



Council of the
European Union

Brussels, 9 September 2015
(OR. en)

11784/15

LIMITE

DATAPROTECT 134
JAI 640
MI 547
DIGIT 63
DAPIX 144
FREMP 176
COMIX 383
CODEC 1162

Interinstitutional File:
2012/0011 (COD)

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

1. On 15th June 2015, the Council agreed on a General Approach (9565/15) on the proposal for a General Data Protection Regulation, thereby giving the Presidency a negotiating mandate to enter into trilogues with Parliament. The Presidency recalls the objective of reaching a conclusion on this reform by the end of 2015, in accordance with the conclusions of the European Council of 25/26th June 2015.

2. With a view to preparing the next trilogue, the Presidency invites delegations to discuss
 - 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
3. Delegations are reminded that provisions relating to articles not covered by this trilogue are marked in [brackets] as they will be discussed at a later stage.
4. While underlining that the General Approach reached by Council on 15th June 2015 constitutes the basis of the Presidency's negotiation mandate, and taking into account the position of the European Parliament on Chapter IV, the Presidency invites delegations to share their views on the different questions and suggestions listed below (points 8 and 9).
5. In order to ensure an efficient discussion process, as well as to maximise its clarity, the Presidency chose to divide the different provisions into three categories.

The first category (points 6 and 7) 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.

The second category (point 8) relates 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.

The third category (point 9) relates to provisions by the Parliament that differ from the provisions of the Council's General Approach. In this context, the Presidency invites delegations to share their views on the issues raised while keeping in mind the Council's General Approach.

Preparation for trilogue

6. Considering the position of the 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.

7. 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)
- 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(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), (5)
- 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 articles, they may do so under point 10.

8. With regard to the position of the European Parliament, the Presidency takes the view that on the following provisions the Council's General Approach should be maintained while remaining flexible on some modifications taking into consideration the Parliament's proposals:

Article 22 – Obligations of the controller

- The titles of this article are different for the European Parliament and the Council. The European Parliament has "*Responsibility and accountability of the controller*" and the Council has "*Obligations of the controller*". The Presidency suggests, as a compromise, to take the term "accountability" from the European Parliament proposal and therefore to have "*Accountability of the controller*" as title of Article 22.
- Concerning Article 22(1), the European Parliament makes a reference to the "*technical and organisational measures*" to be taken by the controller to "*be able to demonstrate in a transparent manner*" the compliance with the regulation. The Council refers to "*appropriate measures and be able to demonstrate*" the compliance. As both texts are rather consensual in substance, the Presidency suggests to accept the wording of the European Parliament "*appropriate technical and organizational measures to be able to demonstrate in a transparent manner*".

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 those two expressions on board.
- 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. The Presidency suggests to incorporate these terms in Article 23(1).

- The European Parliament keeps the term “*appropriate*” before “*technical and organizational measures*”. The Council’s General Approach covers the idea that the technical and organisational measures need to be appropriate, while using a slightly different wording. The Presidency suggests to take on board the European Parliament’s formulation “*appropriate technical and organisational measures*” which also reflect the wording used in Article 22(1).
- In its Article 23(1a), the European Parliament makes a reference to Directive 2004/18/EC. The Presidency suggests to put this 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. In order to clarify that it is the data subject’s intervention that is meant, the Presidency suggests to replace these terms by “*without the need of the data subject’s intervention*”.

Article 26 – Processor

- The European Parliament, in its Article 26(1), refers in the beginning to “*Where processing is to be carried out on behalf of the controller*” and introduces “*and ensure the protection of the rights of the data subject*”. The Presidency considers there is added value in reintroducing these wordings.
- Concerning Article 26(2(f)), the European Parliament added at the end of the paragraph “*taking into account the nature of processing and the information available to the processor*”. The Council’s General Approach does not contain such a wording. Delegations are invited to indicate their flexibility on the possible addition of this wording.
- 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 this formulation is clearer and more complete than the one of the Council’s General Approach. Delegations are invited to share their views on the possible introduction of this wording.

Article 27 – Processing under the authority of the controller and processor

- 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 European Parliament has “*Documentation*” and the Council has “*Records of categories of personal data processing activities*”. The Presidency suggests to keep only 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 European Parliament does not have such wording. Considering the optional nature of this provision given “*where possible*”, delegations are invited to indicate their flexibility on the deletion of these points.

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

- Concerning Article 31(3(e)), the European Parliament’s text contains “*and/or mitigate its effects*”. The Presidency takes the view that this can be added to the Council’s General Approach as a merge with Article 32(3(f)).

Article 33 – Data protection impact assessment

- The Presidency takes the view that Article 33(1a) of the Council’s General Approach is already covered in Article 37(1(f)), with the addition “*where requested*”, and suggests to delete it here.

Article 35 – Designation of the data protection officer

- Concerning Article 35(10), the Presidency suggests to move this paragraph to Article 36 which relates to the position of the data protection officer. Delegations are invited to confirm this reading.

Member States are invited to confirm the Presidency's suggestions or share their views on the issues raised under point 10.

9. Taking the Council's General Approach as a basis, and with regard to the position of the Parliament, the Presidency considers that certain provisions need further clarifications. Consequently the Presidency invites delegations to share their views as regards the following points:

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 considers this list of examples could be regrouped in a recital (for instance recital 60a) instead of enumerating them in each article. Delegations are invited to share their views on this point.

- The European Parliament's Article 32a identifies a certain number of elements to define "risk". These elements are used by the European Parliament in several instances of this chapter. While the Presidency suggests not to take on board this Article and maintain the Council's risk-based approach, the Presidency invites delegations to share their views in particular on the following elements to further precise the Council's notion of 'high 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"*.

Article 22 – Obligations of the controller

- The European Parliament makes a reference in its Article 22(1a) to compliance policies that *"shall to be reviewed at least every two years and updated when necessary"*. The Presidency takes the view that this can bring an added value to the measures that are mentioned in Article 22(2a). Delegations are invited to share their flexibility on the possibility 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 Council's General Approach does not contain this paragraph. The Presidency invites delegations to share their flexibility on a possible introduction of Article 22(3), subject to redrafting.
- 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 Council's General Approach does not have such a reference. The Presidency invites delegations to consider including a similar idea in a recital.

