left empty.

7. With regard to the position of the European Parliament and the Council's General Approach, as well as Member States' comments during the Friends of Presidency DAPIX meeting of 15<sup>th</sup> September 2015 and the JHA Counsellors meeting of 18<sup>th</sup> September 2015, the Presidency considers that compromises can be found on a certain number of provisions:

### General remarks

- The Council's General Approach, in order to illustrate when a processing is likely to result in a high risk for the rights and freedoms of individuals, repeats in Articles 31(1), 32(1) and 33(1) references to "discrimination, identity theft or fraud, financial loss, damage to the reputation, unauthorised reversal of pseudonymisation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage". For reasons of readability and clarity of the text, and without changing the substance, the Presidency suggests to regroup this list of examples in a recital (for instance recital 60a) instead of enumerating them in each article.
- The European Parliament's Article 32a identifies a certain number of elements to define "risk" "processing of personal data relating to more than 5000 data subjects during any consecutive 12-month period", "processing of special categories of data", "location data", "data on children" and data on "employees in large scale filing systems". These elements are used by the European Parliament in several instances of this chapter. The Presidency suggests not to take on board this Article, in particular since a number of these elements are already covered in recital 60a, and maintain the Council's risk-based approach.

12034/15 VH/tt 5
DGD 2C **LIMITE EN** 

### Article 22 – Obligations of the controller

- The Presidency takes the view that, in a spirit of compromise, the title of this article could be changed to "Responsibility or accountability of the controller".
- Concerning Article 22(1), the Presidency suggests to accept the wording of the European Parliament "appropriate technical and organizational measures to be able to demonstrate" without including the reference to "in a transparent manner".
- With regard to the European Parliament's reference to compliance policies that "shall to be reviewed at least every two years and updated when necessary" in its Article 22(1a), the Presidency suggests to add such a review obligation in Article 22(2a) without any reference to a strict periodicity.
- In its Article 22(3), the European Parliament keeps the reference to the accountability of the controller. The Presidency recognises that this accountability is already contained in Article 22(1) and therefore not necessary in Article 22(3).
- In its Article 22(3), the European Parliament added a reference to "any regular general reports of the activities of the controller, such as the obligatory reports by publicly traded companies, shall contain a summary of the measures referred to paragraph 1". The Presidency suggests to maintain the Council's General Approach.

#### Article 23 – Data protection by design and by default

- In its Article 23(1), the European Parliament has the terms "the state of the art" and makes a reference to "international best practices". The Presidency suggests to take on board "state of the art".
- The European Parliament introduces in its Article 22(1) the wording "both at the time of determination of the means for processing and at the time of the processing itself". The Presidency takes the view that these terms have an added value in the context of data protection by design and by default and suggests to incorporate these terms in Article 23(1).
- In Article 23(1), the Presidency suggests to reformulate, without changing the substance, and refer to "appropriate technical and organisational measures".

- In Article 23(1), and elsewhere in the Regulation, the Council's General Approach refers to the "likelihood and severity of the risk". The European Parliament uses simply the term "risk". Even if the concept of "risk" implies already the notions of likelihood and severity, the Presidency suggests to maintain the Council's General Approach for reasons of unambiguousness.
- Concerning Article 23(1), the colegislators approach the concept of data protection by design differently. While bearing in mind the Council's General Approach and in a view of finding a compromise solution, the Presidency takes the view that a reformulation of the principle could be helpful. Therefore, the Presidency suggests to add "technical and organisational measures which are designed to implement data protection principles in an effective way and to integrate the necessary safeguards into the processing in order to".
- With regard to the European Parliament's Article 23(1a) and the reference to Directive 2004/18/EC, the Presidency suggests to maintain the Council's General Approach while remaining flexible for a solution in a recital.
- The Council's General Approach in its Article 23(2) has the terms "without human intervention" when referring to default data protection settings. The Presidency suggests to replace these terms by "without the need of the individual's intervention" in the beginning of the sentence.
- The European Parliament, in its Article 23(2), considers that data protection by default "shall ensure that by default personal data are not made accessible to an indefinite number of individuals". The Council, in its Article 23(2) has the same idea but formulates this as a restriction based on the criterion of providing the public with information. The Presidency suggests to maintain the Council's General Approach while remaining flexible as to the exact formulation.

### Article 24 – Joint Controllers

- The European Parliament proposes in its Article 24(1) that "in case of unclarity of the responsibility, the controllers shall be jointly and severally liable". The Presidency takes the view that the triggering condition of "unclarity of the responsibility" does not ensure legal certainty. Furthermore, this is to be linked with Chapter VIII and should be clarified in particular in Article 77.
- The first sentence in the Council's General Approach in Article 24(3) clarifies that "the arrangement shall duly reflect the joint controller's respective effective roles vis-à-vis data subjects, and the essence of the arrangement shall be made available for the data subject". The European Parliament has the same sentence in its Article 24(1). However, the second sentence of Article 24(3) is not taken by the European Parliament. The Presidency considers that the second sentence is a restriction of the application of Article 24(2) on the exercise of his or her rights under this Regulation in respect of and against each of the controllers. The Presidency suggests to delete the second sentence.

### Article 25 – Representatives of controllers not established in the Union

In Article 25(2)(b), the European Parliament exempts from the obligation to designate a representative "controllers processing personal data which relates to less than 5000 data subjects during any consecutive 12-month period and not processing special categories of personal data as referred to in Article 9(1), location data or data on children or employees in large-scale filing systems". While there might be merit in retaining the exemption for controllers that do not process special categories of personal data or processing of data relating to criminal convictions and offences, the Presidency has doubts on the other cases proposed by the European Parliament. Therefore, the Presidency suggests not to take those additions on board except special categories of personal data or processing of data relating to criminal convictions and offences.

### Article 26 – Processor

- The Presidency considers there is added value in introducing in Article 26(1) the wordings "Where processing is to be carried out on behalf of the controller" and "and ensure the protection of the rights of the data subject".
- The European Parliament, in its Article 26(2(b)), refers to a commitment of confidentiality by employed staff to be included in the contract. The Presidency suggests to reintroduce the Article 26(2(b)) while reformulating it in order to make the provision more practicable.
- Concerning Article 26(2(f)), the Presidency suggests to integrate the European Parliament's addition "taking into account the nature of processing and the information available to the processor" in the article.
- Concerning Article 26(2(g)), the European Parliament added "and delete existing copies unless Union or Member State law requires storage of the data". The Presidency takes the view that the Council's General Approach can be usefully completed with this idea, subject to reformulation.
- Concerning Article 26(2(e)), the Presidency suggests to include, based on the European Parliament's text, a reference to the "appropriate technical and organisational requirements for the fulfillment of the controller's obligation" subject to redrafting.
- Concerning Article 26(3), the European Parliament refers to the instructions by the controller which shall be documented in writing. The Presidency takes the view that the term "instructions" can be added as a part of the contractual arrangement.
- The European Parliament maintains Article 26(4) with the addition "or become the determining party in relation to the purposes and means of data processing". The Presidency suggests to maintain the Council's General Approach on this article.

# <u>Article 27 – Processing under the authority of the controller and processor</u>

- As this provision has the merit to clarify processing under the authority of the controller or of the processor, the Presidency suggests to accept the reintroduction of this article in a spirit of compromise. This would entail the deletion of Article 30(2b) of the Council's General Approach.

## Article 28 – Records of categories of personal data processing activities

- The titles of this article are different for the European Parliament and the Council. The Presidency suggests to keep the terms "*Records of processing activities*" as the title of this Article 28.
- Concerning the 28(1(h)) and the 28(2a(e)), for the controller and the processor respectively, the Council's General Approach states that "where possible, a general description of the technical and organisational security measures referred to in Article 30(1)". The Presidency suggests to maintain these references.
- In Article 28(3a), the Council's General Approach requires that records shall be "in writing, including in an electronic or other non-legible form which is capable of being converted into a legible form". The Presidency suggests to simplify this wording.

### Article 29 – Co-operation with the supervisory authority

- Concerning Article 29(1), the European Parliament keeps the obligation for the controller and the processor to cooperate with the supervisory authority. The Presidency takes the view that the first sentence of the European Parliament can provide a helpful clarification for this chapter overall and suggests to reintroduce Article 29(1), limited to the first sentence "the controller and the processor and, if any, the representative of the controller shall co-operate, on request, with the supervisory authority in the performance of its tasks".

# Article 30 – Security of processing

- Article 30(1a) of the European Parliament makes a list of what should be contained in a security policy. The Presidency takes the view that the elements in this list could be useful indications for controllers and processors. Subject to redrafting, the Presidency suggests to introduce these elements as an indicative list in a recital.
- Concerning Article 30(3), the Presidency suggests maintaining the Council's General Approach while remaining flexible.

Article 31 – Notification of a personal data breach to the supervisory authority

Article 32 – Communication of a personal data breach to the data subject

12034/15 VH/tt 10
DGD 2C **LIMITE EN** 

- The European Parliament takes a gradual approach with regard to the obligations of notification and communication of a personal data breach. With a view to reaching a compromise, the Presidency considers there is merit in such a gradual approach while setting a higher threshold for notifying personal data breaches as compared to the European Parliament's approach. The Presidency suggests the following adaptations: if there is a risk (instead of a high risk as contained in the Council's General Approach), then a notification to the supervisory authority (Article 31) is required. Following the gradual approach, a communication to the data subject (Article 32) shall be done if there is a high risk.
- In Article 31(1a), the Council's General Approach refers to exceptions to the notification obligation to the supervisory authority. Given that the European Parliament does not foresee such an exception, and given the gradual approach proposed, the Presidency suggests to delete this paragraph.
- The European Parliament provides, in its Article 31(3(e)), that "the information may, if necessary, be provided in phases". Considering a similar approach adopted in the ePrivacy Directive, the Presidency takes the view that this idea could be included and merged, subject to redrafting, in Article 31(3a).
- Concerning Article 31(4a), the European Parliament proposes that "the supervisory authority shall keep a public register of the types of breaches notified". The Presidency takes the view that this can preferably be added in Chapter VI, for instance Article 54 concerning activity reports by supervisory authorities.
- Concerning Article 31(5) and Article 32(5), the European Parliaments provides for the European Data Protection Board to issue guidelines, recommendations and best practices for establishing the data breach (Article 31) and the circumstance that trigger communication to the data subject (Article 32). The Council's General Approach does not foresee such a task for the European Data Protection Board. The Presidency suggests to introduce such a task in Article 66.
- Concerning Article 32(2), the European Parliament's text contains a reference to Article 31(3(d)). The Presidency suggests to include this reference.
- Concerning Article 32(3(a)) of the Council's General Approach, the Presidency suggests to keep the terms "*in particular those*".
- Concerning Article 32(3(c)) of the Council's General Approach, the Presidency suggests to move the terms "in particular owing to the number of cases involved" into a recital.

12034/15 VH/tt 11
DGD 2C **LIMITE EN** 

- The Presidency considers that Article 32(3(d)) of the Council's General Approach constitutes a broad exception to the obligation for controllers to communicate personal data breaches to the data subject. The Presidency suggests to keep this exception but to add further safeguards.
- Concerning Article 32(4), the European Parliament keeps the idea that "if the controller has not already communicated the personal data breach to the data subject of the personal data breach, the supervisory authority, having considered the likely adverse effects of the breach, may require it to do so". The Presidency suggest to reintroduce this paragraph.

#### Article 33 – Data protection impact assessment

- The European Parliament has introduced in the last sentence of Article 33(1) that "a single assessment shall be sufficient to address a set of similar processing operations that present similar risks". The Presidency considers that this could be a useful addition, subject to redrafting, for reducing administrative burden for controllers.
- With regard to Article 33(1a) and Article 37(1(f)) of the Council's General Approach, the Presidency suggests to maintain the General Approach.
- In Article 33(2(c)), the Presidency suggests to reformulate in more technologically neutral and future proof way to cover the same idea: "systematic monitoring of a publicly accessible area on a large scale".
- The Presidency suggests to maintain the Council's General Approach when it comes to Article 33(2a), (2b) and (2c).
- In Article 33(3), the Council's General Approach and the European Parliament's text share the same idea but not the same structure. In a spirit of compromise, the Presidency suggests a change of structure and considers that Article 33(3(b)) can be accepted.

### Article 35 – Designation of the data protection officer

- Concerning Article 35(1), the European Parliament takes the approach of a mandatory data protection officer in certain situations. The Council's General Approach provides for an optional designation of a data protection officer. The Presidency suggests to maintain Council's General Approach, even though the Council will show no flexibility on its risk-based approach.
- Concerning Article 35(10), the Presidency suggests to move this paragraph to Article 36 which relates to the position of the data protection officer.

12034/15 VH/tt 12 DGD 2C **LIMITE EN** 

### Article 36 – Position of the data protection officer

- The Presidency considers the European Parliament's Article 36(4) as a useful clarification for the position of data protection officers and an additional guarantee for the controller, subject to redrafting.

## <u>Article 37 – Tasks of the data protection officer</u>

- Concerning Article 37(1), the European Parliament created an open list of the tasks of the data protection officer by adding "at least". The Presidency suggests to accept the approach of an open list of tasks.
- Concerning Article 37(1(j)) of the European Parliament's text relating to the task by the data protection officer "to inform the employee representatives on data processing of the employees", the Presidency suggests to maintain the Council's General Approach.

### Article 38 – Codes of conduct

- In Article 38(1), the Council's General Approach contains a reference to "*micro*, *small and medium sized enterprises*". The Presidency suggests to keep this reference.
- The European Parliament adds in Article 38(1(f)), (g) and (h) further elements to be included in codes of conduct. The Presidency considers there is merit to indicate out-of-court proceedings and other dispute resolution procedures as proposed in Article 38(1(h)).

### Article 39 - Certification

- In Article 39(1), the Council's General Approach contains a reference to "micro, small and medium sized enterprises". The Presidency suggests to keep this reference.
- Based on the European Parliament's Article 39(1b), the Presidency suggests to introduce, in a recital, a reference that "the certification shall be voluntary and available via a process that is transparent".
- In its Article 39(1e) and (1f), the European Parliament foresees that only "supervisory authorities shall grant controllers and processors who, pursuant to the auditing, have been certified that they process the data in compliance with this regulation". The Presidency considers this might constitute a substantial additional burden for supervisory authorities and suggests not to take such an approach.

12034/15 VH/tt 13
DGD 2C **LIMITE EN** 

- The Presidency considers there might be merit if the certification procedure foreseen by the Council's General Approach could result in a standardized data protection mark "European Data Protection Seal". Delegations are invited to share their view on this idea from the European Parliament.
- The Presidency suggests not to take on board the European Parliament's idea in Article 39(1i) concerning the task for the European Data Protection Board to certify that a "data protection—enhancing technical standard" is in compliance with the Regulation.

Member States are invited to confirm the Presidency's suggestions.

8. Finally, the Presidency invites the delegations to raise any other crucial issue related to Chapter IV.

The markings in this table are to be read as follows:

- Second column with first reading Position of the European Parliament: new text is marked in bold italics; deleted parts of the text are marked in strikethrough, text identical with the Commission proposal is marked - with a diagonal line in the box.
- Third column with General Approach of the Council: new text is marked in *bold italics*; deleted parts of the text are marked in strikethrough, parts of the text that have been moved up or down are marked in bold.
- Fourth column: the diagonal line in the box indicates that the text is identical for all three
  institutions; compromise suggestions by the Presidency are included, empty box indicates that
  no text is included.

12034/15 VH/tt 14
DGD 2C **LIMITE EN** 

COM (2012)0011	EP Position / First Reading	Council General Approach (15/06/2015)	Proposition of compromise
(60) Comprehensive responsibility	(60) Comprehensive responsibility	(60) Comprehensive The	(60) The responsibility of the
and liability of the controller for	and liability of the controller for	responsibility and liability of the	controller for any processing of
any processing of personal data	any processing of personal data	controller for any processing of	personal data carried out by the
carried out by the controller or on	carried out by the controller or on	personal data carried out by the	controller or on the controller's
the controller's behalf should be	the controller's behalf should be	controller or on the controller's	behalf should be established. In
established. In particular, the	established, in particular with	behalf should be established. In	particular, the controller should be
controller should ensure and be	regard to documentation, data	particular, the controller should	obliged to implement appropriate
obliged to demonstrate the	security, impact assessments, the	ensure and be obliged to implement	measures to be able to demonstrate
compliance of each processing	data protection officer and	appropriate measures and be able	the compliance of processing
operation with this Regulation.	oversight by data protection	to demonstrate the compliance of	activities with this Regulation.
	authorities. In particular, the	each-processing operation activities	These measures should take into
	controller should ensure and be	with this Regulation. <i>These</i>	account the nature, scope, context
	obliged able to demonstrate the	measures should take into account	and purposes of the processing and
	compliance of each processing	the nature, scope, context and	the risk for the rights and freedoms
	operation with this Regulation. <i>This</i>	purposes of the processing and the	of individuals.
	should be verified by independent	risk for the rights and freedoms of	
	internal or external auditors.	individuals.	
		(60a) Such risks, of varying	(60a) Such risks, of varying
		likelihood and severity, may result	likelihood and severity, may result
		from data processing which could	from data processing which could
		lead to physical, material or moral	lead to physical, material or moral
		damage, in particular where the	damage, in particular where the
		processing may give rise to	processing may give rise to
		discrimination, identity theft or	discrimination, identity theft or
		fraud, financial loss, damage to	fraud, financial loss, damage to the
		the reputation, loss of	reputation, loss of

confidentiality of data protected by professional secrecy, unauthorized reversal of pseudonymisation, 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.

confidentiality of data protected by professional secrecy, unauthorized reversal of pseudonymisation, 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.

	(60b) The likelihood and severity	(60b) The likelihood and severity of
	of the risk should be determined	the risk should be determined in
	in function of the nature, scope,	function of the nature, scope,
	context and purposes of the data	context and purposes of the data
	processing. Risk should be	processing. Risk should be
	evaluated on an objective	evaluated on an objective
	assessment, by which it is	assessment, by which it is
	established whether data	established whether data processing
	processing operations involve a	operations involve a high risk.
	high risk. A high risk is a	
	particular risk of prejudice to the	
	rights and freedoms of	
	individuals.	
	(60c) Guidance for the	(60c) Guidance for the
	implementation of appropriate	implementation of appropriate
	measures, and for demonstrating	measures, and for demonstrating
	the compliance by the controller or	the compliance by the controller or
	processor, especially as regards the	processor, especially as regards the
	identification of the risk related to	identification of the risk related to
	the processing, their assessment in	the processing, their assessment in
	terms of their origin, nature,	terms of their origin, nature,
	likelihood and severity, and the	likelihood and severity, and the
	identification of best practices to	identification of best practices to
	mitigate the risk, could be provided	mitigate the risk, could be provided
	in particular by approved codes of	in particular by approved codes of
	conduct, approved certifications,	conduct, approved certifications,
	guidelines of the European Data	guidelines of the European Data

Protection Board or through the Protection Board or through the indications provided by a data indications provided by a data protection officer. The European protection officer. The European Data Protection Board may also Data Protection Board may also issue guidelines on processing issue guidelines on processing operations that are considered to operations that are considered to be unlikely to result in a high risk for be unlikely to result in a high risk for the rights and freedoms of the rights and freedoms of individuals and indicate what individuals and indicate what measures may be sufficient in such measures may be sufficient in such cases to address such risk. cases to address such risk. Amendment 37 (61) The protection of the rights and freedoms of data subjects with and freedoms of data subjects with and freedoms of data subjects and freedoms of individuals with regard to the processing of personal regard to the processing of personal individuals with regard to the regard to the processing of personal data require that appropriate data require that appropriate processing of personal data require data require that appropriate technical and organisational technical and organisational that appropriate technical and technical and organisational measures are taken, both at the time measures are taken, both at the time organisational measures are taken, measures are taken, both at the time both at the time of the design of the of the design of the processing and of the design of the processing and of the design of the processing and at the time of the processing itself, at the time of the processing itself, processing and at the time of the at the time of the processing itself, to ensure that the requirements of to ensure that the requirements of processing itself, to ensure that the to ensure that the requirements of this Regulation are met. In order to this Regulation are met. In order to requirements of this Regulation are this Regulation are met. In order to ensure and demonstrate compliance ensure and demonstrate compliance met. In order to ensure and be able ensure and be able to demonstrate with this Regulation, the controller with this Regulation, the controller to demonstrate compliance with this compliance with this Regulation, should adopt internal policies and should adopt internal policies and the controller should implement Regulation, the controller should implement appropriate measures, implement appropriate measures, adopt internal policies and appropriate measures, which meet in particular the which meet in particular the implement appropriate measures,

principles of data protection by design and data protection by default. principles of data protection by design and data protection by default. The principle of data protection by design requires data protection to be embedded within the entire life cycle of the technology, from the very early design stage, right through to its ultimate deployment, use and final disposal. This should also include the responsibility for the products and services used by the controller or processor. The principle of data protection by default requires privacy settings on services and products which should by default comply with the general principles of data protection, such as data minimisation and purpose limitation.

which meet in particular the principles of data protection by design and data protection by default. Such measures could consist inter alia of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are either based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations.

which meet in particular the principles of data protection by design and data protection by default. Such measures could consist inter alia of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are either based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations.

