Amendments VNO-NCW and MKB Nederland concerning Articles 28 to 39 Regulation

Article 28 **Documentation**	**Article 28** **Documentation**
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 or, if any, the controller's representative,~~ shall maintain ~~documentation~~ **an overview** of all processing operations under its responsibility, **which pose a high degree of risk to the fundamental rights of the data subjects, in particular their right to privacy, pursuant to the outcome of the privacy impact assessment as referred to in article 33.**
2. The documentation shall contain at least the following information: (a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any; (b) the name and contact details of the data protection officer, if any; (c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1); (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; (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; (g) a 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).	2. The ~~documentation~~ **overview** shall contain at least the following information: (a) the name ~~and contact details~~ of the controller, or any joint controller or processor, and of the representative, if any; ~~(b) the name and contact details of the data protection officer, if any;~~ (c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1); (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; (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; (g) a 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).
3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority.	3. The controller ~~and the processor and~~ or, if any, the controller's representative, shall make the documentation 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: (a) a natural person processing personal data without a commercial interest; or (b) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities.	4. The obligations referred to in paragraphs 1 and 2 shall not apply to ~~the following controllers and processors:~~ ~~(a)~~ a natural persons processing personal data without a commercial interest.~~; or~~ ~~(b) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities.~~
5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the documentation 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.	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.
6. The Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	6. 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).

	Justification *VNO-NCW believes that the organisational size criterion (>250 employees) is not useful to differentiate between organisations with respect to the scope of this article. Instead, a* ***risk-based approach*** *in Article 28 would be better suited to achieve the goals of this Regulation, similar to the notification requirement of article 18 of the current Directive, which this article replaces. The Directive allows for the exemption of a wide range of processing categories, which do not pose a significant risk for the fundamental rights of the data subject. It is consistent therefore to allow also for a similar exemption with regard to the documentation requirements under article 28 and to limit those to processing that poses a high degree of risk. Although organisations with a high maturity level in compliance and risk management would consider the documentation of data processing sound risk management, requiring all organisations to document each and every form of data processing taking place in the organisation (from the main customer database down to the secretary's birthday list) would place an excessive and disproportional burden on organisations, and would not be consistent with the statements of the Commission with regard to implementation cost. In order to determine a high degree of risk, reference is made to the privacy impact assessment of Article 33. When the privacy impact assessment indicates a high degree of risk, the documentation obligation is triggered.* *Moreover, VNO-NCW believes that this obligation should only apply to controllers, and not to processors, in order to avoid duplication of work. Not only does the controller have an overall responsibility with regard to compliance, the controller should also understand the processing on the part of the processor, and should therefore require processors, though the processor contract or otherwise, to provide the information relevant to the documentation obligation of the controller. Also, the role of the representative, in view of its dependency to the controller's compliance, should only be required to make the documentation available to the supervisory authority and not have a documentation requirement of its own.*
Article 29 **Co-operation with the supervisory authority** 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. 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.	**Article 29** **Co-operation with the supervisory authority** 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. 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. **3. Where the supervisory authority requires the cooperation of a processor, the supervisory authority shall allow the relevant controller or controllers to protect their**

	interests. *Justification:* *The duty to cooperate with the supervisory authority on the part of the processor should not deprive the controller from its legal rights to protect its interests with respect to compliance with this Regulation vis-à-vis the supervisory authority.*
Article 30 **Security of processing** 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. 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. 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. 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: (a) prevent any unauthorised access to personal data; (b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data; (c) ensure the verification of the lawfulness of processing operations. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	**Article 30** **Security of processing** 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. 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 **access, use,** disclosure, dissemination ~~or access~~, or alteration of personal data. 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. 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: (a) prevent any unauthorised access to personal data; (b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data; (c) ensure the verification of the lawfulness of processing operations. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2). *Justification (par. 1)* *There should be clarity on who is ultimately responsible for determining the required security measures in any processing of personal data. Making both the controller and the processor responsible for implementing appropriate security measures, would not only distort the commercial negotiation process between controller and processors (as security measures implemented autonomously by processors increase costs for controllers), it also means that both sides of the table could have different views on what security measures would be considered "appropriate". Therefore, it is not desirable that both parties are responsible for the implementation of "appropriate security*

Comment [redacted] Opmerkingen in vergadering V&J. Suggestie V&J: lid 1 en 2 integreren a la art. 17 Richtlijn 95/46.