Article 23 – Data protection by design and by default

- In Article 23(1), the Council’s General Approach refers to the “*likelihood and severity of the risk*”. The European Parliament uses simply the term “*risk*”. The Presidency invites delegations to express their views on those terms and in particular in relation to fact that the concept of “*risk*” implies already the notions of likelihood and severity. This could be explained in a recital. A similar approach could be taken on such reference in Article 30.
- Concerning Article 23(1), the legislators 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, it is suggested 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*”. Delegations are invited to share their views on this formulation which better reflect the principle of data protection by design.
- 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. Delegations are invited to share their views on these two approaches, and in particular provide concrete examples on the restriction as formulated in the Council’s General Approach.

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 the Chapter VIII and should be clarified in particular in Article 77. Delegations are invited to share their views on it.

- 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. Delegations are invited to indicate their flexibility on the possible deletion of 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. Delegations are invited to share their views on these elements.

Article 26 – Processor

- 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 Council has deleted this paragraph. The Presidency suggests to reintroduce the Article 26(2(b)) subject to redrafting in order to make the provision more practicable.
- Concerning Article 26(2(e)), the European Parliament’s text has a reference to the “*appropriate and relevant technical and organisational requirements for the fulfillment of the controller’s obligation*”. The Council has deleted this reference. Delegations are invited to share their views on these terms.

- Concerning Article 26(3), the European Parliament refers to the instructions by the controller which shall be documented in writing. The Council's General Approach does not refer to instructions by the controller and states that "*the contract or other legal act referred to in paragraphs 2 and 2a shall be in writing, including in an electronic form*". Delegations are invited to share their views on the possible introduction of the term "*instructions*" 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 understands this addition that a powerful processor may be dictating the terms of a processing, and thereby no longer can be considered a processor. The Council's General Approach did not retain Article 26(4). Delegations are invited to indicate their flexibility on the possible reintroduction of Article 26(4) which maintains a clear categorisation of controller and processor. Additionally, delegations are invited to share their views on the inclusion of the added idea by the European Parliament.

Article 28 – Records of categories of personal data processing activities

- 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 invites delegations to indicate the necessity of this paragraph.

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 Council's General Approach does not include this obligation. The Presidency takes the view that the first sentence of the European Parliament can provide a helpful clarification for this chapter overall. Delegations are invited to share their flexibility on the possible reintroduction of the 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 Council's General Approach does not contain such a list in its Article 30(1a). The Presidency takes the view that the elements in this list, subject to redrafting, could be useful indications for the controllers and processors. Subject to redrafting, delegations are invited to share their flexibility on the possible introduction of the Article 30(1a) of the European Parliament's text as an indicative and open list.
- Concerning Article 30(3), the European Parliament provides for the European Data Protection Board to issue guidelines, recommendations and best practices for the technical and organisational security measures. The Council's General Approach does not foresee such a task for the European Data Protection Board. Delegations are invited to indicate their flexibility on the possible introduction of such a task in Article 66.

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

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

- 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 his or her rights and freedoms are severely affected (instead of a high risk as contained in the Council's General Approach). Delegations are invited to share their views on this gradual approach.
- 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, delegations are invited to indicate their flexibility for deleting this paragraph.

- The European Parliament provides for, in its Article 31(3(c)), 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*”. Delegations are invited to indicate their flexibility for introducing such a paragraph. 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. Delegations are invited to indicate their flexibility on the possible introduction of such a task in Article 66.
- Concerning Article 32(2), the European Parliament’s text contains a reference to Article 31(3(d)) that relates to the “*likely consequences of the personal data breach*”. The Council’s General Approach does not have such a reference. Delegations are invited to share their views on this.
- Concerning Article 32(3(a)) of the Council’s General Approach, the Presidency invite delegations to share their views on the added value of the terms “*in particular those*”.
- Concerning Article 32(3(c)) of the Council’s General Approach, the Presidency invite delegations to share their views on the added value of the terms “*in particular owing to the number of cases involved*”.
- 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 invites delegations to share their views on cases that justify this exception with no 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*”. Delegations are invited to indicate their flexibility for re-introducing this paragraph.

- 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. Delegations are invited to comment on the introduction of this idea.
- In Article 33(2(c)), the Council’s General Approach refers to “*optic-electronic devices*”. The Presidency considers that this may not be technologically neutral or futureproof, and suggests to use a more neutral term to cover the same idea, for example “*systematic monitoring of a publicly accessible area on a large scale*”.
- In Article 33(2a), (2b) and (2c) of the Council’s General Approach, the Presidency takes the view that such public lists could be usefully established by the European Data Protection Board. This would ensure a more harmonised and efficient approach. Delegations are invited to share their views on this possibility.
- In Article 33(3), the Council’s General Approach and the European Parliament’s text share the same idea but not the same structure. The Presidency invites delegations to share their flexibility on a possible change of structure. Considering the European Parliament’s extensive list in Article 33(3) and in a spirit of compromise, the Presidency considers that Article 33(3(b)) has some merit and invites the views of the delegations on this point.

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 takes the view that these different approaches require a necessary compromise. Considering the fact that the Council will show no flexibility on its risk-based approach, the Presidency invites delegations to consider the possibility for a mandatory data protection officer in strictly limited cases, in consistency with the risk-based approach. For instance, a mandatory data protection officer could be justified in case the processing activities of the controller or processor constitute a high risk for the rights and freedoms of individuals. The Presidency considers that there should be incentives for the designation of a data protection officer (whether mandatory or not) such as exemption from the obligation of prior consultation (article 34).

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. Delegations are invited to share their views on this idea.

Article 37 – Tasks of the data protection officer

- Concerning Article 37(1), the European Parliament created an open list of the tasks of the data protection officer by adding "*at least*". The Council's General Approach adopts a closed list. The Presidency invites delegations to share their flexibility for 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 invites delegations to share their views on the introduction of such a paragraph.

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 invites delegations to share their views on those terms and more particularly about the added value of keeping the reference which does not seem consistent with the risk-based approach.
- The European Parliament adds in Article 38(1(f)), (g) and (h) further elements to be included in codes of conduct. Delegations are invited to share their views on these points, in particular the possibility 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 invites delegations to share their views on those terms and more particularly about the added value of keeping the reference which does not seem consistent with the risk-based approach.
- In its Article 39(1b), the European Parliament proposes that “*the certification shall be voluntary and available via a process that is transparent and not unduly burdensome*”. The Presidency invites delegations to indicate their flexibility for introducing such an idea, possibly in a recital
- 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 invites the comments from delegations. Additionally, delegations are invited to share their views on the proposed standardized data protection mark named “European Data Protection Seal”.

The European Parliament envisages in Article 39(1i) that the European Data Protection Board certifies that a “data protection-enhancing technical standard” is in compliance with the Regulation. The Presidency invites the comments from delegations on such an approach.