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

(62) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processor, also in relation to the monitoring by and measures of supervisory authorities, requires a clear attribution of the responsibilities under this Regulation, including where a controller determines the purposes, conditions and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller. The arrangement between the joint controllers should reflect the joint controllers' effective roles and relationships. The processing of personal data under this Regulation should include the permission for a controller to transmit the data to a joint controller or to a processor for the processing of the data on their his or her behalf.

Amendment 38

(62) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors, 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, conditions and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.

(62) The protection of the rights and freedoms of data subjects as well as the responsibility of controllers and processors, 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. The arrangement between the joint controllers should duly reflect the ioint controllers' effective roles and relationships vis-à-vis the data subjects.

(63) Where a controller not established in the Union is processing personal data of data subjects residing in the Union whose processing activities are related to the offering of goods or services to such data subjects, or to the monitoring their behaviour, 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 or a public authority or body or where the controller is only occasionally offering goods or services to such data subjects. The representative should act on behalf of the controller and may be addressed by any supervisory authority.

(63) Where a controller not

Amendment 39

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, 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 or processing relates to fewer than 5000 data subjects during any consecutive 12-month period and is not carried out on special categories of personal data, or is a public authority or body or where the controller is only occasionally offering goods or services to such data subjects. The representative should act on behalf of the controller and may be addressed by any supervisory authority.

(63) Where a controller not established in the Union is processing personal data of data subjects residing in the Union whose processing activities are related to the offering of goods or services to such data subjects, or to the monitoring of their behaviour in the Union, the controller should designate a representative, unless the processing it carries out is occasional and unlikely to result in a risk for the rights and freedoms of data subjects, taking into account the nature, scope, context and purposes of the processing or the controller is established in a third country ensuring an adequate level of protection, or the controller is a small or medium sized enterprise or a public authority or body or where the controller is only occasionally offering goods or services to such data subjects. The representative should act on behalf of the controller and may be addressed by any supervisory authority.

(63) Where a controller or a processor not established in the Union is processing personal data of data subjects who are in the Union, and whose processing activities are related to the offering of goods or services to such data subjects, or to the monitoring of their behaviour in the Union, the controller or the processor should designate a representative, unless the processing it carries out is occasional, does not include processing of special categories of personal data or of data relating to criminal convictions and offences, and is unlikely to result in a risk for the rights and freedoms individuals, taking into account the nature, context, scope and purposes of the processing or the controller or the processor is a public authority body. or The representative should act on behalf of the controller or the processor and may be addressed, in particular, by supervisory authorities and data subjects.

		The representative should be	The representative should be
		explicitly designated by a written	explicitly designated by a written
		mandate of the controller to act on	mandate of the controller or the
		its behalf with regard to the latter's	processor to act on their respective
		obligations under this Regulation.	behalf with regard to their
		The designation of such	obligations under this Regulation.
		representative does not affect the	The designation of such
		responsibility and liability of the	representative does not affect the
		controller under this Regulation.	responsibility of the controller and
		Such representative should	the obligations of the processor
		perform its tasks according to the	under this Regulation. Such
		received mandate from the	representative should perform its
		controller, including to cooperate	tasks according to the received
		with the competent supervisory	mandate from the controller or the
		authorities on any action taken in	processor, including to cooperate
		ensuring compliance with this	with the competent supervisory
		Regulation. The designated	authorities on any action taken in
		representative should be subjected	ensuring compliance with this
		to enforcement actions in case of	Regulation. The designated
		non-compliance by the controller.	representative should be subjected
			to enforcement actions in case of
			non-compliance by the controller or
ļ			the processor.
		(63a) To ensure compliance with	(63a) To ensure compliance with
		the requirements of this	the requirements of this Regulation
		Regulation in respect of the	in respect of the processing to be
		processing to be carried out by the	carried out by the processor on
		processor on behalf of the	behalf of the controller, when
		controller, when entrusting a	entrusting a processor with
		processor with processing	processing activities, the controller
		activities, the controller should use	should use only processors

only processors providing

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. Adherence of the processor to an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the obligations of the controller. The carrying out of processing by a processor should be governed by a contract or other legal act under Union or Member State law, binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purposes of the processing, the type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk for the rights and freedoms of the data subject.

sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, technical implement and organisational measures which will meet the requirements of this Regulation, including for the security of processing. Adherence of the processor to an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the obligations of the controller. The carrying out of processing by a processor should be governed by a contract or other legal act under Union or Member State law, binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purposes of the processing, the type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk for the rights and freedoms of the data subject.

		The controller and processor may choose to use an individual contract or standard contractual clauses which are adopted either directly by the Commission or by a supervisory authority in accordance with the consistency mechanism and then adopted by the Commission, or which are part of a certification granted in the certification mechanism. After the completion of the processing on behalf of the controller, the processor should return or delete the personal data, unless there is a requirement to store the data under Union or Member State law to which the processor is subject.	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, at the choice of the controller, delete or return the personal data and delete existing copies, unless there is a requirement to store the data under Union or Member State law to which the processor is subject.
	Amendment 39		
(64) In order to determine whether a controller is only occasionally offering goods and services to data subjects residing in the Union, it should be ascertained whether it is apparent from the controller's overall activities that the offering of goods and services to such data subjects is ancillary to those main activities.	(64) In order to determine whether a controller is only occasionally offering goods and services to data subjects residing in the Union, it should be ascertained whether it is apparent from the controller's overall activities that the offering of goods and services to such data subjects is ancillary to those main activities.  **Amendment 41**	deleted	

(65) In order to demonstrate compliance with this Regulation, the controller or processor should document each processing operation. Each controller and processor should be obliged to cooperate with the supervisory authority and make this documentation, on request, available to it, so that it might serve for monitoring those processing operations.

(65) In order to be able to demonstrate compliance with this Regulation, the controller or processor should document each processing operation maintain the documentation necessary in order to fulfill the requirements laid down in this Regulation. Each controller and processor should be obliged to co-operate with the supervisory authority and make this documentation, on request, available to it, so that it might serve for monitoring those processing operations evaluating the compliance with this Regulation. However, equal emphasis and significance should be placed on good practice and compliance and not just the completion of documentation.

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

(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 cooperate with the supervisory authority and make these records, on request, available to it, so that it might serve for monitoring those processing operations.

(66) In order to maintain security and to prevent processing in breach of this Regulation, the controller or processor should evaluate the risks inherent to the processing and implement measures to mitigate those risks. These measures should ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks and the nature of the personal data to be protected. When establishing technical standards and organisational measures to ensure security of processing, the Commission should promote technological neutrality, interoperability and innovation, and, where appropriate, cooperate with third countries.

Amendment 42

(66) In order to maintain security and to prevent processing in breach of this Regulation, the controller or processor should evaluate the risks inherent to the processing and implement measures to mitigate those risks. These measures should ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks and the nature of the personal data to be protected. When establishing technical standards and organisational measures to ensure security of processing, the Commission should promote technological neutrality, interoperability and innovation should be promoted and, where appropriate, cooperation with third countries should be encouraged.

(66) In order to maintain security and to prevent processing in breach of this Regulation, the controller or processor should evaluate the risks inherent to the processing and implement measures to mitigate those risks. These measures should ensure an appropriate level of security including confidentiality, taking into account available technology the state of the art and the costs of their implementation in relation to the risks and the nature of the personal data to be protected. When establishing technical standards and organisational measures to ensure security of processing, the Commission should promote technological neutrality, interoperability and innovation, and, where appropriate, cooperate with third countries In assessing data security risk, consideration

(66) In order to maintain security and to prevent processing in breach of this Regulation, the controller or processor should evaluate the risks inherent to the processing and implement measures to mitigate those risks. These measures should ensure an appropriate level of security including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. Such measures could consist inter alia of the ability to ensure that the integrity of the personal data is validated: the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data; the ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident that impacts the availability, integrity and confidentiality of information systems and services; a process for regularly testing, assessing and evaluating the effectiveness of security policies, procedures and

	T	
		plans put in place to ensure ongoing
		effectiveness.
		In assessing data security risk,
		consideration should be given to the
		risks that are presented by data
		processing, such as accidental or
		unlawful destruction, loss,
		alteration, unauthorised disclosure
		of, or access to personal data
		transmitted, stored or otherwise
		processed, which may in particular
		lead to physical, material or moral
		damage.

should be given to the risks that	
are presented by data processing,	
such as accidental or unlawful	
destruction, loss, alteration,	
unauthorised disclosure of, or	
access to personal data	
transmitted, stored or otherwise	
processed, which may in particular	
lead to physical, material or moral	
damage.	
(66a) In order to enhance	(66a) In order to enhance
compliance with this Regulation in	compliance with this Regulation in
cases where the processing	cases where the processing
operations are likely to result in a	operations are likely to result in a
high risk for the rights and	high risk for the rights and
freedoms of individuals, the	freedoms of individuals, the
controller should be responsible	controller should be responsible for
for the carrying out of a data	the carrying out of a data protection
protection impact assessment to	impact assessment to evaluate, in
evaluate, in particular, the origin,	particular, the origin, nature,
nature, particularity and severity	particularity and severity of this
of this risk. The outcome of the	risk. The outcome of the assessment
assessment should be taken into	should be taken into account when
account when determining the	determining the appropriate
appropriate measures to be taken	measures to be taken in order to
in order to demonstrate that the	demonstrate that the processing of
	<u> </u>
processing of personal data is in	personal data is in compliance with
compliance with this Regulation.	this Regulation.

Where a data protection impact Where a data protection impact assessment indicates that assessment indicates that processing operations involve a processing operations involve a high risk which the controller high risk which the controller cannot mitigate by appropriate cannot mitigate by appropriate measures in terms of available measures in terms of available technology and costs of technology and costs ofimplementation, a consultation of implementation, a consultation of the supervisory authority should the supervisory authority should take place prior to the processing. take place prior to the processing. Amendment 43 (67) A personal data breach may, if not addressed in an adequate and timely manner, result in substantial timely manner, result in substantial timely manner, result in physical, timely manner, result in physical, economic loss and social harm, economic loss and social harm, material or moral damage to material or moral damage to individuals such as substantial individuals such loss of control including identity fraud, to the including identity fraud, to the individual concerned. Therefore, as individual concerned. Therefore, as economic loss of control over their over their personal data soon as the controller becomes soon as the controller becomes personal data or limitation of their limitation oftheir rights, aware that such a breach has discrimination, identity theft or rights, discrimination, identity aware that such a breach has occurred, the controller should occurred, the controller should theft or fraud, financial loss, fraud, financial loss, unauthorized notify the breach to the supervisory notify the breach to the supervisory unauthorized reversal of of pseudonymisation, reversal authority without undue delay and, authority without undue delay and, pseudonymisation, damage to the damage to the reputation, loss of where feasible, within 24 hours. where feasible, within 24, which reputation, loss of confidentiality confidentiality of data protected by Where this cannot achieved within should be presumed to be not later of data protected by professional professional secrecy or any other than 72 hours. Where this cannot 24 hours, an explanation of the secrecy or any other economic or economic or disadvantage to the reasons for the delay should achieved within 24 hours If and social harm, including identity individual concerned. accompany the notification. applicable, an explanation of the fraud, disadvantage to the individual concerned reasons for the delay should accompany the notification.

The individuals whose personal data could be adversely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions. A breach should be considered as adversely affecting the personal data or privacy of a data subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation. The notification should describe the nature of the personal data breach as well as recommendations 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 chance for data subjects to mitigate an immediate risk of harm would call for a

The individuals whose personal data could be adversely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions. A breach should be considered as adversely affecting the personal data or privacy of a data subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation. The notification should describe the nature of the personal data breach and formulate as well as recommendations 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 chance for data

Therefore, as soon as the controller becomes aware that such a personal data breach which may result in physical, material or moral damage has occurred, the controller should notify the breach to the supervisory authority without undue delay and, where feasible, within 24 72 hours. Where this cannot *be* achieved within 24 72 hours, an explanation of the reasons for the delay should accompany the notification. The individuals whose rights and freedoms personal data could be adversely severely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions. A breach should be considered as adversely affecting the personal data or privacy of a data subject where it could result in. for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation. The notification should describe the nature of the personal data breach as well as

Therefore, as soon as the controller becomes aware that a personal data breach which may result in physical, material or moral damage has occurred, the controller should notify the breach to the supervisory authority without undue delay and, where feasible, within 72 hours. Where this cannot be achieved within 72 hours, an explanation of the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay.

(67a new) The individuals whose rights and freedoms could be severely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions. The notification should describe the nature of the personal data breach as well as recommendations for the individual concerned to mitigate potential adverse effects. Notifications to data subjects should be made as soon as reasonably feasible, and in close cooperation with the supervisory authority and respecting guidance provided by it or other relevant

	authorities (e.g. law enforcement
	authorities). For example, the need
	to mitigate an immediate risk of
	damage would call for a prompt
	notification of data subjects
	whereas the need to implement
	appropriate measures against
	continuing or similar data breaches
	may justify a longer delay.

prompt notification of data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify a longer delay. subjects 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.

recommendations 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 chance for data subjects need to mitigate an immediate risk of harmdamage 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 should be ascertained whether the controller has implemented and applied appropriate technological protection and organisational measures to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject, before a damage to personal and economic interests occurs, taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject.

(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 should be ascertained whether the controller has implemented and applied appropriate technological protection and organisational measures to establish immediately whether a personal data/breach has taken place and to inform promptly the supervisory authority and the data subject, before/a damage to personal and economic interests occurs, taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data/subject.

(68) In order to determine It must whether a personal data breach is notified to the supervisory authority and to the data subject without undue delay, it should be ascertained whether the controller has implemented and applied 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. before a damage to personal and economic interests occurs, The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation.

(68) It must be ascertained whether appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation.

(68a) The communication of a (68a) The communication of a personal data breach to the data personal data breach to the data subject should not be required if subject should not be required if the the controller has implemented controller has implemented appropriate technological appropriate technological and organisational measures, and that protection measures, and that those measures were applied to the those measures were applied to the data affected by the personal data data affected by the personal data breach. Such technological breach. Such technological protection measures should protection measures should include include those that render the data those that render the data unintelligible to any person who is unintelligible to any person who is not authorised to access it, in not authorised to access it, in particular by encrypting the particular by encrypting the personal data. personal data. (69) In setting detailed rules (69) In setting detailed rules (69) In setting detailed rules concerning the format and concerning the format and concerning the format and procedures applicable to the procedures applicable to the procedures applicable to the notification of personal data notification of personal data notification of personal data breaches, due consideration should breaches, due consideration should breaches, due consideration should be given to the circumstances of be given to the circumstances of the be given to the circumstances of the the breach, including whether or breach, including whether or not breach, including whether or not not personal data had been personal data had been protected by personal data had been protected by protected by appropriate technical appropriate technical protection appropriate technical protection protection measures, effectively measures, effectively limiting the measures, effectively limiting the limiting the likelihood of identity likelihood of identity fraud or other likelihood of identity fraud or other fraud or other forms of misuse. forms of misuse. 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 obligation should be abolished, and replaced by effective procedures and mechanism which focus instead on those processing operations which are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes. In such cases, a data protection impact assessment should be carried out by

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 obligation should be abolished, and replaced by effective procedures and mechanism which focus instead on those processing operations which are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes. In such cases, a data protection impact assessment should be carried out by

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 *types of* processing operations which are likely to present specific result in a high risks to the rights and freedoms of data subjectsindividuals by virtue of their nature, their scope, context and or their purposes. In such

(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 types of processing operations which are likely to result in a high risks to the rights and freedoms of individuals by virtue of their nature, scope, context and purposes.

the controller or processor prior to the controller or processor prior to Such types of processing operations cases, a data protection impact the processing, which should assessment should be carried out by the processing, which should may be those which in particular, include in particular the envisaged include in particular the envisaged the controller or processor prior to involve using new technologies, or measures, safeguards and measures, safeguards and the types of processing, operations are of a new kind and where no data mechanisms for ensuring the mechanisms for ensuring the may be those which should include protection impact assessment has protection of personal data and for protection of personal data and for in particular, involve using new been carried out before by the demonstrating the compliance with demonstrating the compliance with technologies, or are of a new kind controller, or where they become necessary in the light of the time this Regulation. this Regulation. and where no data protection that has elapsed since the initial impact assessment has been carried out before by the processing. controller, or where they become necessary in the light of the time that has elapsed since the initial processing the envisaged measures, safeguards and mechanisms for ensuring the protection of personal data and for demonstrating the compliance with this Regulation. (70a) In such cases, a data (70a) In such cases, a data protection impact assessment protection impact assessment should be carried out by the should be carried out by the controller prior to the processing in controller prior to the processing in order to assess the particular order to assess the particular likelihood and severity of the high likelihood of the high risk, taking into account the nature, scope, risk, taking into account the nature, scope, context and context and purposes of the purposes of the processing and the processing and the sources of the sources of the risk, which should risk, which should

include in particular the envisaged include in particular the envisaged measures, safeguards and measures, safeguards and mechanisms for mitigating that mechanisms for mitigating that risk risk and for ensuring the and for ensuring the protection of personal data and for demonstrating protection of personal data and for demonstrating the compliance with the compliance with this this Regulation. Regulation. (71) This should in particular apply (71) This should in particular apply/ (71) This should in particular apply (71) This should in particular apply to newly established large-scale to newly established large scale to newly established large scale large-scale processing filing systems, which aim at filing systems, which aim at filing systems processing operations, which aim at processing processing a considerable amount processing a considerable amount operations, which aim at a considerable amount of personal of personal data at regional, of personal data at regional, processing a considerable amount data at regional, national or national or supranational level and national or supranational level and of personal data at regional, supranational level and which could which could affect a large number which could affect a large number national or supranational level and affect a large number of data of data subjects. of data subjects. which could affect a large number subjects and which are likely to of data subjects and which are result in a high risk, for example, likely to result in a high risk, for on account of their sensitivity, example, on account of their where in accordance with the sensitivity, where in accordance achieved state of the art a new technology is used on a large scale with the achieved state of technological knowledge a new as well as to other processing technology is used on a large scale operations which result in a high as well as to other processing risk for the rights and freedoms of operations which result in a high data subjects, in particular where risk for the rights and freedoms of those operations render it more data subjects, in particular where difficult for data subjects those operations render it more exercise their rights. A data difficult for data subjects to protection impact assessment should also be made in cases where data are processed for taking decisions regarding specific individuals following anv

	systematic and extensive evaluation of personal aspects relating to natural persons based on automated processing, including profiling, profiling those data or following the processing of special categories of personal data, biometric data, or data on criminal convictions and offences or related security measures. A data protection impact
	personal data, biometric data, or data on criminal convictions and offences or related security measures. A data protection impact assessment is equally required for systematic monitoring publicly accessible areas on a large scale, such as when using optic-electronic devices or for any other operations where the competent supervisory authority considers that the processing is likely to result in a high risk for the rights and freedoms of data subjects, in
	particular because they prevent data subjects from exercising a right or using a

exercise their rights. A data protection impact assessment should also be made in cases where data are processed for taking decisions regarding specific individuals following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data or following the processing of special categories of personal data, biometric data, or data on criminal convictions and offences or related security measures. A data protection impact assessment is equally required for monitoring publicly accessible areas on a large scale, especially when using optic-electronic devices or for any other operations where the competent supervisory authority considers that the processing is likely to result in a high risk for the rights and freedoms of data subjects, in particular because they prevent data subjects from exercising a right or using a

service or a contract, or because they are carried out systematically on a large scale. The processing of personal data should not be considered as being on a large scale if the processing concerns personal data from patients or clients by an individual doctor, health care professional or attorney. In these cases a data protection impact assessment should not be mandatory.

	service or a contract, or because they are carried out systematically on a large scale. The processing of personal data irrespective of the volume or the nature of the data, should not be considered as being on a large scale, if the processing of these data is protected by professional secrecy, such as the processing of personal data from patients or clients by an individual doctor, health care professional, hospital or attorney. In these cases a data protection impact assessment should not be mandatory.	
Amendment 44		
(71a) Impact assessments are the essential core of any sustainable data protection framework, making sure that businesses are aware from the outset of all possible consequences of their data processing operations. If impact assessments are thorough, the likelihood of any data breach or privacy-intrusive operation can		

be fundamentally limited. Data protection impact assessments should consequently have regard to the entire lifecycle management of personal data from collection to processing to deletion, describing in detail the envisaged processing operations, the risks to the rights	
and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure compliance with the this R+egulation.  Amendment 45	
(71b) Controllers should focus on the protection of personal data throughout the entire data lifecycle from collection to processing to deletion by investing from the outset in a sustainable data management framework and by following it up with a comprehensive compliance mechanism.	