COM (2012)0011	EP Position / First Reading	Council General Approach (15/06/2015)	Proposition of compromise
(60) Comprehensive responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should ensure and be obliged to demonstrate the compliance of each processing operation with this Regulation.	(60) Comprehensive responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established, <i>in particular with regard to documentation, data security, impact assessments, the data protection officer and oversight by data protection authorities.</i> In particular, the controller should ensure and be obliged <i>able</i> to demonstrate the compliance of each processing operation with this Regulation. <i>This should be verified by independent internal or external auditors.</i>	(60) Comprehensive <i>The</i> responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should ensure and be obliged <i>to implement appropriate measures and be able</i> to demonstrate the compliance of each processing operation <i>activities</i> with this Regulation. <i>These measures should take into account the nature, scope, context and purposes of the processing and the risk for the rights and freedoms of individuals.</i>	

		<p><i>(60a) Such risks, of varying likelihood and severity, may result from data processing which could lead to physical, material or moral damage, in particular where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality 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</i></p>	
--	--	--	--

		<p><i>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.</i></p>	
--	--	--	--

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

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

	<i>Amendment 38</i>		
(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. <i>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.</i>	(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.	

	<i>Amendment 39</i>		
<p>(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.</p>	<p>(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 <i>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</i> 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.</p>	<p>(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 <i>of</i> their behaviour <i>in the Union,</i> the controller should designate a representative, unless <i>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</i> 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.</p>	

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

		<p><i>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.</i></p>	
--	--	---	--

		<i>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.</i>	
	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.	<i>deleted</i>	

	<i>Amendment 41</i>		
(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 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.	(65) In order to <i>be able to</i> demonstrate compliance with this Regulation, the controller or processor should document each processing operation <i>maintain the documentation necessary in order to fulfill the requirements laid down in this Regulation.</i> 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 <i>evaluating the compliance with this Regulation.</i> <i>However, equal emphasis and significance should be placed on good practice and compliance and not just the completion of documentation.</i>	(65) In order to demonstrate compliance with this Regulation, the controller or processor should document each <i>maintain records regarding all categories of processing operation activities under its responsibility.</i> Each controller and processor should be obliged to co-operate with the supervisory authority and make this documentation <i>these records</i> , on request, available to it, so that it might serve for monitoring those processing operations.	

	<i>Amendment 42</i>		
(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.	(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 <i>should be promoted</i> and, where appropriate, cooperate <i>cooperation</i> with third countries <i>should be encouraged</i> .	(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 <i>including confidentiality</i> , taking into account <i>available technology</i> 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 <i>In assessing data security risk, consideration</i>	

		<i>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.</i>	
		<i>(66a) In order to enhance compliance with this Regulation in cases where the processing operations are likely to result in a high risk for the rights and freedoms of individuals, the controller should be responsible for the carrying out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of this risk. The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data is in compliance with this Regulation.</i>	

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

<p>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</p>	<p>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</p>	<p>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</p>	
---	--	---	--

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 <i>need</i> to mitigate an immediate risk of harm 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.	
---	---	---	--

<p>(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.</p>	<p>(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.</p>	<p>(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 <i>all</i> appropriate technological protection and organisational measures <i>have been implemented</i> 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, <i>The fact that the notification was made without undue delay should be established</i> taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. <i>Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation.</i></p>	
---	---	--	--

		<p><i>(68a) The communication of a personal data breach to the data subject should not be required if the controller has implemented appropriate technological protection measures, and that those measures were applied to the data affected by the personal data breach. Such technological protection measures should include those that render the data unintelligible to any person who is not authorised to access it, in particular by encrypting the personal data .</i></p>	
<p>(69) In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of the breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse.</p>	<p>(69) In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of the breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse.</p>	<p>(69) In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of the breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse.</p>	

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.	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.	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	(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	(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 result in a high risks to the rights and freedoms of data individuals by virtue of their nature, their scope, context and or their purposes. In such	

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

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

		<p><i>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</i></p>	
--	--	--	--

		<p><i>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.</i></p>	
	<i>Amendment 44</i>		
	<p><i>(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</i></p>		

	<i>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 Regulation.</i>		
	<i>Amendment 45</i>		
	<i>(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.</i>		

(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.	
	<i>Amendment 46</i>		
(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.	<i>deleted</i>	(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.	

	<i>Amendment 47</i>		
(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.	(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 operations processing activities, on a risky processing which might not be in compliance with this Regulation, and to make proposals to remedy such situation.	

		<p>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. <i>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,</i></p>	
--	--	---	--

		<i>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.</i>	
	Amendment 48		
	<i>(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.</i>		

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

	<i>Amendment 49</i>		
(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	(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 .	

	<p><i>whether or not performing that task full time, should be in a position to perform their duties and tasks independently and enjoy special protection against dismissal. Final responsibility should stay with the management of an organisation. The data protection officer should in particular be consulted prior to the design, procurement, development and setting-up of systems for the automated processing of personal data, in order to ensure the principles of privacy by design and privacy by default.</i></p>		
	<i>Amendment 50</i>		
	<p><i>(75a) The data protection officer should have at least the following qualifications: extensive knowledge of the substance and application of data protection law, including technical and organisational measures and procedures; mastery of technical requirements for privacy by design, privacy by default and data</i></p>		

	<p><i>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.</i></p>		
--	--	--	--

	<i>Amendment 51</i>		
(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, <i>after consultation of the representatives of the employees,</i> 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. <i>Such codes should make compliance with this Regulation easier for industry.</i>	(76) Associations or other bodies representing categories of controllers <i>or processors</i> 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 <i>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.</i>	

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

	<p><i>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.</i></p>		
--	---	--	--

<i>Article 4</i>	<i>Article 4</i>	<i>Article 4</i>	
<i>Definitions</i>	<i>Definitions</i>	<i>Definitions</i>	
	<i>Amendment 98</i>		
(9) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;	(9) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;	(9) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;	
(15) 'enterprise' means any entity engaged in an economic activity, irrespective of its legal form, thus including, in particular, natural and legal persons, partnerships or associations regularly engaged in an economic activity;	(15) 'enterprise' means any entity engaged in an economic activity, irrespective of its legal form, thus including, in particular, natural and legal persons, partnerships or associations regularly engaged in an economic activity;	(15) 'enterprise' means any <i>natural or legal person</i> entity engaged in an economic activity, irrespective of its legal form, thus including, in particular, natural and legal persons, partnerships or associations regularly engaged in an economic activity;	

CHAPTER IV CONTROLLER AND PROCESSOR	CHAPTER IV CONTROLLER AND PROCESSOR	CHAPTER IV CONTROLLER AND PROCESSOR	
SECTION 1 GENERAL OBLIGATIONS	SECTION 1 GENERAL OBLIGATIONS	SECTION 1 GENERAL OBLIGATIONS	
<i>Article 22</i>	<i>Article 22</i>	<i>Article 22</i>	
	<i>Amendment 117</i>		
<i>Responsibility of the controller</i>	<i>Responsibility and accountability of the controller</i>	<i>Responsibility</i> <i>Obligations of the controller</i>	
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 <i>appropriate</i> policies and implement appropriate <i>an demonstrable technical and organisational</i> measures to ensure and be able to demonstrate <i>in a transparent manner</i> that the processing of personal data is performed in compliance with this Regulation, <i>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</i>	1. <i>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,</i> 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.	