(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.	(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.	(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.	(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.
widery used norizontal activity.	Amendment 46	used nortzontal activity.	Juscu Horizontal activity.
(73) Data protection impact assessments should 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.	deleted	(73) Data protection impact assessments should 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.	(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 processing operations involve a high degree of specific risks to the rights and freedoms of data subjects, such as excluding individuals from their right, or by the use of specific new technologies, the supervisory authority should be consulted, prior to the start of operations, on a risky processing which might not be in compliance with this Regulation, and to make proposals to remedy such situation. Such consultation should equally take place in the course of the preparation either of a measure by the national parliament or of a measure based on such legislative measure which defines the nature of the processing and lays down appropriate safeguards.

## Amendment 47

(74) Where a data protection impact assessment indicates that processing operations involve a high degree of specific risks to the rights and freedoms of data subjects, such as excluding individuals from their right, or by the use of specific new technologies, the data protection officer or the supervisory authority should be consulted, prior to the start of operations, on a risky processing which might not be in compliance with this Regulation, and to make proposals to remedy such situation. Such A consultation of the supervisory authority should equally take place in the course of the preparation either of a measure by the national parliament or of a measure based on such legislative measure which defines the nature of the processing and lays down appropriate safeguards.

(74) Where a data protection impact assessment indicates that *the* processing would, despite the envisaged safeguards, security measures and mechanisms to mitigate the operations involve a high degree of specific risks to the result in a high risk to the rights and freedoms of data subjects individuals and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, such as excluding individuals from their right, or by the use of specific new technologies, the supervisory authority should be consulted, prior to the start of operationsprocessing activities, on a risky processing which might not be in compliance with this Regulation, and to make proposals to remedy such situation.

(74) Where a data protection impact assessment indicates that processing would, despite the envisaged safeguards, security and mechanisms measures mitigate the risk, result in a high risk to the rights and freedoms of individuals and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, supervisory authority should be consulted, prior to the start of processing activities. Such high risk is likely to result from certain types of data processing and the extent and frequency of processing, which may result also in a realisation of damage or interference with the rights and freedoms ofindividual. The supervisory authority should respond to the request for consultation in a defined period. However, the absence of a the supervisory reaction of authority within this period should be without prejudice to any intervention of the supervisory authority in accordance with its tasks and powers laid down in this

	Regulation, including the power to prohibit processing operations. As part of this consultation process, the
	outcome of a data protection impact
	assessment carried out with regard
	to the processing at issue pursuant
	to Article 33 may be submitted to
	the supervisory authority, in
	particular the measures envisaged
	to mitigate the risk for the rights
	and freedoms of individuals.

Such consultation should equally take place in the course of the preparation either of a measure by the national parliament or of a measure based on such legislative measure which defines the nature of the processing and lays down appropriate safeguards. Such high risk is likely to result from certain types of data processing and certain extent and frequency of processing, which may result also in a realisation of damage or interference with the rights and freedoms of the data subject. The supervisory authority should respond to the request for consultation in a defined period. However, the absence of a reaction of the supervisory authority within this period should be without prejudice to any intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation, including the power to prohibit processing operations. As part of this consultation process,

	the outcome of a data protection impact assessment carried out with regard to the processing at issue pursuant to Article 33 may be submitted to the supervisory authority, in particular the measures envisaged to mitigate the risk for the rights and freedoms of individuals.	
Amendment 48	inuiviuuuis.	
Amenament 48  (74a) Impact assessments can only be of help if controllers make sure that they comply with the promises originally laid down in them. Data controllers should therefore conduct periodic data protection compliance reviews demonstrating that the data processing mechanisms in place comply with assurances made in the data protection impact assessment. It should further demonstrate the ability of the data controller to comply with the autonomous choices of data subjects. In addition, in case the review finds compliance inconsistencies, it should highlight these and present recommendations on how to achieve full compliance.		

(74a) The processor should assist	(74a) The processor should assist
the controller, where necessary	the controller, where necessary and
and upon request, in ensuring	upon request, in ensuring
compliance with the obligations	compliance with the obligations
deriving from the carrying out of	deriving from the carrying out of
data protection impact assessments	data protection impact assessments
and from prior consultation of the	and from prior consultation of the
supervisory authority.	supervisory authority.
(74b) A consultation with the	(74b) A consultation with the
supervisory authority should also	supervisory authority should also
take place in the course of the	take place in the course of the
preparation of a legislative or	preparation of a legislative or
regulatory measure which provides	regulatory measure which provides
for the processing of personal	for the processing of personal data,
data, in order to ensure the	in order to ensure the compliance of
compliance of the intended	the intended processing with this
processing with this Regulation	Regulation and in particular to
and in particular to mitigate the	mitigate the risk involved for the
risk involved for the data subject.	data subject.

(75) Where the processing is carried out in the public sector or where, in the private sector, processing is carried out by a large enterprise, or where its core activities, regardless of the size of the enterprise, involve processing operations which require regular and systematic monitoring, a person should 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 independently.

(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 relates to more than 5000 data subjects within 12 months, or where its core activities, regardless of the size of the enterprise, involve processing operations on sensitive data, or processing operations which require regular and systematic monitoring, a person should assist the controller or processor to monitor internal compliance with this Regulation. When establishing whether data about a large number of data subjects are processed, archived data that are restricted in such a way that they are not subject to the normal data access and processing operations of the controller and can no longer be changed should not be taken into account. Such data protection officers, whether or not an employee of the controller and

Amendment 49

(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 should 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* independently manner.

(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.

	1	
	not performing that	
task full til	<i>ne</i> , should be in a	
position to	perform their duties and	
tasks indep	endently <i>and enjoy</i>	
special pro	tection against	
	Final responsibility	
	with the management	
	nisation. The data	
	officer should in	
	be consulted prior to the	
	oc consuited prior to the ocurement, development	
9 . 1	-up of systems for the	
	processing of personal	
	_	
	der to ensure the	
	of privacy by design and	
privacy by	·	
	Amendment 50	
(75a) The	data protection officer	
should hav	e at least the following	
qualificati	ons: extensive	
	of the substance and	
S .	of data protection law,	
	technical and	
	onal measures and	
	s; mastery of technical	
-	nts for privacy by	
<u> </u>	vacy by default and data	
uesign, pri	vacy by acjaun ana aana	

security; industry-specific knowledge in accordance with the size of the controller or processor and the sensitivity of the data to be processed; the ability to carry out inspections, consultation, documentation, and log file analysis; and the ability to work with employee representation. The controller should enable the data protection officer to take part in advanced training measures to maintain the specialized knowledge required to perform his or her duties. The designation as a data protection officer does not necessarily require fulltime occupation of the respective employee.

(76) Associations or other bodies representing categories of controllers 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.

(76) Associations or other bodies representing categories of controllers should be encouraged, after consultation of the representatives of the employees, 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. Such codes should make compliance with this Regulation easier for industry.

Amendment 51

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

(76) Associations or other bodies representing categories 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 small and micro. medium enterprises. In particular such codes of conduct could calibrate the obligations of controllers and processors, taking into account the risk likely to result from the processing for the rights and freedoms of individuals. Such codes may be used as an element to demonstrate compliance with this Regulation.

		(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.	(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.
(	Amendment 52		
(77) In order to enhance	(77) In order to enhance	(77) In order to enhance	(77) In order to enhance
transparency and compliance with this Regulation, the establishment	transparency and compliance with this Regulation, the establishment	transparency and compliance with this Regulation, the establishment	transparency and compliance with this Regulation, the establishment
of certification mechanisms, data	of certification mechanisms, data	of certification mechanisms, data	of certification mechanisms, data
protection seals and marks should	protection seals and <i>standardised</i>	protection seals and marks should	protection seals and marks should
be encouraged, allowing data	marks should be encouraged,	be encouraged, allowing data	be encouraged, allowing data
subjects to quickly assess the level	allowing data subjects to quickly,	subjects to quickly assess the level	subjects to quickly assess the level
of data protection of relevant	reliably and verifiably assess the	of data protection of relevant	of data protection of relevant
products and services.	level of data protection of relevant products and services.	products and services.	products and services.

A "European Data Protection	
Seal" should be established on the	
European level to create trust	
among data subjects, legal	
certainty for controllers, and at the	
same time export European data	
protection standards by allowing	
non-European companies to more	
easily enter European markets by	
being certified.	

Article 4	Article 4	Article 4	
Definitions	Definitions	Definitions	
(9) 'personal data breach' means a	(9) 'personal data breach' means a	(9) 'personal data breach' means a	(9) 'personal data breach' means a
breach of security leading to the	breach of security leading to the	breach of security leading to the	breach of security leading to the
accidental or unlawful destruction,	accidental or unlawful destruction,	accidental or unlawful destruction,	accidental or unlawful destruction,
loss, alteration, unauthorised	loss, alteration, unauthorised	loss, alteration, unauthorised	loss, alteration, unauthorised
disclosure of, or access to, personal	disclosure of, or access to, personal	disclosure of, or access to, personal	disclosure of, or access to, personal
data transmitted, stored or	data transmitted, stored or	data transmitted, stored or	data transmitted, stored or
otherwise processed;	otherwise processed;	otherwise processed;	otherwise processed;
(15) 'enterprise' means any entity	(15) 'enterprise' means any entity	(15) 'enterprise' means any <i>natural</i>	(15) 'enterprise' means any natural
engaged in an economic activity,	engaged in an economic activity,	or legal person entity engaged in an	or legal person engaged in an
irrespective of its legal form, thus	irrespective of its legal form, thus	economic activity, irrespective of	economic activity, irrespective of
including, in particular, natural and	including, in particular, natural and	its legal form, thus including, in	its legal form, including,
legal persons, partnerships or	legal persons, partnerships or	<del>particular, natural and legal</del>	partnerships or associations
associations regularly engaged in	associations regularly engaged in an	<del>persons,</del> partnerships or	regularly engaged in an economic
an economic activity;	economic activity;	associations regularly engaged in an	activity;
		economic activity;	

CHAPTER IV CONTROLLER AND PROCESSOR SECTION 1	CHAPTER IV CONTROLLER AND PROCESSOR SECTION 1	CHAPTER IV CONTROLLER AND PROCESSOR SECTION 1	
GENERAL OBLIGATIONS	GENERAL OBLIGATIONS	GENERAL OBLIGATIONS	
Article 22	Article 22	Article 22	
	Amendment 117		
Responsibility of the controller	Responsibility and accountability of the controller	Responsibility-Obligations of the controller	Responsibility or accountability of the controller
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.	1. The controller shall adopt appropriate policies and implement appropriate an demonstrable technical and organisational measures to ensure and be able to demonstrate in a transparent manner that the processing of personal data is performed in compliance with this Regulation, having regard to the state of the art, the nature of personal data processing, the context, scope and purposes of processing, the risks for the rights and freedoms of the	1. Taking into account the nature, scope, context and purposes of the processing as well as the likelihood and severity of risk for the rights and freedoms of individuals, It he 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.	1. Taking into account the nature, scope, context and purposes of the processing as well as the likelihood and severity of risk for the rights and freedoms of individuals, the controller shall implement appropriate measures to be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.

	data subjects and the type of the organisation, both at the time of the determination of the means for processing and at the time of the processing itself.  1a. Having regard to the state of the art and the cost of implementation, the controller shall take all reasonable steps to implement compliance policies and procedures that persistently respect the autonomous choices of data subjects. These compliance policies shall be reviewed at least every two years and updated where necessary.		
2. The measures provided for in paragraph 1 shall in particular include:	deleted	deleted	
(a) keeping the documentation pursuant to Article 28;	deleted	deleted	
(b) implementing the data security requirements laid down in Article 30;	deleted	deleted	
(c) performing a data protection impact assessment pursuant to Article 33;	deleted	deleted	

(d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2);	deleted	deleted	
(e) designating a data protection officer pursuant to Article 35(1).	deleted	deleted	
officer pursuant to ratione 35(1).		2a. Where proportionate in relation to the processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.	2a. Where proportionate in relation to the processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller. These measures shall be reviewed and updated where necessary.
		2b. Adherence to approved codes of conduct pursuant to Article 38 or an approved certification mechanism pursuant to Article 39 may be used as an element to demonstrate compliance with the obligations of the controller.	2b. Adherence to approved codes of conduct pursuant to Article 38 or an approved certification mechanism pursuant to Article 39 may be used as an element to demonstrate compliance with the obligations of the controller.
3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2.	3. The controller shall implement mechanisms to ensure the verification of thebe able to demonstrate the adequacy and effectiveness of the measures referred to in paragraphs 1 and 2.	deleted	

If proportionate, this verification	If proportionate, this verification	
shall be carried out by independent	shall be carried out by independent	
internal or external auditors.	internal or external auditors Any	
	regular general reports of the	
	activities of the controller, such as	
	the obligatory reports by publicly	
	traded companies, shall contain a	
	summary description of the	
	policies and measures referred to	
	in paragraph 1.	
	3a. The controller shall have the	
	right to transmit personal data	
	inside the Union within the group	
	of undertakings the controller is	
	part of, where such processing is	
	necessary for legitimate internal	
	administrative purposes between	
	connected business areas of the	
	group of undertakings and an	
	adequate level of data protection	
	as well as the interests of the data	
	subjects are safeguarded by	
	internal data protection provisions	
	or equivalent codes of conduct as	
	referred to in Article 38.	

4. The Commission shall be	deleted	deleted	
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.			

Article 23	Article 23	Article 23	
Data protection by design and by	Data protection by design and by	Data protection by design and by	
default	default	default	
	Amendment 118		
1. Having regard to the state of the	1. Having regard to the state of the	1. Having regard to <i>available</i>	1. Having regard to the state of the
art and the cost of implementation,	art and the cost of implementation,	technology the state of the art and	art and the cost of implementation
the controller shall, both at the time	current technical knowledge,	the cost of implementation and	and taking account of the nature,
of the determination of the means	international best practices and	taking account of the nature,	scope, context and purposes of the
for processing and at the time of the	the risks represented by the data	scope, context and purposes of the	processing as well as the likelihood
processing itself, implement	processing, the controller and the	processing as well as the likelihood	and severity of the risk for rights
appropriate technical and	processor, if any, shall, both at the	and severity of the risk for rights	and freedoms of individuals posed
organisational measures and	time of the determination of the	and freedoms of individuals posed	by the processing, the controllers
procedures in such a way that the	purposes and means for processing	by the processing, the controllers	shall, both at the time of the
processing will meet the	and at the time of the processing	shall, both at the time of the	determination of the means for
requirements of this Regulation and	itself, implement appropriate and	determination of the means for	processing and at the time of the
ensure the protection of the rights	<i>proportionate</i> technical and	processing and at the time of the	processing itself, implement
of the data subject.	organisational measures and	processing itself, implement	appropriate technical and
	procedures in such a way that the	appropriate technical and	organisational measures, such as
	processing will meet the	organisational measures	data minimisation and
	requirements of this Regulation and	appropriate to the processing	pseudonymisation, which are
	ensure the protection of the rights	activity being carried out and its	designed to implement data
	of the data subject, in particular	objectives, such as data	protection principles in an effective
	with regard to the principles laid	minimisation and	way and to integrate the necessary
	down in Article 5. Data protection	pseudonymisation, and procedures	safeguards into the processing in
	by design shall have particular	in such a way that the processing	order to meet the requirements of
	regard to the entire lifecycle	will meet the requirements of this	this Regulation and protect the
	management of personal data	Regulation and ensure protect the	rights of data subjects.
	from collection to processing to	<del>protection of the rights of the data</del>	
		subjects.	

	· · · · · · · · · · · · · · · · · · ·
deletion, systematically foc	using
on comprehensive procedu	ral
safeguards regarding the	
accuracy, confidentiality, in	ntegrity,
physical security and deleti	on of
personal data. Where the	
controller has carried out a	data data
protection impact assessme	nt
pursuant to Article 33, the	results
shall be taken into account	when
developing those measures	and
procedures.	
1a. In order to foster its	
widespread implementation	in
different economic sectors,	data
protection by design shall b	pe a
prerequisite for public	
procurement tenders accor	ding to
Directive 2004/18/EC of the	
European Parliament and	
Council <sup>1</sup> as well as accordi	
Directive 2004/17/EC of the	
European Parliament and	
Council <sup>2</sup> (Utilities Directive	
Directive 2004/18/EC of	
European Parliament and	· ·
Council of 31 March 2004	
coordination of procedures	
award of public works cont	
public supply contracts and	
service contracts (OJ L 134	
30.4.2004, p. 114).	

	<sup>2</sup> Directive 2004/17/EC of the European Parliament and of the Council of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sector (OJ L 134, 30.4.2004, p.1)		
2. The controller shall implement	2. The controller shall implement	2. The controller shall implement	2. The controller shall implement
mechanisms for ensuring that, by	mechanisms for ensuring ensure	mechanisms appropriate measures	appropriate measures for ensuring
default, only those personal data are	that, by default, only those personal	for ensuring that, by default, only	that, by default, whithout the need
processed which are necessary for	data are processed which are	those personal data are processed	of the individual's intervention,
each specific purpose of the	necessary for each specific purpose	which are necessary for each	only personal data which are
processing and are especially not	of the processing and are especially	specific purpose of the processing	necessary for each specific purpose
collected or retained beyond the	not collected-or, retained or	and are especially not collected or	of the processing are processed; this
minimum necessary for those	disseminated beyond the minimum	retained beyond the minimum	applies to the amount of data
purposes, both in terms of the	necessary for those purposes, both	necessary for those purposes, both	collected, the extent of their
amount of the data and the time of	in terms of the amount of the data	in terms of are processed; this	processing, the period of their
their storage. In particular, those	and the time of their storage. In	<i>applies to</i> the amount of the data	storage and their accessibility.
mechanisms shall ensure that by	particular, those mechanisms shall	collected, the extent of their	Where the purpose of the
default personal data are not made	ensure that by default personal data	processing, and the time period of	processing is not intended to
accessible to an indefinite number	are not made accessible to an	their storage and their accessibility.	provide the public with information,
of individuals.	indefinite number of individuals	Where the purpose of the	mechanisms shall ensure that by
	and that data subjects are able to	processing is not intended to	default personal data are not made
	control the distribution of their	provide the public with	accessible to an indefinite number
	personal data.	informationIn particular, those	of individuals.

		mechanisms shall ensure that by	
		default personal data are not made	
		accessible without human	
		intervention to an indefinite	
		number of individuals.	
			2a An approved contification
		2a. An approved certification	2a. An approved certification
		mechanism pursuant to Article 39	mechanism pursuant to Article 39
		may be used as an element to	may be used as an element to
		demonstrate compliance with the	demonstrate compliance with the
		requirements set out in paragraphs	requirements set out in paragraphs 1
		1 and 2.	and 2.
3. The Commission shall be	deleted	deleted	
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	deleted	deleted	
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).			

Article 24	Article 24	Article 24	Article 24
Joint controllers	Joint controllers	Joint controllers	Joint controllers
	Amendment 119		
Where a controller determines the purposes, conditions and means of the processing of personal data jointly with others, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them.	Where a controllers jointly determine the purposes, conditions and means of the processing of personal data jointly with others, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them. The arrangement shall duly reflect the joint controllers' respective effective roles and relationships vis-à-vis data subjects, and the essence of the arrangement shall be made available for the data subject. In case of unclarity of the responsibility, the controllers shall be jointly and severally liable.	1. Where two or more acontrollers jointly determines the purposes; eonditions and means of the processing of personal data jointly with others, they are joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 14 and 14a, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement shall designate which of the joint controllers shall act as single point of contact for data subjects to exercise their rights.	I. Where two or more controllers jointly determine the purposes and means of the processing of personal data, they are joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement shall designate a single point of contact for data subjects to exercise their rights.

		2. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.  3. The arrangement shall duly reflect the joint controllers' respective effective roles and relationships vis-à-vis data subjects, and the essence of the arrangement shall be made available for the data subject. Paragraph 2 does not apply where the data subject has been informed in a transparent and unequivocal manner which of the joint controllers is responsible, unless such arrangement other than one determined by Union or Member State law is unfair with regard to his or her rights.	2. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.  3. The arrangement shall duly reflect the joint controllers' respective effective roles and relationships vis-à-vis data subjects, and the essence of the arrangement shall be made available for the data subject.
Article 25	Article 25	Article 25	Article 25
Representatives of controllers not established in the Union	Representatives of controllers not established in the Union	Representatives of controllers not established in the Union	Representatives of controllers not established in the Union
1. In the situation referred to in	1. In the situation referred to in	1. In the situation referred to in	1. Where Article 3(2) applies, the
Article 3(2), the controller shall	Article 3(2), the controller shall	Where Article 3(2) applies, the	controller or the processor shall
designate a representative in the	designate a representative in the	controller shall designate <i>inwriting</i>	designate in writing a representative
Union.	Union.	a representative in the Union.	in the Union.
2. This obligation shall not apply	2. This obligation shall not apply	2. This obligation shall not apply	2. This obligation shall not apply to:
to:	to:	to:	
(a) a controller established in a third	(a) a controller established in a third	deleted	

country where the Commission has decided that the third country ensures an adequate level of protection in accordance with Article 41; or  (b) an enterprise employing fewer than 250 persons; or	country where the Commission has decided that the third country ensures an adequate level of protection in accordance with Article 41; or  (b) an enterprise employing fewer than 250 personsa controller processing personal data which relates to less than 5000 data subjects during any consecutive 12-month period and not processing special categories of personal data as referred to in Article 9(1), location data or data on children or employees in large-scale filing systems; or	(b) an enterprise employing fewer than 250 persons processing which is occasional and unlikely to result in a risk for the rights and freedoms of individuals, taking into account the nature, context, scope and purposes of the processing; or	(b) processing which is occasional, does not include processing of special categories of data as referred to in Article 9(1) or processing of data relating to criminal convictions and offences referred to in Article 9a, or is unlikely to result in a risk for the rights and freedoms of individuals, taking into account the nature, context, scope and purposes of the processing; or
(c) a public authority or body; or	(c) a public authority or body; or	(c) a public authority or body; or	(c) a public authority or body; or
(d) a controller offering only occasionally goods or services to data subjects residing in the Union.	(d) a controller offering only occasionally offering goods or services to data subjects residing in the Union, unless the processing of personal data concerns special categories of personal data as referred to in Article 9(1), location data or data on children or employees in large-scale filing systems.	deleted	

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.	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 themthe data subjects, or whose behaviour is monitored, reside the monitoring of them, takes place.	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.	3. The representative shall be established in one of those Member States where the data subjects are and whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored.
		3a. The representative shall be mandated by the controller to be addressed in addition to or instead of the controller by, in particular, supervisory authorities and data subjects, on all issues related to the processing of personal data, for the purposes of ensuring compliance with this Regulation.	3a. The representative shall be mandated by the controller or the processor to be addressed in addition to or instead of the controller or the processor 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.	4. The designation of a representative by the controller shall be without prejudice to legal actions which could be initiated against the controller itself.	4. The designation of a representative by the controller shall be without prejudice to legal actions which could be initiated against the controller itself.	4. The designation of a representative by the controller or the processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.

Article 26	Article 26	Article 26	
Processor	Processor	Processor	
	Amendment 121		
1. Where a processing operation is	1. Where a processing operation is	1. Where a processing operation is	1. Where a processing is to be
to be carried out on behalf of a	to be carried out on behalf of a	to be carried out on behalf of a	carried out on behalf of a controller,
controller, the controller shall	controller, the controller shall	controller, the <i>The</i> controller shall	the controller shall use only
choose a processor providing	choose a processor providing	choose use only aprocessors	processors providing sufficient
sufficient guarantees to implement	sufficient guarantees to implement	providing sufficient guarantees to	guarantees to implement
appropriate technical and	appropriate technical and	implement appropriate technical	appropriate technical and
organisational measures and	organisational measures and	and organisational measures and	organisational measures in such a
procedures in such a way that the	procedures in such a way that the	<del>procedures</del> in such a way that the	way that the processing will meet
processing will meet the	processing will meet the	processing will meet the	the requirements of this Regulation
requirements of this Regulation and	requirements of this Regulation and	requirements of this Regulationand	and ensure the protection of the
ensure the protection of the rights	ensure the protection of the rights	ensure the protection of the rights	rights of the data subject.
of the data subject, in particular in	of the data subject, in particular in	of the data subject, in particular in	
respect of the technical security	respect of the technical security	respect of the technical security	
measures and organizational	measures and organisational	measures and organizational	
measures governing the processing	measures governing the processing	measures governing the processing	
to be carried out and shall ensure	to be carried out and shall ensure	to be carried out and shall ensure	
compliance with those measures.	compliance with those measures.	compliance with those measures.	

		1a. The processor shall not enlist	1a. The processor shall not enlist
		another processor without the	another processor without the prior
		prior specific or general written	specific or general written consent
		consent of the controller. In the	of the controller. In the latter case,
		latter case, the processor should	the processor should always inform
		always inform the controller on	the controller on any intended
		any intended changes concerning	changes concerning the addition or
		the addition or replacement of	replacement of other processors,
		other processors, thereby giving	thereby giving the opportunity to
		the opportunity to the controller to	the controller to object to such
		object to such changes.	changes.
2. The carrying out of processing	2. The carrying out of processing	2. The carrying out of processing	2. The carrying out of processing by
by a processor shall be governed by	by a processor shall be governed by	by a processor shall be governed by	a processor shall be governed by a
a contract or other legal act binding	a contract or other legal act binding	a contract or other a legal act under	contract or other legal act under
the processor to the controller and	the processor to the controller. <i>The</i>	Union or Member State law	Union or Member State law,
stipulating in particular that the	controller and the processor shall	binding the processor to the	binding the processor to the
processor shall:	be free to determine respective	controller, setting out the subject-	controller, setting out the subject-
	roles and tasks with respect to the	matter and duration of the	matter and duration of the
	requirements of this Regulation,	processing, the nature and purpose	processing, the nature and purpose
	and shall provide that and	of the processing, the type of	of the processing, the type of
	stipulating in particular that the	personal data and categories of	personal data and categories of data
	processor shall:	data subjects, the rights of binding	subjects, the obligations and rights
		the processor to the controller and	of the controller and stipulating in
		stipulating in particular that the	particular that the processor shall:
		processor shall:	

(a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;	(a) act process personal data only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited, unless otherwise required by Union law or Member State law;	(a) process the personal data act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing the data, unless that law prohibits such information on important grounds of public interest;	(a) process the personal data only on instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing the data, unless that law prohibits such information on important grounds of public interest;
(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;	(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;	deleted	(b) ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under a statutory obligation of confidentiality;
(c) take all required measures pursuant to Article 30;	(c) take all required measures pursuant to Article 30;	(c) take all <del>required</del> measures <b>required</b> pursuant to Article 30;	(c) take all measures required pursuant to Article 30;
(d) enlist another processor only with the prior permission of the controller;	(d) enlist determine the conditions for enlisting another processor only with the prior permission of the controller, unless otherwise determined;	(d) respect the conditions for enlisting another processor only with the prior permission such as a requirement of specific prior permission of the controller;	(d) respect the conditions referred to in paragraphs 1a and 2a for enlisting another processor;

	T	T	
(e) insofar as this is possible given	(e) insofar as this is possible given	(e) insofar as this is possible given	(e) taking into account the nature of
the nature of the processing, create	the nature of the processing, create	taking into account the nature of	the processing, assist the controller
in agreement with the controller the	in agreement with the controller the	the processing, assist create in	by appropriate technical and
necessary technical and	necessary appropriate and relevant	agreement with the controller the	organisational means, insofar as this
organisational requirements for the	technical and organisational	necessary technical and	is possible, for the fulfilment of the
fulfilment of the controller's	requirements for the fulfilment of	organisational requirements for the	controller's obligation to respond to
obligation to respond to requests for	the controller's obligation to	fulfilment of the controller's	requests for exercising the data
exercising the data subject's rights	respond to requests for exercising	obligation to in responding to	subject's rights laid down in
laid down in Chapter III;	the data subject's rights laid down	requests for exercising the data	Chapter III;
	in Chapter III;	subject's rights laid down in	
		Chapter III;	
(f) assist the controller in ensuring	(f) assist the controller in ensuring	(f) assist the controller in ensuring	(f) assist the controller in ensuring
compliance with the obligations	compliance with the obligations	compliance with the obligations	compliance with the obligations
pursuant to Articles 30 to 34;	pursuant to Articles 30 to 34,	pursuant to Articles 30 to 34;	pursuant to Articles 30 to 34 taking
	taking into account the nature of		into account the nature of
	processing and the information		processing and the information
	available to the processor;		available to the processor;
(g) hand over all results to the	(g) hand over return all results to	(g) hand over all results to return	(g) at the choice of the controller,
controller after the end of the	the controller after the end of the	or delete, at the choice of the	delete or return all the personal data
processing and not process the	processing, and not process the	controller after the end of the	to the controller after the end of the
	personal data otherwise <i>and delete</i>	<del>processing and not process</del> the	provision of data processing
	existing copies unless Union or	1 -	services, and delete existing copies
			unless Union or Member State law
	of the data;		requires storage of the data;
		in the contract or other legal act,	
		9	
		store the data under Union or	
		Member State law to which the	
1	1	1	1
(g) hand over all results to the controller after the end of the processing and not process the personal data otherwise;	(g) hand over return all results to the controller after the end of the processing, and not process the personal data otherwise and delete existing copies unless Union or Member State law requires storage	or delete, at the choice of the controller after the end of the processing and not process the personal data otherwise upon the termination of the provision of data processing services specified in the contract or other legal act, unless there is a requirement to store the data under Union or	(g) at the choice of the controller delete or return all the personal d to the controller after the end of t provision of data processing services, and delete existing copi

(h) make available to the controller	(h) make available to the controller	(h) make available to the controller	(h) make available to the controller
and the supervisory authority all	and the supervisory authority all	and the supervisory authority all	all information necessary to
information necessary to control	information necessary to control	information necessary to control	demonstrate compliance with the
compliance with the obligations	demonstrate compliance with the	demonstrate compliance with the	obligations laid down in this Article
laid down in this Article.	obligations laid down in this Article	obligations laid down in this Article	and allow for and contribute to
	and allow on-site inspections;	and allow for and contribute to	audits conducted by the controller.
		audits conducted by the controller.	The processor shall immediately
		The processor shall immediately	inform the controller if, in his
		inform the controller if, in his	opinion, an instruction breaches this
		opinion, an instruction breaches	Regulation or Union or Member
		this Regulation or Union or	State data protection provisions.
		Member State data protection	1
		provisions.	
		2a. Where a processor enlists	2a. Where a processor enlists
		another processor for carrying out	another processor for carrying out
		specific processing activities on	specific processing activities on
		behalf of the controller, the same	behalf of the controller, the same
		data protection obligations as set	data protection obligations as set
		out in the contract or other legal	out in the contract or other legal act
		act between the controller and the	between the controller and the
		processor as referred to in	processor as referred to in
		paragraph 2 shall be imposed on	paragraph 2 shall be imposed on
		that other processor by way of a	that other processor by way of a
		contract or other legal act under	contract or other legal act under
		Union or Member State law, in	Union or Member State law, in
		particular providing sufficient	particular providing sufficient
		guarantees to implement	guarantees to implement
		appropriate technical and	appropriate technical and
		organisational measures in such a	organisational measures in such a
		way that the processing will meet	way that the processing will meet
		the requirements of this	the requirements of this Regulation.
		Regulation. Where that other	Where that other processor fails to

processor fails to fulfil its data	fulfil its data protection obligations,
protection obligations, the initial	the initial processor shall remain
processor shall remain fully liable	fully liable to the controller for the
to the controller for the	performance of that other
performance of that other	processor's obligations.
processor's obligations.	
2aa. Adherence of the processor to	2aa. Adherence of the processor to
an approved code of conduct	an approved code of conduct
pursuant to Article 38 or an	pursuant to Article 38 or an
approved certification mechanism	approved certification mechanism
pursuant to Article 39 may be used	pursuant to Article 39 may be used
as an element to demonstrate	as an element to demonstrate
sufficient guarantees referred to in	sufficient guarantees referred to in
paragraphs 1 and 2a.	paragraphs 1 and 2a.
2ab. Without prejudice to an	2ab. Without prejudice to an
individual contract between the	individual contract between the
controller and the processor, the	controller and the processor, the
contract or the other legal act	contract or the other legal act
referred to in paragraphs 2 and 2a	referred to in paragraphs 2 and 2a
may be based, in whole or in part,	may be based, in whole or in part,
on standard contractual clauses	on standard contractual clauses
referred to in paragraphs 2b and	referred to in paragraphs 2b and 2c
2c or on standard contractual	or on standard contractual clauses
clauses which are part of a	which are part of a certification
	granted to the controller or
	processor pursuant to Articles 39
	and 39a.

		certification granted to the	
		controller or processor pursuant to	
		Articles 39 and 39a.	
		2b. The Commission may lay down	2b. The Commission may lay down
		standard contractual clauses for	standard contractual clauses for the
		the matters referred to in	matters referred to in paragraph 2
		paragraph 2 and 2a and in	and 2a and in accordance with the
		accordance with the examination	examination procedure referred to
			-
		procedure referred to in Article	in Article 87(2).
		87(2).	2 4
		2c. A supervisory authority may	2c. A supervisory authority may
		adopt standard contractual clauses	adopt standard contractual clauses
		for the matters referred to in	for the matters referred to in
		paragraph 2 and 2a and in	paragraph 2 and 2a and in
		accordance with the consistency	accordance with the consistency
		mechanism referred to in Article	mechanism referred to in Article
		57.	57.
3. The controller and the processor	3. The controller and the processor	3. The controller and the processor	3. The contract or the other legal act
shall document in writing the	shall document in writing the	shall document in writing the	referred to in paragraphs 2 and 2a,
controller's instructions and the	controller's instructions and the	controller's instructions and the	including instructions, shall be in
processor's obligations referred to	processor's obligations referred to	processor's obligations referred to	writing, including in an electronic
in paragraph 2.	in paragraph 2.	in paragraph 2 The contract or the	form.
m paragraph 2.	paragrapii 2.	other legal act referred to in	1011111
		paragraphs 2 and 2a shall be in	
		writing, including in an electronic	
		form.	

	3a. The sufficient guarantees		See §2aa
	referred to in paragraph 1 may be		Ü
	demonstrated by adherence to		
	codes of conduct or certification		
	mechanisms pursuant to Articles		
	38 or 39 of this Regulation.		
4. If a processor processes personal	4. If a processor processes personal	deleted	
data other than as instructed by the	data other than as instructed by the		
controller, the processor shall be	controller or becomes the		
considered to be a controller in	determining party in relation to the		
respect of that processing and shall	purposes and means of data		
be subject to the rules on joint	<i>processing</i> , the processor shall be		
controllers laid down in Article 24.	considered to be a controller in		
	respect of that processing and shall		
	be subject to the rules on joint		
	controllers laid down in Article 24.		
5. The Commission shall be	deleted	deleted	
empowered to adopt delegated acts			
in accordance with Article 86 for			
the purpose of further specifying			
the criteria and requirements for the			
responsibilities, duties and tasks in			
relation to a processor in line with			
paragraph 1, and conditions which			
allow facilitating the processing of			
personal data within a group of			
undertakings, in particular for the			
purposes of control and reporting.			