	<i>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.</i>		
	<i>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.</i>		
2. The measures provided for in paragraph 1 shall in particular include:	<i>deleted</i>	<i>deleted</i>	
(a) keeping the documentation pursuant to Article 28;	<i>deleted</i>	<i>deleted</i>	
(b) implementing the data security requirements laid down in Article 30;	<i>deleted</i>	<i>deleted</i>	
(c) performing a data protection impact assessment pursuant to Article 33;	<i>deleted</i>	<i>deleted</i>	

(d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2);	<i>deleted</i>	<i>deleted</i>	
(e) designating a data protection officer pursuant to Article 35(1).	<i>deleted</i>	<i>deleted</i>	
		<i>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.</i>	
		<i>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.</i>	
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 the be able to demonstrate the adequacy and effectiveness of the measures referred to in paragraphs 1 and 2.	<i>deleted</i>	

<p>If proportionate, this verification shall be carried out by independent internal or external auditors.</p>	<p>If proportionate, this verification shall be carried out by independent internal or external auditors <i>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.</i></p>		
	<p><i>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.</i></p>		

<p>4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures referred to in paragraph 1 other than those already referred to in paragraph 2, the conditions for the verification and auditing mechanisms referred to in paragraph 3 and as regards the criteria for proportionality under paragraph 3, and considering specific measures for micro, small and medium-sized-enterprises.</p>	<p><i>deleted</i></p>	<p><i>deleted</i></p>	
---	-----------------------	-----------------------	--

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

	<p><i>deletion, systematically focusing on comprehensive procedural safeguards regarding the accuracy, confidentiality, integrity, physical security and deletion of personal data. Where the controller has carried out a data protection impact assessment pursuant to Article 33, the results shall be taken into account when developing those measures and procedures.</i></p>		
	<p><i>1a. In order to foster its widespread implementation in different economic sectors, data protection by design shall be a prerequisite for public procurement tenders according to Directive 2004/18/EC of the European Parliament and of the Council¹ as well as according to Directive 2004/17/EC of the European Parliament and of the Council² (Utilities Directive).</i></p> <p><i>¹ Directive 2004/18/EC of the European Parliament and of the Council of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public</i></p>		

	<p><i>service contracts (OJ L 134, 30.4.2004, p. 114).</i></p> <p>² <i>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)</i></p>		
<p>2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.</p>	<p>2. The controller shall implement mechanisms for ensuring ensure that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained or disseminated beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals and that data subjects are able to control the distribution of their personal data.</p>	<p>2. The controller shall implement mechanisms appropriate measures for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of are processed; this applies to the amount of the data collected, the extent of their processing, and the time-period of their storage and their accessibility. <i>Where the purpose of the processing is not intended to provide the public with information</i> In particular, those</p>	

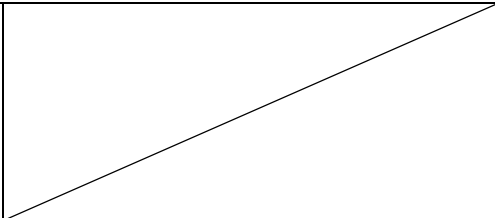
		mechanisms shall ensure that by default personal data are not made accessible <i>without human intervention</i> to an indefinite number of individuals.	
		<i>2a. An approved certification mechanism pursuant to Article 39 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2.</i>	
3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.	<i>deleted</i>	<i>deleted</i>	
4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	<i>deleted</i>	<i>deleted</i>	

<i>Article 24</i>	<i>Article 24</i>	<i>Article 24</i>	
<i>Joint controllers</i>	<i>Joint controllers</i>	<i>Joint controllers</i>	
	<i>Amendment 119</i>		
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 controller determines several 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 a controllers jointly determines the purposes, conditions 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>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.</i>	
		<i>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.</i>	

<i>Article 25</i>	<i>Article 25</i>	<i>Article 25</i>	
<i>Representatives of controllers not established in the Union</i>	<i>Representatives of controllers not established in the Union</i>	<i>Representatives of controllers not established in the Union</i>	
	<i>Amendment 120</i>		
1. In the situation referred to in Article 3(2), the controller shall designate a representative in the Union.	1. In the situation referred to in Article 3(2), the controller shall designate a representative in the Union.	1. In the situation referred to in Where Article 3(2) applies , the controller shall designate in writing a representative in the Union.	
2. This obligation shall not apply to:	2. This obligation shall not apply to:	2. This obligation shall not apply to:	
(a) a controller established in a third country where the Commission has decided that the third country ensures an adequate level of protection in accordance with Article 41; or	(a) a controller established in a third country where the Commission has decided that the third country ensures an adequate level of protection in accordance with Article 41; or	deleted	
(b) an enterprise employing fewer than 250 persons; or	(b) an enterprise employing fewer than 250 persons a 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	

(c) a public authority or body; or	(c) a public authority or body; or	(c) a public authority or body;	
(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 them the 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.	
		3a. The representative shall be mandated by the controller to be addressed in addition to or instead of the controller by, in particular, supervisory authorities and data subjects, on all issues related to the processing of personal data, for the purposes of ensuring compliance with this Regulation.	