Article 27	Article 27	Article 27	Article 27
Processing under the authority of the controller and processor	Processing under the authority of the controller and processor	Processing under the authority of the controller and processor	Processing under the authority of the controller and processor
The processor and any person acting under the authority of the controller or of the processor who has access to personal data shall not process them except on instructions from the controller, unless required to do so by Union or Member State law.	The processor and any person acting under the authority of the controller or of the processor who has access to personal data shall not process them except on instructions from the controller, unless required to do so by Union or Member State law.	deleted	The processor and any person acting under the authority of the controller or of the processor who has access to personal data shall not process them except on instructions from the controller, unless required to do so by Union or Member State law.
Article 28	Article 28	Article 28	
Documentation	Documentation	Records of categories of personal data processing activities	Records of processing activities
	Amendment 122		
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 regularly updated documentation of all processing operations under its responsibility necessary to fulfill the requirements laid down in this Regulation.	1. Each controller and processor and, if any, the controller's representative, shall maintain a record documentation of all categories of personal data processing operations activities under its responsibility. The documentation This record shall contain at least the following information:	1. Each controller and, if any, the controller's representative, shall maintain a record of processing activities under its responsibility. This record shall contain the following information:

2. The documentation shall contain at least the following information:	2. The In addition, each controller and processor shall maintain documentation shall contain at least of the following information:	[Merged with 1. above and slightly modified]	
(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 controller, or any joint controller or processor, and of the representative, if any;	(a) the name and contact details of the controller, or and any joint controller or processor, and of the controller's representative and data protection officer, if any;	(a) the name and contact details of the controller and any joint controller, the controller's representative and the data protection officer, 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 officer, if any;	deleted	
(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);	deleted	(c) the purposes of the processing, including the legitimate interests pursued by the controller wherewhen the processing is based on point (f) of Article 6(1)(f);	(c) the purposes of the processing;
(d) a description of categories of data subjects and of the categories of personal data relating to them;	deleted	(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;
(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 recipients or categories of recipients of the personal data, including name and contact details of the controllers to whom personal data are disclosed for the legitimate interest pursued by them, if any;	(e) the recipients or categories of recipients of to whom the personal data, including the controllers to whom personal data are have been or will be disclosed for the legitimate interest pursued by them in particular recipients in third countries;	(e) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries;

(f) where applicable, transfers of	deleted	(f) where applicable, <i>the categories</i>	(f) where applicable, the categories
data to a third country or an		of transfers of personal data to a	of personal data transferred to third
international organisation,		third country or an international	country
including the identification of that		organisation <del>, including the</del>	•
third country or international		identification of that third country	
organisation and, in case of		or international organisation and, in	
transfers referred to in point (h) of		case of transfers referred to in point	
Article 44(1), the documentation of		(h) of Article 44(1), the	
appropriate safeguards;		documentation of appropriate	
		safeguards;	
(g) a general indication of the time	deleted	(g) where possible, the envisaged a	(g) where possible, the envisaged
limits for erasure of the different		general indication of the time limits	time limits for erasure of the
categories of data;		for erasure of the different	different categories of data;
		categories of data;	-
(h) the description of the	deleted	(h) where possible, a general	(h) where possible, a general
mechanisms referred to in Article		description of the technical and	description of the technical and
22(3).		organisational security measures	organisational security measures
		the description of the mechanisms	referred to in Article 30(1).
		referred to in Article $\frac{2230(31)}{3}$ .	
		2a. Each processor shall maintain	2a. Each processor and, if any, the
		a record of all categories of	processor's representative shall
		personal data processing activities	maintain a record of all categories
		carried out on behalf of a	of personal data processing
		controller, containing:	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;	(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 or the processor's representative, and the data protection officer, 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;	(c) the categories of processing carried out on behalf of each controller;
(d) where applicable, the categories of transfers of personal data to a third country or an international organisation;	(d) where applicable, the categories of transfers of personal data to a third country or an international organisation;
(e) where possible, a general description of the technical and organisational security measures referred to in Article 30(1).	(e) where possible, a general description of the technical and organisational security measures referred to in Article 30(1).
3a. The records referred to in paragraphs 1 and 2a shall be in writing, including in an electronic or other non-legible form which is	3a. The records referred to in paragraphs 1 and 2a shall be in writing, including in an electronic form.
capable of being converted into a legible form.	

3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority.	deleted	3. <i>On request</i> , Tthe controller and the processor and, if any, the controller's representative, shall make the documentation record available, on request, to the supervisory authority.	3. Upon request, the controller and the processor and, if any, the controller's or the processor's representative, shall make the record available to the supervisory authority.
4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers and processors:	deleted	4. The obligations referred to in paragraphs 1 and 2 <i>a</i> shall not apply to the following controllers and processors:	4. The obligations referred to in paragraphs 1 and 2a shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a high risk for the rights and freedoms of data subject.
(a) a natural person processing personal data without a commercial interest; or	deleted	(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.	deleted	(b) an enterprise or an organisation employing fewer than 250 persons that is unless the processing personal data only as an activity ancillary to its main activities it carries out is likely to result in a high risk for the rights and freedoms of data subject such as discrimination, identity theft or fraud, unauthorized reversal of pseudonymisation, financial loss, damage to the reputation, loss of confidentiality of data protected by professional secrecy or any other economic or social disadvantage	See §4 chapeau

		for the data subjects, taking into account the nature, scope, context and purposes of the processing.	
5. The Commission shall be	deleted	deleted	
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 responsibilities of the			
controller and the processor and, if any, the controller's representative.			
6. The Commission may lay down	deleted	deleted	
standard forms for the	ueieieu	ueieieu	
documentation referred to in			
paragraph 1. Those implementing			
acts shall be adopted in accordance			
with the examination procedure			
referred to in Article 87(2).			

Article 29	Article 29	Article 29	
Co-operation with the supervisory	Co-operation with the supervisory	Co-operation with the supervisory	
authority	authority	authority	
	Amendment 123		
1. The controller and the processor and, if any, the representative of the controller, shall co-operate, on request, with the supervisory authority in the performance of its duties, in particular by providing the information referred to in point (a) of Article 53(2) and by granting access as provided in point (b) of that paragraph.	1. The controller and, <i>if any</i> , the processor and, <i>if any</i> , the representative of the controller, shall co-operate, on request, with the supervisory authority in the performance of its duties, in particular by providing the information referred to in point (a) of Article 53(2) and by granting access as provided in point (b) of	deleted	1. The controller and the processor and, if any, the representative of the controller or the processor, shall cooperate, on request, with the supervisory authority in the performance of its tasks.
2. In response to the supervisory authority's exercise of its powers under Article 53(2), the controller and the processor shall reply to the supervisory authority within a reasonable period to be specified by the supervisory authority. The reply shall include a description of the measures taken and the results achieved, in response to the remarks of the supervisory authority.	that paragraph.  2. In response to the supervisory authority's exercise of its powers under Article 53(2), the controller and the processor shall reply to the supervisory authority within a reasonable period to be specified by the supervisory authority. The reply shall include a description of the measures taken and the results achieved, in response to the remarks of the supervisory authority.	deleted	

SECTION 2 DATA SECURITY	SECTION 2 DATA SECURITY	SECTION 2 DATA SECURITY	
Article 30	Article 30	Article 30	
Security of processing	Security of processing	Security of processing	
	Amendment 124		
1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation.	1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, taking into account the results of a data protection impact assessment pursuant to Article 33, having regard to the state of the art and the costs of their implementation.	1. Having regard to available technology and the costs of implementation and taking into account the nature, scope, context and purposes of the processing as well as the likelihood and severity of the risk for the rights and freedoms of individuals, #the controller and the processor shall implement appropriate technical and organisational measures, such as pseudonymisation of personal data to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation.	1. Having regard to the state of the art and the costs of implementation and taking into account the nature, scope, context and purposes of the processing as well as the likelihood and severity of the risk for the rights and freedoms of individuals, the controller and the processor shall implement appropriate technical and organisational measures, such as pseudonymisation of personal data, to ensure a level of security appropriate to the risk.

Ia. Having regard to the state of the art and the cost of implementation, such a security policy shall include:	1a. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by data processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data	1a. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by data processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data
	transmitted, stored or otherwise processed.	transmitted, stored or otherwise processed.
(a) the ability to ensure that the integrity of the personal data is validated;		
(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data;		
(c) the ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident that impacts the availability, integrity and confidentiality of information systems and services;		

	•	•	
	(d) in the case of sensitive personal		
	data processing according to		
	Articles 8 and 9, additional		
	security measures to ensure		
	situational awareness of risks and		
	the ability to take preventive,		
	corrective and mitigating action in		
	near real time against		
	vulnerabilities or incidents		
	detected that could pose a risk to		
	the data;		
	<i>'</i>		
	(e) a process for regularly testing,		
	assessing and evaluating the		
	effectiveness of security policies,		
	procedures and plans put in place		
	to ensure ongoing effectiveness.		
2. The controller and the processor	2. The controller and the processor	deleted	
shall, following an evaluation of the	shall, following an evaluation of the		
risks, take the measures referred to	risks, take the measures referred to		
in paragraph 1 to protect personal	in paragraph 1 to protect personal		
data against accidental or unlawful	data against accidental or unlawful		
destruction or accidental loss and to	destruction or accidental loss and to		
prevent any unlawful forms of	prevent any unlawful forms of		
processing, in particular any	processing, in particular any		
unauthorised disclosure,	unauthorised disclosure,		
dissemination or access, or	dissemination or access, or		
alteration of personal data.	alteration of personal data. shall at		
	least:		

(a) ensure that personal data can be accessed only by authorised personnel for legally authorised purposes;		
	2a. Adherence to approved codes of conduct pursuant to Article 38 or an approved certification mechanism pursuant to Article 39 may be used as an element to demonstrate compliance with the requirements set out in paragraph 1.	2a. Adherence to an approved code of conduct pursuant to Article 38 or an approved certification mechanism pursuant to Article 39 may be used as an element to demonstrate compliance with the requirements set out in paragraph 1.
(b) protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure; and		
	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.	

	(c) ensure the implementation of a		
	security policy with respect to the		
	processing of personal data.		
3. The Commission shall be	3. The Commission European Data	deleted	
empowered to adopt delegated acts	<b>Protection Board</b> shall be		
in accordance with Article 86 for	empowered to adopt delegated acts		
the purpose of further specifying	in accordance with Article 86 for		
the criteria and conditions for the	the purpose of further specifying		
technical and organisational	the criteria and conditions		
measures referred to in paragraphs	entrusted with the task of issuing		
1 and 2, including the	guidelines, recommendations and		
determinations of what constitutes	best practices in accordance with		
the state of the art, for specific	point (b) of Article 66(1) for the		
sectors and in specific data	technical and organisational		
processing situations, in particular	measures referred to in paragraphs		
taking account of developments in	1 and 2, including the		
technology and solutions for	determinations of what constitutes		
privacy by design and data	the state of the art, for specific		
protection by default, unless	sectors and in specific data		
paragraph 4 applies.	processing situations, in particular		
	taking account of developments in		
	technology and solutions for		
	privacy by design and data		
	protection by default <del>, unless</del>		
	<del>paragraph 4 applies</del> .		

4. The Commission may adopt, where necessary, implementing acts for specifying the requirements laid down in paragraphs 1 and 2 to various situations, in particular to:	deleted	deleted	
(a) prevent any unauthorised access to personal data;	deleted	deleted	
(b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data;	deleted	deleted	
(c) ensure the verification of the lawfulness of processing operations.	deleted	deleted	
Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	deleted	deleted	

Article 31	Article 31	Article 31	
Notification of a personal data	Notification of a personal data	Notification of a personal data	
breach to the supervisory authority	breach to the supervisory authority	breach to the supervisory authority	
	Amendment 125		
1. In the case of a personal data	1. In the case of a personal data	1. In the case of a personal data	1. In the case of a personal data
breach, the controller shall without	breach, the controller shall without	breach which is likely to result in a	breach which is likely to result in a
undue delay and, where feasible,	undue delay <del>and, where feasible,</del>	high risk for the rights and	risk for the rights and freedoms of
not later than 24 hours after having	not later than 24 hours after having	freedoms of individuals, such as	individuals, the controller shall
become aware of it, notify the	become aware of it, notify the	discrimination, identity theft or	without undue delay and, where
personal data breach to the	personal data breach to the	fraud, financial loss, unauthorized	feasible, not later than 72 hours
supervisory authority. The	supervisory authority. The	reversal of pseudonymisation,	after having become aware of it,
notification to the supervisory	notification to the supervisory	damage to the reputation, loss of	notify the personal data breach to
authority shall be accompanied by a	authority shall be accompanied by a	confidentiality of data protected by	the supervisory authority competent
reasoned justification in cases	reasoned justification in cases	professional secrecy or any other	in accordance with Article 51. The
where it is not made within 24	where it is not made within 24	significant economic or social	notification to the supervisory
hours.	hours.	disadvantage, the controller shall	authority shall be accompanied by a
		without undue delay and, where	reasoned justification in cases
		feasible, not later than 24-72 hours	where it is not made within 72
		after having become aware of it,	hours.
		notify the personal data breach to	
		the supervisory authority <i>competent</i>	
		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 24-72	
		hours.	

2. Pursuant to point (f) of Article 26(2), the processor shall alert and	2. Pursuant to point (f) of Article 26(2), the <i>The</i> processor shall alert	1a. The notification referred to in paragraph 1 shall not be required if a communication to the data subject is not required under Article 32(3)(a) and (b).  2. Pursuant to point (f) of Article 26(2), † The processor shall	2. The processor shall notify the controller without undue delay after
inform the controller immediately after the establishment of a personal	and inform the controller immediately without undue delay	alertnotify and inform the controller immediately after the establishment	becoming aware of a personal data breach.
data breach.	after the establishment of a personal data breach.	without undue delay after becoming award of a personal data breach.	
3. The notification referred to in paragraph 1 must at least:	3. The notification referred to in paragraph 1 must at least:	3. The notification referred to in paragraph 1 must at least:	3. The notification referred to in paragraph 1 must at least:
(a) describe the nature of the personal data breach including the	(a) describe the nature of the personal data breach including the	(a) describe the nature of the personal data breach including	(a) describe the nature of the personal data breach including
categories and number of data subjects concerned and the	categories and number of data subjects concerned and the	where possible and appropriate, the approximate categories and	where possible, the categories and approximate number of data
categories and number of data records concerned;	categories and number of data records concerned;	number of data subjects concerned and the categories and <i>approximate</i> number of data records concerned;	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	(b) communicate the identity and contact details of the data protection officer or other contact point where more information can	(b) communicate the identity and contact details of the data protection officer or other contact point where more information can	(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
be obtained;	be obtained;	be obtained;	

(c) recommend measures to	(c) recommend measures to	deleted	
mitigate the possible adverse effects	mitigate the possible adverse effects		
of the personal data breach;	of the personal data breach;		
(d) describe the consequences of	(d) describe the consequences of	(d) describe the <i>likely</i> consequences	(d) describe the likely consequences
the personal data breach;	the personal data breach;	of the personal data breach	of the personal data breach;
		identified by the controller;	_
(e) describe the measures proposed	(e) describe the measures proposed	(e) describe the measures <i>taken or</i>	(e) describe the measures taken or
or taken by the controller to address	or taken by the controller to address	proposed or-to be taken by the	proposed to be taken by the
the personal data breach.	the personal data breach <i>and/or</i>	controller to address the personal	controller to address the personal
	mitigate its effects.	data breach.; and	data breach and/or to mitigate its
	The information may if necessary		possible adverse effects.
	be provided in phases.		
		(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	3a. Where, and in so far as, it is not
		not possible to provide the	possible to provide the information
		information referred to in	at the same time, the information
		paragraph 3 (d), (e) and (f) at the	may be provided in phases without
		same time as the information	undue further delay.
		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	4. The controller shall document	4. The controller shall document	4. The controller shall document
any personal data breaches,	any personal data breaches,	any personal data breaches <i>referred</i>	any personal data breaches referred
comprising the facts surrounding	comprising the facts surrounding	to in paragraphs 1 and 2,	to in paragraphs 1 and 2,
the breach, its effects and the	the breach, its effects and the	comprising the facts surrounding	comprising the facts surrounding
remedial action taken. This	remedial action taken. This	the breach, its effects and the	the breach, its effects and the
documentation must enable the	documentation must <i>be sufficient</i>	remedial action taken. This	remedial action taken. This
supervisory authority to verify	to enable the supervisory authority	documentation must enable the	documentation must enable the
compliance with this Article. The	to verify compliance with this	supervisory authority to verify	supervisory authority to verify
documentation shall only include	Article <i>and with Article 30</i> . The	compliance with this Article. The	compliance with this Article.
the information necessary for that	documentation shall only include	documentation shall only include	
purpose.	the information necessary for that	the information necessary for that	
	purpose.	<del>purpose.</del>	
	4a. The supervisory authority shall		
	keep a public register of the types		
	of breaches notified.		
5. The Commission shall be	5. The Commission European Data	deleted	
empowered to adopt delegated acts	<b>Protection Board</b> shall be		
in accordance with Article 86 for	empowered to adopt delegated acts		
the purpose of further specifying	in accordance with Article 86 for		
the criteria and requirements for	the purpose entrusted with the task		
establishing the data breach referred	of further specifying the criteria and		
to in paragraphs 1 and 2 and for the	requirements issuing guidelines,		
particular circumstances in which a	recommendations and best		
controller and a processor is	practices in accordance with point		
required to notify the personal data	(b) of Article 66(1) for establishing		
breach.	the data breach and determining		
	the undue delay referred to in		
	paragraphs 1 and 2 and for the		

	particular circumstances in which a controller and a processor isare required to notify the personal data breach.		
6. The Commission may lay down	deleted	deleted	
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).			

Article 32	Article 32	Article 32	
Communication of a personal data	Communication of a personal data	Communication of a personal data	
breach to the data subject	breach to the data subject	breach to the data subject	
	Amendment 126		
1. When the personal data breach is	1. When the personal data breach is	1. When the personal data breach is	1. When the personal data breach is
likely to adversely affect the	likely to adversely affect the	likely to <del>adversely affect the</del>	likely to to result in a high risk for
protection of the personal data or	protection of the personal data, <i>the</i>	protection of the personal data or	the rights and freedoms of
privacy of the data subject, the	or-privacy, the rights or the	privacy of the data subject result in	individuals, the controller shall
controller shall, after the	<i>legitimate interests</i> of the data	a high risk for the rights and	communicate the personal data
notification referred to in Article	subject, the controller shall, after	freedoms of individuals, such as	breach to the data subject without
31, communicate the personal data	the notification referred to in	discrimination, identity theft or	undue delay.
breach to the data subject without	Article 31, communicate the	fraud, financial loss, damage to	
undue delay.	personal data breach to the data	the reputation, unauthorized	
	subject without undue delay.	reversal of pseudonymisation, loss	
		of confidentiality of data protected	
		by professional secrecy or any	
		other significant economic or	
		social disadvantage, the controller	
		shall <del>, after the notification referred</del>	
		to in Article 31, communicate the	
		personal data breach to the data	
		subject without undue delay.	

- 2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b) and (c) of Article 31(3).
- 2. The communication to the data subject referred to in paragraph 1 shall be comprehensive and use clear and plain language. It shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b) and, (c) and (d) of Article 31(3) and information about the rights of the data subject, including redress.
- 2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b), (e) and (ef) of Article 31(3).
- 2. The communication to the data subject referred to in paragraph 1 shall describe in clear and plain language the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b), (d) and (e) of Article 31(3).

- 3. The communication of a personal data breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.
- 3. The communication of a personal data breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.
- 3. The communication of a personal data breach to the data subject *referred to in paragraph 1* shall not be required if:
- a. the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological and organisational protection measures, and that those measures were applied to the data concernedaffected by the personal data breach, in particular those that .Such technological protection measures shall 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
- 3. The communication to the data subject referred to in paragraph 1 shall not be required if: a. the controller has implemented appropriate technological and organisational measures, and that those measures were applied to the data affected by the personal data breach, in particular those that render the data unintelligible to any person who is not authorised to access it, such as encryption; or b. the controller has taken subsequent measures which ensure that the high risk for the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise: or c. it would involve disproportionate effort, in particular owing to the

95

		ensure that the high risk for the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise; or c. it would involve disproportionate effort, in particular owing to the number of cases involved. In such case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner; or d. it would adversely affect a substantial public interest.	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 determined in Union or Member State law.
4. Without prejudice to the controller's obligation to communicate the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject of the personal data breach, the supervisory authority, having considered the likely adverse effects of the breach, may require it to do so.	4. Without prejudice to the controller's obligation to communicate the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject of the personal data breach, the supervisory authority, having considered the likely adverse effects of the breach, may require it to do so.	deleted	If the controller has not already communicated the personal data breach to the data subject of the personal data breach, the supervisory authority, having considered the likely adverse effects of the breach, may require it to do so.