4. The designation of a representative by the controller shall be without prejudice to legal actions which could be initiated against the controller itself.	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.	
--	--	--	---

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

		<i>1a. The processor shall not enlist another processor without the prior specific or general written consent of the controller. In the latter case, the processor should always inform the controller on any intended changes concerning the addition or replacement of other processors, thereby giving the opportunity to the controller to object to such changes.</i>	
2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall:	2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller. <i>The controller and the processor shall be free to determine respective roles and tasks with respect to the requirements of this Regulation, and shall provide that and stipulating in particular that the processor shall:</i>	2. The carrying out of processing by a processor shall be governed by a contract or other a legal act <i>under Union or Member State law binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, the rights of binding</i> the processor to the controller and stipulating in particular that the 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;	
(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	
(c) take all required measures pursuant to Article 30;	(c) take all required measures pursuant to Article 30;	(c) take all required required measures 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;	

(e) insofar as this is possible given the nature of the processing, create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;	(e) insofar as this is possible given the nature of the processing, create in agreement with the controller the necessary appropriate and relevant technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;	(e) insofar as this is possible given taking into account the nature of the processing, assist create in assist create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to in responding to requests for exercising the data subject's rights laid down in Chapter III;	
(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;	(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34, taking into account the nature of processing and the information available to the processor;	(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;	
(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 of the data;	(g) hand over all results to return 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 Member State law to which the processor is subject;	

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

		<i>organisational measures in such a way that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.</i>	
		<i>2aa. Adherence of the processor 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 sufficient guarantees referred to in paragraphs 1 and 2a.</i>	
		<i>2ab. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 2 and 2a may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 2b and 2c or on standard contractual clauses which are part of a</i>	

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

	<i>3a. The sufficient guarantees referred to in paragraph 1 may be demonstrated by adherence to codes of conduct or certification mechanisms pursuant to Articles 38 or 39 of this Regulation.</i>		
4. If a processor processes personal data other than as instructed by the controller, the processor shall be 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.	4. If a processor processes personal data other than as instructed by the controller <i>or becomes the determining party in relation to the purposes and means of data processing</i> , the processor shall be 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.	<i>deleted</i>	
5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the 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.	<i>deleted</i>	<i>deleted</i>	

<i>Article 27</i>	<i>Article 27</i>	<i>Article 27</i>	
<i>Processing under the authority of the controller and processor</i>	<i>Processing under the authority of the controller and processor</i>	<i>Processing under the authority of the controller and processor</i>	
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.	<i>deleted</i>	
<i>Article 28</i>	<i>Article 28</i>	<i>Article 28</i>	
<i>Documentation</i>	<i>Documentation</i>	<i>Records of categories of personal data processing activities</i>	
	<i>Amendment 122</i>		
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 <i>regularly updated</i> documentation of all processing operations under its responsibility <i>necessary to fulfill the requirements laid down in this Regulation.</i>	1. Each controller and processor and, if any, the controller's representative, shall maintain <i>a record</i> documentation of all <i>categories of personal data processing operations activities</i> under its responsibility. The documentation <i>This record</i> shall contain at least the following information:	

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

(f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;	<i>deleted</i>	(f) where applicable, <i>the categories of</i> transfers of <i>personal</i> data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;	
(g) a general indication of the time limits for erasure of the different categories of data;	<i>deleted</i>	(g) <i>where possible, the envisaged a</i> general indication of the time limits for erasure of the different categories of data;	
(h) the description of the mechanisms referred to in Article 22(3).	<i>deleted</i>	(h) <i>where possible, a general description of the technical and organisational security measures</i> the description of the mechanisms referred to in Article 22 <i>30(31)</i> .	
		<i>2a. Each processor shall maintain a record of all categories of personal data processing activities carried out on behalf of a controller, containing:</i>	

		<i>(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;</i>	
		<i>(b) the name and contact details of the data protection officer, if any;</i>	
		<i>(c) the categories of processing carried out on behalf of each controller;</i>	
		<i>(d) where applicable, the categories of transfers of personal data to a third country or an international organisation;</i>	
		<i>(e) where possible, a general description of the technical and organisational security measures referred to in Article 30(1).</i>	
		<i>3a. The records referred to in paragraphs 1 and 2a shall be in writing, including in an electronic or other non-legible form which is capable of being converted into a legible form.</i>	

3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority.	<i>deleted</i>	3. <i>On request,</i> The controller and the processor and, if any, the controller's representative, shall make the documentation <i>record</i> available, on request, to the supervisory authority.	
4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers and processors:	<i>deleted</i>	4. The obligations referred to in paragraphs 1 and 2 <i>a</i> shall not apply to the following controllers and processors:	
(a) a natural person processing personal data without a commercial interest; or	<i>deleted</i>	(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.	<i>deleted</i>	(b) an enterprise or an organisation employing fewer than 250 persons that is <i>unless the</i> processing personal data only as an activity ancillary to its main activities <i>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</i>	

		<i>for the data subjects, taking into account the nature, scope, context and purposes of the processing.</i>	
5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the documentation referred to in paragraph 1, to take account of in particular the responsibilities of the controller and the processor and, if any, the controller's representative.	<i>deleted</i>	<i>deleted</i>	
6. The Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	<i>deleted</i>	<i>deleted</i>	

<i>Article 29</i>	<i>Article 29</i>	<i>Article 29</i>	
<i>Co-operation with the supervisory authority</i>	<i>Co-operation with the supervisory authority</i>	<i>Co-operation with the supervisory authority</i>	
	<i>Amendment 123</i>		
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, 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.	<i>deleted</i>	
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.	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.	<i>deleted</i>	

SECTION 2 DATA SECURITY	SECTION 2 DATA SECURITY	SECTION 2 DATA SECURITY	
<i>Article 30</i>	<i>Article 30</i>	<i>Article 30</i>	
<i>Security of processing</i>	<i>Security of processing</i>	<i>Security of processing</i>	
	<i>Amendment 124</i>		
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.	

	<i>1a. Having regard to the state of the art and the cost of implementation, such a security policy shall include:</i>	<i>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.</i>	
	<i>(a) the ability to ensure that the integrity of the personal data is validated;</i>		
	<i>(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data;</i>		
	<i>(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;</i>		

	<i>(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.</i>		
2. The controller and the processor shall, following an evaluation of the risks, take the measures referred to in paragraph 1 to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data.	2. The controller and the processor shall, following an evaluation of the risks, take the measures referred to in paragraph 1 to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data. shall at least:	deleted	

	<i>(a) ensure that personal data can be accessed only by authorised personnel for legally authorised purposes;</i>		
		<i>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.</i>	
	<i>(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</i>		
		<i>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.</i>	

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

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:	<i>deleted</i>	<i>deleted</i>	
(a) prevent any unauthorised access to personal data;	<i>deleted</i>	<i>deleted</i>	
(b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data;	<i>deleted</i>	<i>deleted</i>	
(c) ensure the verification of the lawfulness of processing operations.	<i>deleted</i>	<i>deleted</i>	
Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	<i>deleted</i>	<i>deleted</i>	

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

		<i>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).</i>	
2. Pursuant to point (f) of Article 26(2), the processor shall alert and inform the controller immediately after the establishment of a personal data breach.	2. Pursuant to point (f) of Article 26(2), the The processor shall alert and inform the controller immediately without undue delay after the establishment of a personal data breach.	2. Pursuant to point (f) of Article 26(2), the processor shall alert notify and inform the controller immediately after the establishment without undue delay after becoming aware 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:	
(a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned;	(a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned;	(a) describe the nature of the personal data breach including where possible and appropriate, the approximate categories and number of data subjects concerned and the categories and approximate number of data records concerned;	
(b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained;	(b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained;	(b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained;	

(c) recommend measures to mitigate the possible adverse effects of the personal data breach;	(c) recommend measures to mitigate the possible adverse effects of the personal data breach;	<i>deleted</i>	
(d) describe the consequences of the personal data breach;	(d) describe the consequences of the personal data breach;	(d) describe the likely consequences of the personal data breach identified by the controller ;	
(e) describe the measures proposed or taken by the controller to address the personal data breach.	(e) describe the measures proposed or taken by the controller to address the personal data breach and/or mitigate its effects . <i>The information may if necessary be provided in phases.</i>	(e) describe the measures taken or proposed or to be taken by the controller to address the personal data breach; and	
		(f) where appropriate, indicate measures to mitigate the possible adverse effects of the personal data breach.	
		3a. Where, and in so far as, it is not possible to provide the information referred to in paragraph 3 (d), (e) and (f) at the same time as the information referred to in points (a) and (b) of paragraph 3, the controller shall provide this information without undue further delay.	

4. The controller shall document any personal data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose.	4. The controller shall document any personal data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must <i>be sufficient to</i> enable the supervisory authority to verify compliance with this Article <i>and with Article 30</i> . The documentation shall only include the information necessary for that purpose.	4. The controller shall document any personal data breaches <i>referred to in paragraphs 1 and 2</i> , comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose.	
	<i>4a. The supervisory authority shall keep a public register of the types of breaches notified.</i>		
5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for establishing the data breach referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor is required to notify the personal data breach.	5. The Commission <i>European Data Protection Board</i> shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose <i>entrusted with the task</i> of further specifying the criteria and requirements <i>issuing guidelines, recommendations and best practices in accordance with point (b) of Article 66(1)</i> for establishing the data breach <i>and determining the undue delay</i> referred to in paragraphs 1 and 2 and for the	deleted	

	particular circumstances in which a controller and a processor is are required to notify the personal data breach.		
6. The Commission may lay down the standard format of such notification to the supervisory authority, the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	<i>deleted</i>	<i>deleted</i>	

<i>Article 32</i>	<i>Article 32</i>	<i>Article 32</i>	
<i>Communication of a personal data breach to the data subject</i>	<i>Communication of a personal data breach to the data subject</i>	<i>Communication of a personal data breach to the data subject</i>	
	<i>Amendment 126</i>		
1. When the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay.	1. When the personal data breach is likely to adversely affect the protection of the personal data, the or privacy, the rights or the legitimate interests of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay.	1. When the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject result in a high risk for the rights and freedoms of individuals, such as discrimination, identity theft or fraud, financial loss, damage to the reputation, unauthorized reversal of pseudonymisation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage , the controller shall, after the notification referred 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 <i>be comprehensive and use clear and plain language. It shall</i> describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b) and , (c) <i>and (d)</i> of Article 31(3) <i>and information about the rights of the data subject, including redress.</i>	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), <i>(e)</i> and <i>(ef)</i> 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: <i>a.</i> the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological <i>and organisational</i> protection measures, and that those measures were applied to the data concerned <i>affected</i> by the personal data breach, <i>in particular those that</i> Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it, <i>such as encryption; or</i>	

		<p><i>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</i></p> <p><i>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</i></p> <p><i>d. it would adversely affect a substantial public interest.</i></p>	
<p>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.</p>	<p>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.</p>	<p><i>deleted</i></p>	

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements as to the circumstances in which a personal data breach is likely to adversely affect the personal data referred to in paragraph 1.	5. The Commission European Data Protection Board shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose entrusted with the task of further specifying the criteria and requirements issuing guidelines, recommendations and best 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.	<i>deleted</i>	
6. The Commission may lay down the format of the communication to the data subject referred to in paragraph 1 and the procedures applicable to that communication. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	<i>deleted</i>	<i>deleted</i>	

	<i>Amendment 127</i>		
	<i>Article 32a</i>		
	<i>Respect to Risk</i>		
	<i>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.</i>		
	<i>2. The following processing operations are likely to present specific risks:</i>		
	<i>(a) processing of personal data relating to more than 5000 data subjects during any consecutive 12-month period;</i>		
	<i>(b) processing of 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;</i>		

	<i>(c) profiling on which measures are based that produce legal effects concerning the individual or similarly significantly affect the individual;</i>		
	<i>(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;</i>		
	<i>(e) automated monitoring of publicly accessible areas on a large scale;</i>		
	<i>(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);</i>		
	<i>(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;</i>		

	<i>(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>		
	<i>(i) where personal data are made accessible to a number of persons which cannot reasonably be expected to be limited.</i>		
	<i>3. According to the result of the risk analysis:</i>		
	<i>(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;</i>		

	<i>(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;</i>		
	<i>(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;</i>		
	<i>(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.</i>		

	<p><i>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.</i></p>		
--	---	--	--

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

		<i>significant economic or social disadvantage</i> , 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 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:	<i>deleted</i>	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:	
(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	<i>deleted</i>	(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	

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

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

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

	<i>(a) a systematic description of the envisaged processing operations, the purposes of the processing and, if applicable, the legitimate interests pursued by the controller;</i>		
	<i>(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;</i>		
	<i>(c) an assessment of the risks to the rights and freedoms of data subjects, including the risk of discrimination being embedded in or reinforced by the operation;</i>		
	<i>(d) a description of the measures envisaged to address the risks and minimise the volume of personal data which is processed;</i>		
	<i>(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;</i>		

	<i>(f) a general indication of the time limits for erasure of the different categories of data;</i>		
	<i>(g) an explanation which data protection by design and default practices pursuant to Article 23 have been implemented;</i>		
	<i>(h) a list of the recipients or categories of recipients of the personal data;</i>		
	<i>(i) where applicable, a list of the intended transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;</i>		
	<i>(j) an assessment of the context of the data processing.</i>		
	<i>3a. If the controller or the processor has designated a data protection officer, he or she shall be involved in the impact assessment proceeding.</i>		

	<p><i>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.</i></p>		
		<p><i>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.</i></p>	

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.	<i>deleted</i>	4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.	
5. Where the controller is a public authority or body and where the processing results from a legal obligation pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing operations and regulated by Union law, paragraphs 1 to 4 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.	<i>deleted</i>	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.	