5. The Commission shall be	5. The Commission-European Data	deleted	
empowered to adopt delegated acts	Protection Board shall be		
in accordance with Article 86 for	empowered to adopt delegated acts		
the purpose of further specifying	in accordance with Article 86 for		
the criteria and requirements as to	the purpose entrusted with the task		
the circumstances in which a	of further specifying the criteria and		
personal data breach is likely to	requirements issuing guidelines,		
adversely affect the personal data	recommendations and best		
referred to in paragraph 1.	practices in accordance with point		
	(b) of Article 66(1) as to the		
	circumstances in which a personal		
	data breach is likely to adversely		
	affect the personal data, the		
	privacy, the rights or the legitimate		
	interests of the data subject		
	referred to in paragraph 1.		
6. The Commission may lay down	deleted	deleted	
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).			

Amendment 127	
Article 32a	
Respect to Risk	
1. The controller, or where applicable the processor, shall carry out a risk analysis of the potential impact of the intended data processing on the rights and freedoms of the data subjects, assessing whether its processing operations are likely to present specific risks.	
2. The following processing operations are likely to present specific risks:	
(a) processing of personal data relating to more than 5000 data subjects during any consecutive 12-month period;	
(b) processing of special categorie of personal data as referred to in Article 9(1), location data or data on children or employees in large scale filing systems;	

(c) profiling on which measures are based that produce legal effects concerning the individual or similarly significantly affect the individual;	
(d) processing of personal data 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;	
(e) automated monitoring of publicly accessible areas on a large scale;	
(f) other processing operations for which the consultation of the data protection officer or supervisory	
authority is required pursuant to point (b) of Article 34(2); (g) where a personal data breach	
would likely adversely affect the protection of the personal data, the privacy, the rights or the legitimate	
interests of the data subject;	

(h) 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;	
(i) where personal data are made accessible to a number of persons which cannot reasonably be expected to be limited.  3. According to the result of the	
risk analysis:  (a) where any of the processing operations referred to in points (a) or (b) of paragraph 2 exist, controllers not established in the	
Union shall designate a representative in the Union in line with the requirements and exemptions laid down in Article 25;	

(b) where any of the processing	
operations referred to in points (a),	
(b) or (h)of paragraph 2 exist, the	
controller shall designate a data	
protection officer in line with the	
requirements and exemptions laid	
down in Article 35;	
(c) where any of the processing	
operations referred to in points (a),	
(b), (c), (d), (e), (f), (g) or (h) of	
paragraph 2 exist, the controller or	
the processor acting on the	
controller's behalf shall carry out	
a data protection impact	
assessment pursuant to Article 33;	
(d) where processing operations	
referred to in point (f) of	
paragraph 2 exist, the controller	
shall consult the data protection	
officer, or in case a data protection	
officer has not been appointed, the	
supervisory authority pursuant to	
Article 34.	

4. The risk analysis shall be	
reviewed at the latest after one	
year, or immediately, if the nature,	
the scope or the purposes of the	
data processing operations change	
significantly. Where pursuant to	
point (c) of paragraph 3 the	
controller is not obliged to carry	
out a data protection impact	
assessment, the risk analysis shall	
be documented.	

	Amendment 128		
SECTION 3	SECTION 3	SECTION 3	
DATA PROTECTION	LIFECYCLE DATA	DATA PROTECTION	
IMPACT ASSESSMENT	PROTECTION	IMPACT ASSESSMENT	
AND PRIOR	MANAGEMENT	AND PRIOR	
AUTHORISATION		AUTHORISATION	
Article 33	Article 33	Article 33	
Data protection impact assessment	Data protection impact assessment	Data protection impact assessment	
1. Where processing operations	1. Where <del>processing operations</del>	1. Where <i>a type of</i> processing <i>in</i>	1. Where a type of processing in
present specific risks to the rights	present specific risks to the rights	particular using new technologies,	particular using new technologies,
and freedoms of data subjects by	and freedoms of data subjects by	and taking into account operations	and taking into account the nature,
virtue of their nature, their scope or	virtue of their nature, their scope or	present specific risks to the rights	scope, context and purposes of the
their purposes, the controller or the	their purposes, required pursuant	and freedoms of data subjects by	processing, is likely to result in a
processor acting on the controller's	to point (c) of Article 32a(3) the	virtue of their the nature, their	high risk for the rights and
behalf shall carry out an assessment	controller or the processor acting on	scope, context and or their	freedoms of individuals, the
of the impact of the envisaged	the controller's behalf shall carry	purposes of the processing, is likely	controller shall, prior to the
processing operations on the	out an assessment of the impact of	to result in a high risk for the	processing, carry out an assessment
protection of personal data.	the envisaged processing operations	rights and freedoms of individuals,	of the impact of the envisaged
	on the <i>rights and freedoms of the</i>	such as discrimination, identity	processing operations on the
	data subjects, especially their right	theft or fraud, financial loss,	protection of personal data. A
	to protection of personal data. A	damage to the reputation,	single assessment may address a set
	single assessment shall be	unauthorised reversal of	of similar processing operations
	sufficient to address a set of	pseudonymisation, loss of	that present similar high risks.
	similar processing operations that	confidentiality of data protected by	
	present similar risks.	professional secrecy or any other	

		significant economic or social disadvantage, the controller or the processor acting on the controller's behalf shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.  1a. The controller shall seek the advice of the data protection	1a. The controller shall seek the advice of the data protection
		officer, where designated, when carrying out a data protection impact assessment.	officer, where designated, when carrying out a data protection impact assessment.
2. The following processing operations in particular present specific risks referred to in paragraph 1:	deleted	2. The following processing operations in particular present specific risks A data protection impact assessment referred to in paragraph 1 shall in particular be required in the following cases:	2. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the following cases:
(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	deleted	(a) a systematic and extensive evaluation of personal aspects relating to a-natural persons 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 which is	(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling and on which decisions are based that produce legal effects concerning the individual or significantly affect the individual;

		hand on machine and on within	
measures are based that produce		based on profiling and on which	
legal effects concerning the		measures decisions are based that	
individual or significantly affect the		produce legal effects concerning the	
individual;		individual data subjects or	
		significantly severely affect the	
		individualdata subjects;	
(b) information on sex life, health,	deleted	(b) information on sex life, health,	(b) processing on a large scale of
race and ethnic origin or for the		race and ethnic origin or for the	special categories of personal data
provision of health care,		provision of health care,	referred to in Article 9(1), of data
epidemiological researches, or		epidemiological researches, or	relating to criminal convictions and
surveys of mental or infectious		surveys of mental or infectious	offences referred to Article 9a, and
diseases, where the data are		diseases processing of special	of biometric data;
processed for taking measures or		categories of personal data under	
decisions regarding specific		Article 9(1), biometric data or data	
individuals on a large scale;		on criminal convictions and	
		offences or related security	
		<i>measures</i> , where the data are	
		processed for taking measures or	
		decisions regarding specific	
		individuals on a large scale;	
(c) monitoring publicly accessible	deleted	(c) monitoring publicly accessible	(c) a sytematic monitoring of a
areas, especially when using optic-		areas on a large scale, especially	publicly accessible area on a large
electronic devices (video		when using optic-electronic devices	scale
surveillance) on a large scale;		(video surveillance) on a large	
Sai ventance) on a large scale,		scale:	
(d) personal data in large scale	deleted	deleted	
filing systems on children, genetic	ucicicu	ucicicu	
1			
data or biometric data;			

(e) other processing operations for	deleted	deleted	
which the consultation of the			
supervisory authority is required			
pursuant to point (b) of Article			
34(2).			
		2a. The supervisory authority shall	2a. The supervisory authority shall
		establish and make public a list of	establish and make public a list of
		the kind of processing operations	the kind of processing operations
		which are subject to the	which are subject to the
		requirement for a data protection	requirement for a data protection
		impact assessment pursuant to	impact assessment pursuant to
		paragraph 1. The supervisory	paragraph 1. The supervisory
		authority shall communicate those	authority shall communicate those
		lists to the European Data	lists to the European Data
		Protection Board.	Protection Board
		2b. The supervisory authority may	2b. The supervisory authority may
		also establish and make public a	also establish and make public a
		list of the kind of processing	list of the kind of processing
		operations for which no data	operations for which no data
		protection impact assessment is	protection impact assessment is
		required. The supervisory	required. The supervisory
		authority shall communicate those	authority shall communicate those
		lists to the European Data	lists to the European Data
		Protection Board.	Protection Board.

2c. Prior to the adoption of the 2c. Prior to the adoption of the lists lists referred to in paragraphs 2a referred to in paragraphs 2a and and 2b the competent supervisory 2b the competent supervisory authority shall apply the authority shall apply the consistency mechanism referred to consistency mechanism referred to in Article 57 where such lists in Article 57 where such lists involve processing activities which involve processing activities which are related to the offering of goods are related to the offering of goods or services to data subjects or to or services to data subjects or to the monitoring of their behaviour the monitoring of their behaviour in several Member States, or may in several Member States, or may substantially affect the free substantially affect the free movement of personal data within movement of personal data within the Union. the Union. 3. The assessment shall contain at 3. The assessment shall contain at 3. The assessment shall *have regard* 3. The assessment shall contain at to the entire lifecycle management least a general description of the least a general description of the least: envisaged processing operations, an of personal data from collection to envisaged processing operations, an processing to deletion. It shall assessment of the risks to the rights assessment evaluation of the risks contain at least a general description to the rights and freedoms of data and freedoms of data subjects, the of the envisaged processing measures envisaged to address the subjects referred to in paragraph operations, an assessment of the risks risks, safeguards, security measures 1, the measures envisaged to to the rights and freedoms of data and mechanisms to ensure the address the risks, including subjects, the measures envisaged to safeguards, security measures and protection of personal data and to address the risks, safeguards, security mechanisms to ensure the demonstrate compliance with this measures and mechanisms to ensure Regulation, taking into account the protection of personal data and to the protection of personal data and to rights and legitimate interests of demonstrate compliance with this demonstrate compliance with this data subjects and other persons Regulation, taking into account the Regulation, taking into account the rights and legitimate interests of concerned. rights and legitimate interests of data data subjects and other persons subjects and other persons concerned. concerned:

(a) a quat	or of the	(a) a compand decomination of the
(a) a systematic description	•	(a) a general description of the
envisaged processing ope	-	envisaged processing operations;
the purposes of the proce		
and, if applicable, the leg		
interests pursued by the c	controller;	
(b) an assessment of the i	necessity	(b) an assessment of the necessity
and proportionality of the	e	and proportionality of the
processing operations in	relation	processing operations in relation to
to the purposes;		the purposes;
(c) an assessment of the i	risks to	(c) an assessment evaluation of the
the rights and freedoms of	of data	risks to the rights and freedoms of
subjects, including the ris	sk of	data subjects referred to in
discrimination being emb	bedded in	paragraph 1
or reinforced by the oper	ration;	
(d) a description of the m	easures	(d) the measures envisaged to
envisaged to address the	risks and	address the risk including
minimise the volume of p	personal	safeguards, security measures and
data which is processed;		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.

(e) a list of safeguards, security measures and mechanisms to ensure the protection of personal data, such as pseudonymisation, and to demonstrate compliance with this Regulation, taking into account the rights and legitimate	
interests of data subjects and other persons concerned;	

•	dication of the time ure of the different ata;
protection by a	tion which data lesign and default uant to Article 23 lemented;
(h) a list of the categories of repersonal data;	recipients or ecipients of the
intended trans third country of organisation, i identification of	of that third country
in case of tran- point (h) of Ar documentation safeguards;	of appropriate
(j) an assessme the data proces	ent of the context of ssing.
	designated a data cer, he or she shall the impact

3b. The assessment shall be documented and lay down a schedule for regular periodic data protection compliance reviews pursuant to Article 33a(1). The assessment shall be updated without undue delay, if the results of the data protection compliance review referred to in Article 33a show compliance inconsistencies. The controller and the processor and, if any, the controller's representative shall make the assessment available, on request, to the supervisory authority.		
	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.	3a. Compliance with approved codes of conduct referred to in Article 38 by the relevant controllers or processors shall be taken into due account in assessing lawfulness and impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.

4. The controller shall 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.	deleted	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. Where appropriate, 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.	deleted	5. Where the controller is a public authority or body and where the processing results from a legal obligation pursuant to point (c) or (e) of Article 6(1) providing for rules and procedures pertaining to the processing operations and regulated by has a legal basis in Union law, paragraphs 1 to 4 shall not apply, unless or the law of the Member States 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.	5. Where the processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or the law of the Member State to which the controller is subject, and such law regulates the specific processing operation or set of operations in question and an assessment has already been made in the context of the adoption of this legal basis, paragraphs 1 to 3 shall not apply.

6. The Commission shall be	deleted	deleted	
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	deleted	deleted	
standards and procedures for			
carrying out and verifying and			
auditing the assessment referred to			
in paragraph 3. Those			
implementing acts shall be adopted			
in accordance with the examination			
procedure referred to in Article			
87(2).			

	Amendment 130	
	Article 33 a (new)	
D	Oata protection compliance review	
	At the latest two years after the	
ca	arrying out of an impact	
as	ssessment pursuant to Article	
33	3(1), the controller or the	
	rocessor acting on the	
	ontroller's behalf shall carry out	
	compliance review. This	
	ompliance review shall	
	emonstrate that the processing of	
	ersonal data is performed in	
	ompliance with the data	
pi	rotection impact assessment.	
	The compliance review shall be	
	arried out periodically at least	
	nce every two years, or	
	nmediately when there is a	
	hange in the specific risks	
-	resented by the processing	
op	verations.	

2 1171 .1 1	
3. Where the compliance review	
results show compliance	
inconsistencies, the compliance	
review shall include	
recommendations on how to	
achieve full compliance.	
4. The compliance review and its	
recommendations shall be	
documented. The controller and	
the processor and, if any, the	
controller's representative shall	
make the compliance review	
available, on request, to the	
supervisory authority.	
5. If the controller or the processor	
has designated a data protection	
officer, he or she shall be involved	
in the compliance review	
proceeding.	

Article 34	Article 34	Article 34	
	Amendment 131		
Prior authorisation and prior consultation	Prior consultation	Prior <del>authorisation and prior</del> consultation	Prior consultation
1. The controller or the processor as	deleted	deleted	deleted
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.			

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 <i>data protection officer</i> , <i>or in case a data protection officer has not been appointed, the</i> 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 where a data protection impact assessment as provided for in Article 33 indicates that the in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the would result in a high risks involved for the data subjects where:in the absence of measures to be taken by the controller to mitigate the risk.	2. The controller shall consult the supervisory authority prior to the processing of personal data where a data protection impact assessment as provided for in Article 33 indicates that the processing would result in a high risk in the absence of measures to be taken by the controller to mitigate the risk.
(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 processing operations are by virtue of their nature, their scope or their purposes, likely to present a high degree of specific risks; or	deleted	See §2

- (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 data protection officer or 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.

## deleted

- 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 *competent* supervisory authority is of the opinion *determines in accordance* with its power 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 non-compliance.
- 3. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 2 would does not comply with this Regulation, in particular where the controller has risks are insufficiently identified or mitigated the risk, it shall prohibit the intended processing and make appropriate proposals to remedy such incompliance within a maximum period of 6 weeks following the request for consultation give advice to the data controller, in writing, and may use any of its powers referred to in Article 53. This period may be extended for a further six weeks, taking into account the complexity
- 3. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 2 would not comply with this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, it shall within a maximum period of 6 weeks following the request for consultation give advice to the data controller, in writing, and may use any of its powers referred to in Article 53. 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.

118

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  European Data Protection Board 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.	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.  deleted	
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.	deleted	deleted	

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, on request, with the data protection impact assessment provided for in pursuant to 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. When consulting the supervisory authority pursuant to paragraph2, The controller of processor 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 subjects pursuant to this Regulation;
- (d) where applicable, the contact details of the data protection officer;
- (e) the data protection impact assessment provided for in Article 33; and

- 6. When consulting the supervisory authority pursuant to paragraph2, 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;
- (d) where applicable, the contact details of the data protection officer;
- (e) the data protection impact assessment provided for in Article 33; and
- (f) any other information requested by the supervisory authority.

7. Member States shall consult the	7. Member States shall consult the	(f), on request, with any other information to allow requested by 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	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.	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.	supervisory authority in-during the preparation of a proposal for a legislative measure to be adopted by thea national parliament or of a regulatory measure based on such a legislative measure, which defines the nature of the processing, in order to ensure the compliance of the intended provide for the processing with this Regulation and in particular to mitigate the risks	supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament or of a regulatory measure based on such a legislative measure, which relates to the processing of personal data.
		involved for the data subjects of personal data.	

		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.	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.
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.	deleted	deleted	

9. The Commission may set out	deleted	deleted	
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).			

SECTION 4 DATA PROTECTION OFFICER Article 35 Designation of the data protection officer	SECTION 4 DATA PROTECTION OFFICER Article 35 Designation of the data protection officer	SECTION 4 DATA PROTECTION OFFICER Article 35 Designation of the data protection officer	
1. The controller and the processor shall designate a data protection officer in any case where:	Amendment 132  1. The controller and the processor shall designate a data protection officer in any case where:	1. The controller and or the processor may, or where required by Union or Member State law shall designate a data protection officer in any case where:	1. The controller or the processor may, or where required by Union or Member State law shall designate a data protection officer.
(a) the processing is carried out by a public authority or body; or (b) the processing is carried out by an enterprise employing 250 persons or more; or	(a) the processing is carried out by a public authority or body; or (b) the processing is carried out by an enterprise employing 250 persons or more a legal person and relates to more than 5000 data subjects in any consecutive 12-month period; or	deleted	

(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; or	deleted	
	(d) the core activities of the controller or the processor consist of processing special categories of data pursuant to Article 9(1), location data or data on children or employees in large scale filing systems.		See (c)
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 A group of undertakings may appoint a single main responsible data protection officer, provided it is ensured that a data protection officer is easily accessible from each establishment.	2. In the case referred to in point (b) of paragraph 1, a A group of undertakings may appoint a single data protection officer.	2. A group of undertakings may appoint a single data protection officer.

3. Where the controller or the	3. Where the controller or the	3. Where the controller or the	
processor is a public authority or	processor is a public authority or	processor is a public authority or	
body, the data protection officer	body, the data protection officer	body, the a single data protection	
may be designated for several of its	may be designated for several of its	officer may be designated for	
entities, taking account of the	entities, taking account of the	several-of its entities such	
organisational structure of the	organisational structure of the	authorities or bodies, taking	
public authority or body.	public authority or body.	account of the ir organisational	
		structure of the public authority or	
		body and size.	
4. In cases other than those referred	4. In cases other than those referred	deleted	
to in paragraph 1, the controller or	to in paragraph 1, the controller or		
processor or associations and other	processor or associations and other		
bodies representing categories of	bodies representing categories of		
controllers or processors may	controllers or processors may		
designate a data protection officer.	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 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.