6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.	<i>deleted</i>	<i>deleted</i>	
7. The Commission may specify standards and procedures for carrying out and verifying and auditing the assessment referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	<i>deleted</i>	<i>deleted</i>	

	<i>Amendment 130</i>		
	<i>Article 33 a (new)</i>		
	<i>Data protection compliance review</i>		
	<p><i>1. At the latest two years after the carrying out of an impact assessment pursuant to Article 33(1), the controller or the processor acting on the controller's behalf shall carry out a compliance review. This compliance review shall demonstrate that the processing of personal data is performed in compliance with the data protection impact assessment.</i></p>		
	<p><i>2. The compliance review shall be carried out periodically at least once every two years, or immediately when there is a change in the specific risks presented by the processing operations.</i></p>		

	<i>3. Where the compliance review results show compliance inconsistencies, the compliance review shall include recommendations on how to achieve full compliance.</i>		
	<i>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.</i>		
	<i>5. If the controller or the processor has designated a data protection officer, he or she shall be involved in the compliance review proceeding.</i>		

<i>Article 34</i>	<i>Article 34</i>	<i>Article 34</i>	
	<i>Amendment 131</i>		
Prior authorisation and prior consultation	<i>Prior consultation</i>	Prior authorisation and prior consultation	
1. The controller or the processor as the case may be shall obtain an authorisation from the supervisory authority prior to the processing of personal data, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where a controller or processor adopts contractual clauses as provided for in point (d) of Article 42(2) or does not provide for the appropriate safeguards in a legally binding instrument as referred to in Article 42(5) for the transfer of personal data to a third country or an international organisation.	<i>deleted</i>	<i>deleted</i>	

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, 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 <i>where a data protection impact assessment as provided for in Article 33 indicates that the</i> in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the <i>would result in a high</i> risks involved for the data subjects where: <i>in the absence of measures to be taken by the controller to mitigate the risk.</i>	
(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	<i>deleted</i>	

<p>(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.</p>	<p>(b) <i>the data protection officer or</i> 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.</p>	<p><i>deleted</i></p>	
<p>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 non-compliance.</p>	<p>3. Where the <i>competent</i> supervisory authority is of the opinion <i>determines in accordance with its power</i> 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.</p>	<p>3. Where the supervisory authority is of the opinion that the intended processing <i>referred to in paragraph 2 would</i> does not comply with this Regulation, in particular where <i>the controller has</i> risks are insufficiently identified or mitigated the risk, it shall prohibit the intended processing and make appropriate proposals to remedy such non-compliance <i>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</i></p>	

		<i>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.</i>	
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.	<i>deleted</i>	
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.	<i>deleted</i>	<i>deleted</i>	

<p>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.</p>	<p>6. The controller or processor shall provide the supervisory authority, <i>on request</i>, with the data protection impact assessment provided for in <i>pursuant to</i> 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.</p>	<p><i>6. When consulting the supervisory authority pursuant to paragraph 2, The controller or processor shall provide the supervisory authority, with</i></p> <p><i>(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;</i></p> <p><i>(b) the purposes and means of the intended processing;</i></p> <p><i>(c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;</i></p> <p><i>(d) where applicable, the contact details of the data protection officer;</i></p> <p><i>(e) the data protection impact assessment provided for in Article 33; and</i></p>	
--	--	---	--

		(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 supervisory authority in the preparation of a legislative measure to be adopted by the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects.	7. Member States shall consult the supervisory authority in the preparation of a legislative measure to be adopted by the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects.	7. Member States shall consult the supervisory authority in during the preparation of a proposal for a legislative measure to be adopted by the 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 involved for the data subjects of personal data.	

		<i>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.</i>	
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.	<i>deleted</i>	<i>deleted</i>	

9. The Commission may set out standard forms and procedures for prior authorisations and consultations referred to in paragraphs 1 and 2, and standard forms and procedures for informing the supervisory authorities pursuant to paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	<i>deleted</i>	<i>deleted</i>	
--	----------------	----------------	--

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

(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; <i>or</i>	<i>deleted</i>	
	<i>(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.</i>		
2. In the case referred to in point (b) of paragraph 1, a group of undertakings may appoint a single data protection officer.	2. In the case referred to in point (b) of paragraph 1, a group of undertakings may appoint a single <i>main responsible</i> data protection officer, <i>provided it is ensured that a data protection officer is easily accessible from each establishment.</i>	2. In the case referred to in point (b) of paragraph 1, a group of undertakings may appoint a single data protection officer.	

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

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 <i>shall be designated</i> 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, <i>particularly the absence of any conflict of interests.</i> The necessary level of expert knowledge shall be determined in particular according to the data processing carried out and the protection required for the personal data processed by the controller or the processor.	
6. The controller or the processor shall ensure that any other professional duties of the data protection officer are compatible with the person's tasks and duties as data protection officer and do not result in a conflict of interests.	6. The controller or the processor shall ensure that any other professional duties of the data protection officer are compatible with the person's tasks and duties as data protection officer and do not result in a conflict of interests.	<i>deleted</i>	

<p>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.</p>	<p>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.</p>	<p>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.</p>	
<p>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.</p>	<p>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.</p>	<p>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.</p>	

9. The controller or the processor shall communicate the name and contact details of the data protection officer to the supervisory authority and to the public.	9. The controller or the processor shall communicate the name and contact details of the data protection officer to the supervisory authority and to the public.	9. The controller or the processor shall communicate publish the name and contact details of the data protection officer and communicate these to the supervisory authority and to the public .	
10. Data subjects shall have the right to contact the data protection officer on all issues related to the processing of the data subject's data and to request exercising the rights under this Regulation.	10. Data subjects shall have the right to contact the data protection officer on all issues related to the processing of the data subject's data and to request exercising the rights under this Regulation.	10. Data subjects shall have the right to may contact the data protection officer on all issues related to the processing of the data subject's data and to request exercising the the exercise of their rights under this Regulation.	
11. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the core activities of the controller or the processor referred to in point (c) of paragraph 1 and the criteria for the professional qualities of the data protection officer referred to in paragraph 5.	deleted	deleted	

<i>Article 36</i>	<i>Article 36</i>	<i>Article 36</i>	
<i>Position of the data protection officer</i>	<i>Position of the data protection officer</i>	<i>Position of the data protection officer</i>	
	<i>Amendment 133</i>		
1. The controller or the processor shall ensure that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data.	1. The controller or the processor shall ensure that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data.	1. The controller or the processor shall ensure that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data.	
2. The controller or processor shall ensure that the data protection officer performs the duties and tasks independently and does not receive any instructions as regards the exercise of the function. The data protection officer shall directly report to the management of the controller or the processor.	2. The controller or processor shall ensure that the data protection officer performs the duties and tasks independently and does not receive any instructions as regards the exercise of the function. The data protection officer shall directly report to the <i>executive</i> management of the controller or the processor. <i>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.</i>	2. The controller or processor shall ensure that <i>support</i> the data protection officer <i>in</i> performing the duties and tasks <i>referred to in Article 37 by providing resources necessary to carry out these tasks as well as access to personal data and processing operations</i> independently and does not receive any instructions as regards the exercise of the function. The data protection officer shall directly report to the management of the controller or the processor.	

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

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

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

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

(c) to monitor the implementation and application of this Regulation, in particular as to the requirements related to data protection by design, data protection by default and data security and to the information of data subjects and their requests in exercising their rights under this Regulation;	(c) to monitor the implementation and application of this Regulation, in particular as to the requirements related to data protection by design, data protection by default and data security and to the information of data subjects and their requests in exercising their rights under this Regulation;	<i>deleted</i>	
(d) to ensure that the documentation referred to in Article 28 is maintained;	(d) to ensure that the documentation referred to in Article 28 is maintained;	<i>deleted</i>	
(e) to monitor the documentation, notification and communication of personal data breaches pursuant to Articles 31 and 32;	(e) to monitor the documentation, notification and communication of personal data breaches pursuant to Articles 31 and 32;	<i>deleted</i>	
(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;	(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 <i>to</i> Articles <i>32a</i> , 33 and 34;	(f) to monitor the performance of <i>provide advice where requested as regards</i> the data protection impact assessment by the controller or processor and the application for prior authorisation or prior consultation, if required <i>monitor its performance</i> pursuant Articles 33 and 34;	

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

2. 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 tasks, certification, status, powers and resources of the data protection officer referred to in paragraph 1.	<i>deleted</i>	<i>deleted</i>	
		<i>2a. The data protection officer shall in the performance his or her tasks have due regard to the risk associated with the processing operations, taking into account the nature, scope, context and purposes of the processing.</i>	

SECTION 5 CODES OF CONDUCT AND CERTIFICATION	SECTION 5 CODES OF CONDUCT AND CERTIFICATION	SECTION 5 CODES OF CONDUCT AND CERTIFICATION	
<i>Article 38</i>	<i>Article 38</i>	<i>Article 38</i>	
<i>Codes of conduct</i>	<i>Codes of conduct</i>	<i>Codes of conduct</i>	
	<i>Amendment 135</i>		
1. The Member States, the supervisory authorities and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various data processing sectors, in particular in relation to:	1. The Member States, the supervisory authorities and the Commission shall encourage the drawing up of codes of conduct <i>or the adoption of codes of conduct drawn up by a supervisory authority</i> intended to contribute to the proper application of this Regulation, taking account of the specific features of the various data processing sectors, in particular in relation to:	1. The Member States, the supervisory authorities, <i>the European Data Protection Board</i> and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various data processing sectors, in particular in relation to: <i>and the specific needs of micro, small and medium-sized enterprises.</i>	

		<i>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:</i>	
(a) fair and transparent data processing;	(a) fair and transparent data processing;	(a) fair and transparent data processing;	
	<i>(aa) respect for consumer rights;</i>		
		<i>(aa) the legitimate interests pursued by controllers in specific contexts;</i>	
(b) the collection of data;	(b) the collection of data;	(b) the collection of data;	
		<i>(bb) the pseudonymisation of personal data;</i>	
(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 in the exercise of their rights <i>of data subjects;</i>	

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

		<p><i>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.</i></p>	
--	--	---	--

		<i>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.</i>	
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 <i>referred to in paragraph 1a</i> representing categories of controllers or processors in one Member State which intend to draw up <i>prepare a</i> codes of conduct or to amend or extend an existing codes, of conduct may <i>shall</i> submit them to an opinion of <i>draft code to the</i>	

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

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

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

		<i>Article 38a</i>	
		<i>Monitoring of approved codes of conduct</i>	
		<i>1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 52 and 53, the monitoring of compliance with a code of conduct pursuant to Article 38 (1b), may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for this purpose by the competent supervisory authority.</i>	
		<i>2. A body referred to in paragraph 1 may be accredited for this purpose if:</i>	
		<i>(a) it has demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority;</i>	

		<i>(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;</i>	
		<i>(c) it has established procedures and structures to deal with complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make these procedures and structures transparent to data subjects and the public;</i>	
		<i>(d) it demonstrates to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.</i>	
		<i>3. The competent supervisory authority shall submit the draft criteria for accreditation of a body referred to in paragraph 1 to the European Data Protection Board pursuant to the consistency mechanism referred to in Article 57.</i>	

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

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

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

	<i>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.</i>		
	<i>1b. The certification shall be voluntary, affordable, and available via a process that is transparent and not unduly burdensome.</i>		
	<i>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.</i>		
	<i>1d. During the certification procedure, the supervisory authorities 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</i>		

	<i>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.</i>		
	<i>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".</i>		
	<i>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.</i>		
	<i>1g. Notwithstanding paragraph 1f, the certification shall be valid for maximum five years.</i>		

	<i>1h. 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 public.</i>		
	<i>1i. The European Data Protection Board may on its own initiative certify that a data protection-enhancing technical standard is compliant with this Regulation.</i>		
2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the data protection certification mechanisms referred to in paragraph 1, including conditions for granting and withdrawal, and requirements for recognition within the Union and in third countries.	2. The Commission shall be empowered to adopt, <i>after requesting an opinion of the European Data Protection Board and consulting with stakeholders, in particular industry and non-governmental organisations,</i> delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the data protection certification mechanisms referred to in paragraph 1 <i>paragraphs 1a to 1h,</i> including <i>requirements for accreditation of auditors,</i> conditions for granting and withdrawal, and requirements for	<i>[Moved and modified under Article 39a point 7]</i>	

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

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

		<i>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.</i>	
		<i>5. The European Data Protection Board shall collect all certification mechanisms and data protection seals in a register and shall make them publicly available through any appropriate means, such as through the European E-Justice Portal.</i>	

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

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

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

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

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

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