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

- 6. 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 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.	7. The controller or the processor shall designate a data protection officer for a period of at least two four years in case of an employee or two years in case of an external service contractor. The data protection officer may be reappointed for further terms. During their his or her term of office, the data protection officer may only be dismissed, if the data protection officer he or she no longer fulfils the conditions required for the performance of their his or her duties.	7. The controller or the processor shall designate a During their term of office, the data protection officer for a period of at least two years. 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 reappointed for further terms. During their term of office, the data protection officer may only be dismissed; only if the data protection officer no longer fulfils the conditions required for the performance of their duties his or her tasks pursuant to Article 37.	
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.	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.	8. The data protection officer may be employed by a staff member of the controller or processor, or fulfil his or her the tasks on the basis of a service contract.	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	9. The controller or the processor	9. The controller or the processor	9. The controller or the processor
shall communicate the name and	shall communicate the name and	shall <del>communicate</del> <i>publish</i> the	shall publish the contact details of
contact details of the data	contact details of the data protection	name and contact details of the data	the data protection officer and
protection officer to the supervisory	officer to the supervisory authority	protection officer and	communicate these to the
authority and to the public.	and to the public.	communicate these to the	supervisory authority.
		supervisory authority and to the	
		<del>public</del> .	
10. Data subjects shall have the	10. Data subjects shall have the	10. Data subjects shall have the	
right to contact the data protection	right to contact the data protection	right to may contact the data	
officer on all issues related to the	officer on all issues related to the	protection officer on all issues	
processing of the data subject's	processing of the data subject's data	related to the processing of the data	
data and to request exercising the	and to request exercising the rights	subject's data and to request	
rights under this Regulation.	under this Regulation.	exercising the the exercise of their	
		rights under this Regulation.	
11. The Commission shall be	deleted	deleted	
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.			

Article 36	Article 36	Article 36	
Position of the data protection	Position of the data protection	Position of the data protection	
officer	officer	officer	
	Amendment 133		
	1. The controller or the processor	1. The controller or the processor	1. The controller or the processor
	shall ensure that the data protection	shall ensure that the data protection	shall ensure that the data protection
	officer is properly and in a timely	officer is properly and in a timely	officer is properly and in a timely
	manner involved in all issues which	manner involved in all issues which	manner involved in all issues which
relate to the protection of personal	relate to the protection of personal	relate to the protection of personal	relate to the protection of personal
	data.	data.	data.
	2. The controller or processor shall	2. The controller or processor shall	2. The controller or processor shall
<u> </u>	ensure that the data protection	ensure that support the data	support the data protection officer
_	officer performs the duties and tasks	protection officer <i>in</i> performs <i>ing</i>	in performing the tasks referred to
	independently and does not receive	the duties and tasks referred to in	in Article 37 by providing resources
	any instructions as regards the	Article 37 by providing resources	necessary to carry out these tasks as
	exercise of the function. The data	necessary to carry out these tasks	well as access to personal data and
-	protection officer shall directly	as well as access to personal data	processing operations.
	report to the <i>executive</i> management	and processing	
	of the controller or the processor.	operations independently and does	
	<u>-</u>		
		•	
	o a constant of the constant o	1	
	1 0		
		or the controller or the processor.	
	ms regumen.		(2a new) Data subjects may contact
			1 ,
			l -
	The controller or processor shall for this purpose designate an executive management member who shall be responsible for the compliance with the provisions of this Regulation.	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.	(2a new) Data subjects may conthe data protection officer on a issues related to the processing the data subject's data and the exercise of their rights under the Regulation.

3. The controller or the processor	3. The controller or the processor	3. The controller or the processor	3. The controller or processor shall
shall support the data protection	shall support the data protection	shall support ensure that the data	ensure that the data protection
officer in performing the tasks and	officer in performing the tasks and	protection officer can act in an	officer can act in an independent
shall provide staff, premises,	shall provide <i>all means</i> , including	independent manner with respect	manner with respect to the
equipment and any other resources	staff, premises, equipment and any	to the performingance of his or her	performance of his or her tasks and
necessary to carry out the duties	other resources necessary to carry	the tasks and shall provide staff,	does not receive any instructions
and tasks referred to in Article 37.	out the duties and tasks referred to	premises, equipment and any other	regarding the exercise of these
	in Article 37, and to maintain his	resources necessary to carry out the	tasks. He or she shall not be
	or her professional knowledge.	duties and does not receive any	dismissed or penalised by the
		instructions regarding the exercise	controller or the processor for
		of these tasks referred to in Article	performing his tasks. The data
		37. He or she shall not be	protection officer shall directly
		penalised by the controller or the	report to the highest management
		processor for performing his tasks.	level of the controller or the
		The data protection officer shall	processor.
		directly report to the highest	_
		management level of the controller	
		or the processor.	
	4. Data protection officers shall be		4. Data protection officers shall be
	bound by secrecy concerning the		bound by professional secrecy
	identity of data subjects and		concerning the performance of his
	concerning circumstances		or her tasks.
	enabling data subjects to be		
	identified, unless they are released		
	from that obligation by the data		
	subject.		

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

Article 37	Article 37	Article 37	
Tasks of the data protection officer	Tasks of the data protection officer	Tasks of the data protection officer	
	Amendment 134		
1. The controller or the processor	1. The controller or the processor	1. The <del>controller or the processor</del>	1. The data protection officer shall
shall entrust the data protection	shall entrust the data protection	shall entrust the data protection	have at least the following tasks:
officer at least with the following	officer at least with the following	officer at least with shall have the	
tasks:	tasks:	following tasks:	
(a) to inform and advise the	(a) to raise awareness, to inform	(a) to inform and advise the	(a) to inform and advise the
controller or the processor of their	and advise the controller or the	controller or the processor and the	controller or the processor and the
obligations pursuant to this	processor of their obligations	employees who are processing	employees who are processing
Regulation and to document this	pursuant to this Regulation, in	personal data of their obligations	personal data of their obligations
activity and the responses received;	particular with regard to technical	pursuant to this Regulation and to	pursuant to this Regulation and to
	and organisational measures and	document this activity and the	other Union or Member State data
	<i>procedures</i> , and to document this	responses received other Union or	protection provisions;
	activity and the responses received;	Member State data protection	
		provisions;	

(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; (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;

(b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with 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, awareness-raising and the training of staff involved in the processing operations, and the related audits;

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

(d) to ensure that the documentation referred to in Article 28 is maintained; (e) to monitor the documentation, notification and communication of personal data breaches pursuant to	(d) to ensure that the documentation referred to in Article 28 is maintained; (e) to monitor the documentation, notification and communication of personal data breaches pursuant to	deleted	
Articles 31 and 32; (f) to monitor the performance of the data protection impact assessment by the controller or processor and the application for prior authorisation or prior consultation, if required pursuant Articles 33 and 34;	Articles 31 and 32; (f) to monitor the performance of the data protection impact assessment by the controller or processor and the application for prior authorisation or prior consultation, if required pursuant to Articles 32a, 33 and 34;	(f) to monitor the performance of provide advice where requested as regards the data protection impact assessment by the controller or processor and the application for prior authorisation or prior consultation, if required monitor its performance pursuant Articles	(f) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 33;

(g) to monitor the response to requests from the supervisory authority, and, within the sphere of	(g) to monitor the response to requests from the supervisory authority, and, within the sphere of	(g) to monitor the responses to requests from the supervisory authority, and, within the sphere of	(g) to monitor responses to requests from the supervisory authority, and, within the sphere of the data
the data protection officer's	the data protection officer's	the data protection officer's	protection officer's competence, to
competence, co-operating with the	competence, co-operating with the	competence, to co-operating operate	cooperate with the supervisory
supervisory authority at the latter's	supervisory authority at the latter's	with the supervisory authority at	authority at the latter's request or on
request or on the data protection	request or on the data protection	the latter's request or on the data	the data protection officer's own
officer's own initiative;	officer's own initiative;	protection officer's own initiative;	initiative;
(h) to act as the contact point for	(h) to act as the contact point for the	(h) to act as the contact point for	(h) to act as the contact point for
the supervisory authority on issues	supervisory authority on issues	the supervisory authority on issues	the supervisory authority on issues
related to the processing and	related to the processing and consult	related to the processing of	related to the processing of personal
consult with the supervisory	with the supervisory authority, if	personal data, including the prior	data, including the prior
authority, if appropriate, on his/her	appropriate, on his/her own	and consultation referred to in	consultation referred to in Article
own initiative.	initiative.	Article 34, and consult, as with	34, and consult, as appropriate, on
		the supervisory authority, if	any other matter.
		appropriate, on his/her own	
		initiative any other matter.	
	(i) to verify the compliance with		
	this Regulation under the prior		
	consultation mechanism laid out in		
	Article 34;		
	(j) to inform the employee		
	representatives on data processing		
	of the employees.		

2. The Commission shall be	deleted	deleted	
empowered to adopt delegated acts			
in accordance with Article 86 for			
the purpose of further specifying			
the criteria and requirements for			
tasks, certification, status, powers			
and resources of the data protection			
officer referred to in paragraph 1.			
		2a. The data protection officer	2a. The data protection officer shall
		shall in the performance his or her	in the performance his or her tasks
		tasks have due regard to the risk	have due regard to the risk
		associated with the processing	associated with the processing
		operations, taking into account the	operations, taking into account the
		nature, scope, context and	nature, scope, context and purposes
		purposes of the processing.	of the processing.

SECTION5	SECTION5	SECTION5	
CODES OF CONDUCT	CODES OF CONDUCT	CODES OF CONDUCT	
AND CERTIFICATION	AND CERTIFICATION	AND CERTIFICATION	
Article 38	Article 38	Article 38	
Codes of conduct	Codes of conduct	Codes of conduct	
	Amendment 135		
1. The Member States, the	1. The Member States, the	1. The Member States, the	1. The Member States, the
supervisory authorities and the	supervisory authorities and the	supervisory authorities, the	supervisory authorities, the
Commission shall encourage the	Commission shall encourage the	European Data Protection Board	European Data Protection Board
drawing up of codes of conduct	drawing up of codes of conduct or	and the Commission shall	and the Commission shall
intended to contribute to the proper	the adoption of codes of conduct	encourage the drawing up of codes	encourage the drawing up of codes
application of this Regulation,	drawn up by a supervisory	of conduct intended to contribute to	of conduct intended to contribute to
taking account of the specific	authority intended to contribute to	the proper application of this	the proper application of this
features of the various data	the proper application of this	Regulation, taking account of the	Regulation, taking account the
processing sectors, in particular in	Regulation, taking account of the	specific features of the various data	specific needs of micro, small and
relation to:	specific features of the various data	processing sectors, in particular in	medium-sized enterprises.
	processing sectors, in particular in	relation to: and the specific needs	
	relation to:	of micro, small and medium-sized	
		enterprises.	

		1a. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of provisions of this Regulation, such as:	1a. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of provisions of this Regulation, such as:
(a) fair and transparent data	(a) fair and transparent data	(a) fair and transparent data	(a) fair and transparent data
processing;	processing; (aa) respect for consumer rights;	processing;	processing;
		(aa) the legitimate interests pursued by controllers in specific contexts;	(aa) the legitimate interests pursued by controllers in specific contexts;
(b) the collection of data;	(b) the collection of data;	(b) the collection of data;	(b) the collection of data;
		(bb) the pseudonymisation of personal data;	(bb) the pseudonymisation of personal data;
(c) the information of the public and of data subjects;	(c) the information of the public and of data subjects;	(c) the information of the public and of data subjects;	(c) the information of the public and of data subjects;
(d) requests of data subjects in exercise of their rights;	(d) requests of data subjects in exercise of their rights;	(d) requests of data subjects inthe exercise of their rights of data subjects;	(d) the exercise of their rights of data subjects;

(e) information and protection of	(e) information and protection of	(e) information and protection of	(e) information and protection of
children;	children;	children and the way to collect the	children and the way to collect the
		parent's and guardian's consent;	parent's and guardian's consent;
		(ee) measures and procedures	(ee) measures and procedures
		referred to in Articles 22 and 23	referred to in Articles 22 and 23
		and measures to ensure security of	and measures to ensure security of
		processing referred to in Article	processing referred to in Article 30;
		30;	
		(ef) notification of personal data	(ef) notification of personal data
		breaches to supervisory authorities	breaches to supervisory authorities
		and communication of such	and communication of such
		breaches to data subjects;	breaches to data subjects;
(f) transfer of data to third countries	(f) transfer of data to third countries	deleted	
or international organisations;	or international organisations;		
(g) mechanisms for monitoring and	(g) mechanisms for monitoring and	deleted	
ensuring compliance with the code	ensuring compliance with the code		
by the controllers adherent to it;	by the controllers adherent to it;		
(h) out-of-court proceedings and	(h) out-of-court proceedings and	deleted	(h) out-of-court proceedings and
other dispute resolution procedures	other dispute resolution procedures		other dispute resolution procedures
for resolving disputes between	for resolving disputes between		for resolving disputes between
controllers and data subjects with	controllers and data subjects with		controllers and data subjects with
respect to the processing of	respect to the processing of personal		respect to the processing of
personal data, without prejudice to	data, without prejudice to the rights		personal data, without prejudice to
the rights of the data subjects	of the data subjects pursuant to		the rights of the data subjects
pursuant to Articles 73 and 75.	Articles 73 and 75.		pursuant to Articles 73 and 75.

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

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

		1b. Such a code of conduct shall contain mechanisms which enable the body referred to in paragraph 1 of article 38a to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors which undertake to apply it, without prejudice to the tasks and powers of the supervisory authority which is competent pursuant to Article 51 or 51a.	1b. Such a code of conduct pursuant to paragraph 1a shall contain mechanisms which enable the body referred to in paragraph 1 of article 38a to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors which undertake to apply it, without prejudice to the tasks and powers of the supervisory authority which is competent pursuant to Article 51 or 51a.
2. Associations and other bodies representing categories of controllers or processors in one Member State which intend to draw up codes of conduct or to amend or extend existing codes of conduct may submit them to an opinion of the supervisory authority in that Member State. The supervisory	2. Associations and other bodies representing categories of controllers or processors in one Member State which intend to draw up codes of conduct or to amend or extend existing codes of conduct may submit them to an opinion of the supervisory authority in that Member State. The supervisory	2. Associations and other bodies referred to in paragraph 1a representing categories of controllers or processors in one Member State which intend to draw up-prepare a codes of conduct or to amend or extend an existing codes, of conduct may shall submit them to an opinion of draft code to the	2. Associations and other bodies referred to in paragraph 1a which intend to prepare a codes-of conduct or to amend or extend an existing codes, shall submit the draft code to the supervisory authority which is competent pursuant to Article 51. The supervisory authority shall give an opinion on whether the draft code, or amended or extended code is in compliance with this Regulation and shall approve such draft, amended or extended code if it finds that it provides sufficient appropriate safeguards.

authority may give an opinion	authority may shall without undue	supervisory authority in that	
whether the draft code of conduct	<i>delay</i> give an opinion <i>on</i> whether	Member State which is competent	
or the amendment is in compliance	the processing under the draft code	pursuant to Article 51. The	
with this Regulation. The	of conduct or the amendment is in	supervisory authority may shall	
supervisory authority shall seek the	compliance with this Regulation.	give an opinion <i>on</i> whether the	
views of data subjects or their	The supervisory authority shall seek	draft code, or amended or extended	
representatives on these drafts.	the views of data subjects or their	code of conduct or the amendment	
	representatives on these drafts.	is in compliance with this	
		Regulation and shall approve such	
		draft, amended or extended code if	
		it finds that it provides sufficient	
		appropriate safeguards. The	
		supervisory authority shall seek the	
		views of data subjects or their	
		representatives on these drafts.	
		2a. Where the opinion referred to	2a. Where the opinion referred to in
		in paragraph 2 confirms that the	paragraph 2 confirms that the code
		code of conduct, or amended or	of conduct, or amended or extended
		extended code, is in compliance	code, is in compliance with this
		with this Regulation and the code	Regulation and the code is
		is approved, and if the code of	approved, and if the code of
		conduct does not relate to	conduct does not relate to
		processing activities in several	processing activities in several
		Member States, the supervisory	Member States, the supervisory
		authority shall register the code	authority shall register and publish
		and publish the details thereof.	the code.

		2b. Where the draft code of	2b. Where the draft code of conduct
		conduct relates to processing	relates to processing activities in
		activities in several Member	several Member States, the
		States, the supervisory authority	supervisory authority competent
		competent pursuant to Article 51	pursuant to Article 51 shall, before
		1 * *	1
		shall, before approval, submit it in	approval, submit it in the procedure referred to in Article 57 to the
		the procedure referred to in Article	
		57 to the European Data	European Data Protection Board
		Protection Board which shall give	which shall give an opinion on
		an opinion on whether the draft	whether the draft code, or amended
		code, or amended or extended	or extended code, is in compliance
		code, is in compliance with this	with this Regulation or, in the
		Regulation or, in the situation	situation referred to in paragraph
		referred to in paragraph 1ab,	1ab, provides appropriate
		provides appropriate safeguards.	safeguards.
3. Associations and other bodies	3. Associations and other bodies	3. Associations and other bodies	3. Where the opinion referred to in
representing categories of	representing categories of	representing categories of	paragraph 2b confirms that the
controllers in several Member	controllers <i>or processors</i> in several	controllers in several Member	codes of conduct, or amended or
States may submit draft codes of	Member States may submit draft	States may submit draft Where the	extended codes, is in compliance
conduct and amendments or	codes of conduct and amendments	opinion referred to in paragraph	with this Regulation, or, in the
extensions to existing codes of	or extensions to existing codes of	2b confirms that the codes of	situation referred to in paragraph
conduct to the Commission.	conduct to the Commission.	conduct, and or amendmentsed or	1ab, provides appropriate
		extensions <i>ded</i> to existing codes, of	safeguards, the European Data
		conduct to the Commission is in	Protection Board shall submit its
		compliance with this Regulation,	opinion to the Commission.
		or, in the situation referred to in	
		paragraph 1ab, provides	
		appropriate safeguards, the	
		European Data Protection Board	
		shall submit its opinion to the	
		Commission.	
		Commission.	

4. The Commission may adopt	4. The Commission may adopt	4. The Commission may adopt	4. The Commission may adopt
implementing acts for deciding that	implementing acts shall be	implementing acts for deciding that	implementing acts for deciding that
the codes of conduct and	empowered to adopt, after	the <i>approved</i> codes of conduct and	the approved codes of conduct and
amendments or extensions to	requesting an opinion of the	amendments or extensions to	amendments or extensions to
existing codes of conduct submitted	European Data Protection Board,	existing approved codes of	existing approved codes of
to it pursuant to paragraph 3 have	delegated acts in accordance with	conduct submitted to it pursuant to	conduct submitted to it pursuant to
general validity within the Union.	Article 86 for deciding that the	paragraph 3 have general validity	paragraph 3 have general validity
Those implementing acts shall be	codes of conduct and amendments	within the Union. Those	within the Union. Those
adopted in accordance with the	or extensions to existing codes of	implementing acts shall be adopted	implementing acts shall be adopted
examination procedure set out in	conduct submitted to it pursuant to	in accordance with the examination	in accordance with the examination
Article 87(2).	paragraph 3 are in line with this	procedure set out in Article 87(2).	procedure set out in Article 87(2).
	Regulation and have general		
	validity within the Union. Those		
	implementing acts delegated acts		
	shall be adopted in accordance with		
	the examination procedure set out in		
	Article 87(2) confer enforceable		
	rights on data subjects.		
5. The Commission shall ensure	5. The Commission shall ensure	5. The Commission shall ensure	5. The Commission shall ensure
appropriate publicity for the codes	appropriate publicity for the codes	appropriate publicity for the	appropriate publicity for the
which have been decided as having	which have been decided as having	approved codes which have been	approved codes which have been
general validity in accordance with	general validity in accordance with	decided as having general validity	decided as having general validity
paragraph 4.	paragraph 4.	in accordance with paragraph 4.	in accordance with paragraph 4.
		5a. The European Data Protection	5a. The European Data Protection
		Board shall collect all approved	Board shall collect all approved
		codes of conduct and amendments	codes of conduct and amendments
		thereto in a register and shall make	thereto in a register and shall make
		them publicly available through any	them publicly available through any
		appropriate means, such as through	appropriate means.
		the European E-Justice Portal.	

Article 38a	
Monitoring of approved codes of	
conduct	
1. Without prejudice to the tasks	1. Without prejudice to the tasks
and powers of the competent	and powers of the competent
supervisory authority under	supervisory authority under Articles
Articles 52 and 53, the monitoring	52 and 53, the monitoring of
of compliance with a code of	compliance with a code of conduct
conduct pursuant to Article 38	pursuant to Article 38, may be
(1b), may be carried out by a body	carried out by a body which has an
which has an appropriate level of	appropriate level of expertise in
expertise in relation to the subject-	relation to the subject-matter of the
matter of the code and is	code and is accredited for this
accredited for this purpose by the	purpose by the competent
competent supervisory authority.	supervisory authority.
2. A body referred to in paragraph	2. A body referred to in paragraph 1
1 may be accredited for this	may be accredited for this purpose
purpose if:	if:
(a) it has demonstrated its	(a) it has demonstrated its
independence and expertise in	independence and expertise in
relation to the subject-matter of	relation to the subject-matter of the
the code to the satisfaction of the	code to the satisfaction of the
competent supervisory authority;	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	(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
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	processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;
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	processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;
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	code, to monitor their compliance with its provisions and to periodically review its operation;
with its provisions and to periodically review its operation;  (c) it has established procedures and structures to deal with complaints about infringements of	with its provisions and to periodically review its operation;
periodically review its operation;  (c) it has established procedures and structures to deal with complaints about infringements of	periodically review its operation;
(c) it has established procedures and structures to deal with complaints about infringements of	
and structures to deal with complaints about infringements of	
complaints about infringements of	and structures to deal with
	complaints about infringements of
the code or the manner in which	the code or the manner in which the
the code has been, or is being,	code has been, or is being,
implemented by a controller or	implemented by a controller or
processor, and to make these	processor, and to make these
procedures and structures	procedures and structures
transparent to data subjects and	transparent to data subjects and the
the public;	public;
(d) it demonstrates to the	(d) it demonstrates to the
satisfaction of the competent	satisfaction of the competent
supervisory authority that its tasks	supervisory authority that its tasks
and duties do not result in a	and duties do not result in a conflict
conflict of interests.	of interests.
3. The competent supervisory	3. The competent supervisory
authority shall submit the draft	authority shall submit the draft
criteria for accreditation of a body	criteria for accreditation of a body
referred to in paragraph 1 to the	referred to in paragraph 1 to the
European Data Protection Board	European Data Protection Board
pursuant to the consistency	pursuant to the consistency
mechanism referred to in Article 57.	mechanism referred to in Article 57.

4. Without prejudice to the	4. Without prejudice to the
provisions of Chapter VIII, a body	provisions of Chapter VIII, a body
referred to in paragraph 1 may,	referred to in paragraph 1 may,
subject to adequate safeguards,	subject to adequate safeguards, take
take appropriate action in cases of	appropriate action in cases of
infringement of the code by a	infringement of the code by a
controller or processor, including	controller or processor, including
suspension or exclusion of the	suspension or exclusion of the
controller or processor concerned	controller or processor concerned
from the code. It shall inform the	from the code. It shall inform the
competent supervisory authority of	competent supervisory authority of
such actions and the reasons for	such actions and the reasons for
taking them.	taking them.
5. The competent supervisory	5. The competent supervisory
authority shall revoke the	authority shall revoke the
accreditation of a body referred to	accreditation of a body referred to
in paragraph 1 if the conditions	in paragraph 1 if the conditions for
for accreditation are not, or no	accreditation are not, or no longer,
longer, met or actions taken by the	met or actions taken by the body
body are not in compliance with	are not in compliance with this
this Regulation.	Regulation.
6. This article shall not apply to	6. This article shall not apply to the
the processing of personal data	processing of personal data carried
carried out by public authorities	out by public authorities and
and bodies.	bodies.

Article 39	Article 39	Article 39	
Certification	Certification	Certification	
	Amendment 136		
1. The Member States and the	deleted	1. The Member States, <i>the</i>	1. The Member States, the
Commission shall encourage, in		European Data Protection Board	supervisory authorities, the
particular at European level, the		and the Commission shall	European Data Protection Board
establishment of data protection		encourage, in particular at	and the Commission shall
certification mechanisms and of		European Union level, the	encourage, in particular at Union
data protection seals and marks,		establishment of data protection	level, the establishment of data
allowing data subjects to quickly		certification mechanisms and of	protection certification mechanisms
assess the level of data protection		data protection seals and marks, for	and of data protection seals and
provided by controllers and		the purpose of demonstrating	marks, for the purpose of
processors. The data protection		compliance with this Regulation of	demonstrating compliance with this
certifications mechanisms shall		processing operations carried out	Regulation of processing operations
contribute to the proper application		allowing data subjects to quickly	carried out by controllers and
of this Regulation, taking account		assess the level of data protection	processors. The specific needs of
of the specific features of the		<del>provided</del> by controllers and	micro, small and medium-sized
various sectors and different		processors. The data protection	entreprises shall be taken into
processing operations.		certifications mechanisms shall	account.
		contribute to the proper application	
		of this Regulation, taking account	
		of the specific features of the	
		various sectors and different	
		processing operationsneeds of	
		micro, small and medium-sized	
		entreprises shall be taken into	
		account.	

	1a. In addition to adherence by	1a. In addition to adherence by
	•	_
	controllers or processors subject to	controllers or processors subject to
	this Regulation, data protection	this Regulation, data protection
	certification mechanisms, seals or	certification mechanisms, seals or
	marks approved pursuant to	marks approved pursuant to
	paragraph 2a may also be	paragraph 2a may also be
	established for the purpose of	established for the purpose of
	demonstrating the existence of	demonstrating the existence of
	appropriate safeguards provided	appropriate safeguards provided by
	by controllers or processors that	controllers or processors that are
	are not subject to this Regulation	not subject to this Regulation
	according to Article 3 within the	according to Article 3 within the
	framework of personal data	framework of personal data
	transfers to third countries or	transfers to third countries or
	international organisations under	international organisations under
	the terms referred to in Article	the terms referred to in Article
	42(2)(e). Such controllers or	42(2)(e). Such controllers or
	processors shall make binding and	processors shall make binding and
	enforceable commitments, via	enforceable commitments, via
	contractual instruments or	contractual instruments or
	otherwise, to apply those	otherwise, to apply those
	appropriate safeguards, including	appropriate safeguards, including as
	as regards data subjects' rights.	regards data subjects' rights.
1a. Any controller or processor		<u> </u>
may request any supervisory		
authority in the Union, for a		
reasonable fee taking into accoun	t	
the administrative costs, to certify		
that the processing of personal		
mu me processing of personal		

data is performed in compliance with this Regulation, in particular with the principles set out in Article 5, 23 and 30, the obligations of the controller and	
the processor, and the data subject's rights.	
1b. The certification shall be voluntary, affordable, and available via a process that is transparent and not unduly	1b. The certification shall be voluntary and available via a process that is transparent.
burdensome.  1c. The supervisory authorities and the European Data Protection	
Board shall cooperate under the consistency mechanism pursuant	
to Article 57 to guarantee a harmonised data protection certification mechanism including harmonised fees within the Union.	
1d. During the certification procedure, the supervisory authorityies may accredit	
specialised third party auditors to carry out the auditing of the controller or the processor on their	
behalf. Third party auditors shall have sufficiently qualified staff, be	

impartial and free from any conflict of interests regarding their duties. Supervisory authorities shall revoke accreditation, if there are reasons to believe that the auditor does not fulfil its duties correctly. The final certification shall be provided by the supervisory authority.	
1e. Supervisory authorities shall grant controllers and processors, who pursuant to the auditing have been certified that they process personal data in compliance with this Regulation, the standardised data protection mark named "European Data Protection Seal".	
1f. The "European Data Protection Seal" shall be valid for as long as the data processing operations of the certified controller or processor continue to fully comply with this Regulation.  1g. Notwithstanding paragraph 1f, the certification shall be valid for maximum five years.	

2. The Commission shall be	Ih. The European Data Protection Board shall establish a public electronic register in which all valid and invalid certificates which have been issued in the Member States can be viewed by the publc.  Ii. The European Data Protection Board may on its own initiative certify that a data protection- enhancing technical standard is compliant with this Regulation.  2. The Commission shall be	[Moved and modified under	
empowered to adopt delegated acts	empowered to adopt, after	Article 39a point 7]	
in accordance with Article 86 for	requesting an opinion of the		
the purpose of further specifying	European Data Protection Board		
the criteria and requirements for the	and consulting with stakeholders,		
data protection certification	in particular industry and non-		
mechanisms referred to in	governmental organisations,		
paragraph 1, including conditions	delegated acts in accordance with		
for granting and withdrawal, and	Article 86 for the purpose of further		
requirements for recognition within the Union and in third countries.	specifying the criteria and requirements for the data protection		
the Omon and in unit countries.	certification mechanisms referred to		
	in <del>paragraph 1 paragraphs 1a to 1h</del> ,		
	including requirements for		
	accreditation of auditors,		
	conditions for granting and		
	withdrawal, and requirements for		

recognition within the Union and in third countries. Those delegated acts shall confer enforceable rights on data subjects.		
	2. A certification pursuant to this	2. A certification pursuant to this
	Article does not reduce the	Article does not reduce the
	responsibility of the controller or	responsibility of the controller or
	the processor for compliance with	the processor for compliance with
	this Regulation and is without	this Regulation and is without
	prejudice to the tasks and powers	prejudice to the tasks and powers of
	of the supervisory authority which	the supervisory authority which is
	is competent pursuant to Article 51	competent pursuant to Article 51 or
	or 51a.	51a.
	2a. A certification pursuant to this	2a. A certification pursuant to this
	Article shall be issued by the	Article shall be issued by the
	certification bodies referred to in	certification bodies referred to in
	Article 39a, or where applicable,	Article 39a, or, by the competent
	by the competent supervisory	supervisory authority on the basis
	authority on the basis of the	of the criteria approved by the
	criteria approved by the competent	competent supervisory authority or,
	supervisory authority or, pursuant	pursuant to Article 57, the
	to Article 57, the European Data	European Data Protection Board.
	Protection Board.	

3. 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).	deleted	[Moved under 39a point 8.]	
		3. The controller or processor	3. The controller or processor
		which submits its processing to the	which submits its processing to the
		certification mechanism shall	certification mechanism shall
		provide the certification body	provide the certification body referred to in Article 39a or the
		referred to in Article 39a, or where applicable, the competent	competent supervisory authority,
		supervisory authority, with all	with all information and access to
		information and access to its	its processing activities which are
		processing activities which are	necessary to conduct the
		necessary to conduct the	certification procedure.
		certification procedure.	continuation procedure.
		4. The certification shall be issued	4. The certification shall be issued
		to a controller or processor for a	to a controller or processor for a
		maximum period of 3 years and	maximum period of 3 years and
		may be renewed under the same	may be renewed under the same
		conditions as long as the relevant	conditions as long as the relevant
		requirements continue to be met. It	requirements continue to be met. It
		shall be withdrawn by the	shall be withdrawn by the
			certification bodies referred to in
			Article 39a, or where applicable, by
			the competent supervisory authority
			where the requirements for the

	certification are not or no longer
	met.

	certification bodies referred to in	
	Article 39a, or where applicable,	
	by the competent supervisory	
	authority where the requirements	
	for the certification are not or no	
	longer met.	
	5. The European Data Protection	5. The European Data Protection
	Board shall collect all certification	Board shall collect all certification
	mechanisms and data protection	mechanisms and data protection
	seals in a register and shall make	seals in a register and shall make
	them publicly available through	them publicly available through any
	any appropriate means, such as	appropriate means.
	through the European E-Justice	
	Portal.	

Article 39a	
Certificationbody and procedure	
1. Without prejudice to the tasks	1. Without prejudice to the tasks
and powers of the competent	and powers of the competent
supervisory authority under	supervisory authority under Articles
Articles 52 and 53, the	52 and 53, the certification shall be
certification shall be issued and	issued and renewed by a
renewed by a certification body	certification body which has an
which has an appropriate level of	appropriate level of expertise in
expertise in relation to data	relation to data protection. Each
protection. Each Member State	Member State shall provide
shall provide whether these	whether these certification bodies
certification bodies are accredited	are accredited by:
by:	
(a) the supervisory authority which	(a) the supervisory authority which
is competent according to Article	is competent according to Article
51 or 51a; and/or	51 [or 51a]; and/or
(b) the National Accreditation	(b) the National Accreditation Body
Body named in accordance with	named in accordance with
Regulation (EC) 765/2008 of the	Regulation (EC) 765/2008 of the
European parliament and the	European parliament and the
Council of 9 July 2008 setting out	Council of 9 July 2008 setting out
the requirements for accreditation	the requirements for accreditation
and market surveillance relating to	and market surveillance relating to
the marketing of products in	the marketing of products in
compliance with EN-ISO/IEC	compliance with EN-ISO/IEC
17065/2012 and with the	17065/2012 and with the additional
	requirements established by the
	supervisory authority which is
	competent according to Article 51
	[or 51a.]

additional requirements	
established by the supervisory	
authority which is competent	
according to Article 51 or 51a.	
2. The certification body referred	2. The certification body referred to
to in paragraph 1 may be	in paragraph 1 may be accredited
accredited for this purpose only if:	for this purpose only if:
(a) it has demonstrated its	(a) it has demonstrated its
independence and expertise in	independence and expertise in
relation to the subject-matter of	relation to the subject-matter of the
the certification to the satisfaction	certification to the satisfaction of
of the competent supervisory	the competent supervisory
authority;	authority;
(aa) it has undertaken to respect	(aa) it has undertaken to respect the
the criteria referred to in	criteria referred to in paragraph 2a
paragraph 2a of Article 39 and	of Article 39 and approved by the
approved by the supervisory	supervisory authority which is
authority which is competent	competent according to Article 51
according to Article 51 or 51a or,	[or 51a] or, pursuant to Article 57,
pursuant to Article 57, the	the European Data Protection
European Data Protection Board;	Board;
(b) it has established procedures	(b) it has established procedures for
for the issue, periodic review and	the issuing, periodic review and
withdrawal of data protection seals	withdrawal of data protection
and marks;	certification, seals and marks;

(c) it has established procedures	(c) it has established procedures
and structures to deal with	and structures to deal with
complaints about infringements of	complaints about infringements of
the certification or the manner in	the certification or the manner in
which the certification has been,	which the certification has been, or
or is being, implemented by the	is being, implemented by the
	<u> </u>
controller or processor, and to	controller or processor, and to make
make these procedures and	these procedures and structures
structures transparent to data	transparent to data subjects and the
subjects and the public;	public;
(d) it demonstrates to the	(d) it demonstrates to the
satisfaction of the competent	satisfaction of the competent
supervisory authority that its tasks	supervisory authority that its tasks
and duties do not result in a	and duties do not result in a conflict
conflict of interests.	of interests.
3. The accreditation of the	3. The accreditation of the
certification bodies referred to in	certification bodies referred to in
paragraph 1 shall take place on the	paragraph 1 shall take place on the
basis of criteria approved by the	basis of criteria approved by the
supervisory authority which is	supervisory authority which is
competent according to Article 51 or	competent according to Article 51 [or
51a or, pursuant to Article 57, the	51a] or, pursuant to Article 57, the
European Data Protection Board.	European Data Protection Board. In
In case of an accreditation pursuant	case of an accreditation pursuant to
to point (b) of paragraph 1, these	point (b) of paragraph 1, these
requirements complement those	requirements complement those
envisaged in Regulation 765/2008	envisaged in Regulation 765/2008
and the technical rules that describe	and the technical rules that describe
the methods and procedures of the	the methods and procedures of the
certification bodies.	certification bodies.

4. The certification body referred	4. The certification body referred to
to in paragraph 1 shall be	in paragraph 1 shall be responsible
responsible for the proper	for the proper assessment leading to
assessment leading to the	the certification or the withdrawal
certification or the withdrawal of	of such certification without
such certification without	prejudice to the responsibility of the
prejudice to the responsibility of	controller or processor for
the controller or processor for	compliance with this Regulation.
compliance with this Regulation.	The accreditation is issued for a
The accreditation is issued for a	maximum period of five years and
maximum period of five years and	can be renewed in the same
can be renewed in the same	conditions as long as the body
conditions as long as the body	meets the requirements.
meets the requirements.	-
5. The certification body referred	5. The certification body referred to
to in paragraph 1 shall provide the	in paragraph 1 shall provide the
competent supervisory authority	competent supervisory authority
with the reasons for granting or	with the reasons for granting or
withdrawing the requested	withdrawing the requested
certification.	certification.
6. The requirements referred to in	6. The requirements referred to in
paragraph 3 and the criteria	paragraph 3 and the criteria referred
referred to in paragraph 2a of	to in paragraph 2a of Article 39
Article 39 shall be made public by	shall be made public by the
the supervisory authority in an	supervisory authority in an easily
easily accessible form. The	accessible form. The supervisory
supervisory authorities shall also	authorities shall also transmit these
transmit these to the European	to the European Data Protection
Data Protection Board.	Board.

The European Data Protection	The European Data Protection
Board shall collect all certification	Board shall collect all certification
mechanisms and data protection	mechanisms and data protection
seals in a register and shall make	seals in a register and shall make
them publicly available through	them publicly available through any
any appropriate means, such as	appropriate means.
through the European E-Justice	appropriate intensity
Portal.	
6a. Without prejudice to the	6a. Without prejudice to the
provisions of Chapter VIII, the	provisions of Chapter VIII, the
competent supervisory authority or	competent supervisory authority or
the National Accreditation Body	the National Accreditation Body
shall revoke the accreditation it	shall revoke the accreditation it
granted to a certification body	granted to a certification body
referred to in paragraph 1 if the	referred to in paragraph 1 if the
conditions for accreditation are	conditions for accreditation are not,
not, or no longer, met or actions	or no longer, met or actions taken
taken by the body are not in	by the body are not in compliance
compliance with this Regulation.	with this Regulation.
7. The Commission shall be	7. The Commission shall be
empowered to adopt delegated acts	empowered to adopt delegated acts in
in accordance with Article 86, for	accordance with Article 86, for the
the purpose of specifying the criteria	purpose of specifying the criteria and
and requirements to be taken into	requirements to be taken into account
account for the data protection	for the data protection certification
certification mechanisms referred to	mechanisms referred to in paragraph
in paragraph 1 including conditions	1.
for granting and withdrawal, and	
requirements for recognition within	
the Union and in third countries.	

		7a. The European Data Protection	7a. The European Data Protection
		Board shall give an opinion to the	Board shall give an opinion to the
		Commission on the criteria and	Commission on the criteria and
		requirements referred to in	requirements referred to in
		paragraph 7.	paragraph 7.
3. The Commission may lay down	deleted	<b>8.</b> The Commission may lay down	<b>8.</b> The Commission may lay down
technical standards for certification		technical standards for certification	technical standards for certification
mechanisms and data protection		mechanisms and data protection	mechanisms and data protection
seals and marks and mechanisms to		seals and marks and mechanisms to	seals and marks and mechanisms to
promote and recognize certification		promote and recognize certification	promote and recognize certification
mechanisms and data protection		mechanisms and data protection	mechanisms and data protection
seals and marks. Those		seals and marks. Those	seals and marks. Those
implementing acts shall be adopted		implementing acts shall be adopted	implementing acts shall be adopted
in accordance with the examination		in accordance with the examination	in accordance with the examination
procedure set out in Article 87(2).		procedure set out in Article 87(2).	procedure set out in Article 87(2).