	measures". Furthermore, the processor is often not the appropriate party to make final choices about data security, as he may not even aware of the type of data that is processed or is not in a position to assess the various interests with respect to the data. Nevertheless, responsible processors may advise their customers (the controllers) on the possible security measures and the pros and cons of their implementation. However, such responsibility should not be codified in this Regulation for the reasons stated above. *Justification (par.2)* *Security is related to access, alteration, disclosure and loss of data, not to unlawful processing as such (e.g., processing without consent could also constitute unlawful processing, but security measures cannot prevent this).*
Article 31 **Notification of a personal data breach to the supervisory authority** 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.	**Article 31** **Notification of a personal data breach to the supervisory authority** 1. ~~**In the case of a personal data breach,**~~ **Where a personal data breach is likely to have a significant adverse effect on the rights and freedoms of the data subjects, especially their right to privacy,** the controller**, after having become aware of it,** shall without ~~**undue**~~ **unreasonable** 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.**~~
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 processor shall alert and inform the controller immediately after the establishment of a personal data breach. **3. The notification of a personal data breach shall not be required if the controller or the processor has implemented appropriate technological measures, which were applied to the data concerned by the personal data breach, such as measures which render the data unintelligible to any person who is not authorised to access it.** **4. In case of joint controllers or where the controller is part of a group of undertakings, the personal data breach may be notified by the main establishment, if any, or by any other controller or undertaking designated by the joint controllers or group of undertakings.** **5. Controllers shall notify the supervisory authority of the Member State in which they are established. Where the notification is carried out in accordance with paragraph 4, the supervisory authority of the Member State in which the controller responsible for the personal data breach is established shall be notified. Controllers which are not established on the territory of the European Union, shall notify the supervisory authority of the Member State in which their representative is established.**
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	6. The notification referred to in paragraphs 1 and 2 must at least: (a) describe the nature of the personal data breach including the categories and number of data subjects

concerned; (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; (d) describe the consequences of the personal data breach; (e) describe the measures proposed or taken by the controller to address the personal data breach.	concerned and the categories and **estimated** number of data records concerned; (b) communicate the identity and contact details of the ~~**data protection officer**~~ **controller** or other contact point where more information can be obtained; (c) recommend measures to mitigate the possible adverse effects of the personal data breach; (d) describe the consequences of the personal data breach; (e) describe the measures proposed or taken by the controller **or processor** to address the personal data breach.
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.	**7.** 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. **This obligation shall also apply to the processor insofar as he is responsible for the personal data breach.**
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.	**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 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.
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).	**9.** 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). ***Justification (par.1)*** *In order to maintain the proportionality between the administrative burden to notify the supervisory authority (and the data subject) and the risk which the personal data breach likely poses to the data subject and to avoid that trifle breaches, which pose little or no harm to data subject, are notified, the amendment limits the scope of the obligation to notify the supervisory authority to personal data breaches which are "likely to have a significant adverse effect on the rights and freedoms of the data subjects, especially their right to privacy". This risk could be determined by the execution of a risk assessment similar to the privacy impact assessment referred to in article 33 Pursuant to paragraph 8 (new), the Commission may adopt standards for the determination of such risk, e.g , similar to the standards for notifying product safety issues in the EU Furthermore, as the priority of the controller in case of a personal data breach should be to address the breach and to limit its consequences, the 24 hour time window for the notification is deleted and replaced by "without unreasonable delay". It's up to the supervisory authority to determine whether in a particular case the delay was reasonable.* *See also amendment to Article 32.* ***Justification (par. 3 new)***

	The use of encryption techniques significantly reduce – and in some cases even negate – the risk of a personal data breach to the rights and freedoms of the data subject. Therefore, in order to maintain the proportionality between the administrative burden to notify the supervisory authority and the risk which the personal data breach poses to the data subject, security breaches which involve encrypted data should not be notified to the supervisory authority. Moreover, the fact that the Commission's proposal excluded encrypted data from the notification obligation to the data subject, but not from the notification obligation to the supervisory authority, signifies unreasonable distrust in organisations and does not stimulate them to invest in encryption techniques to protect the data ***Justification (par. 4 new)*** *In order to avoid multiple notifications for the same personal data breach, the supervisory authority may be notified by the main establishment, which is likely to have the expertise, or by the controller designated by the group or joint controllers in case the controller responsible for the personal data breach is part of a group of companies or where multiple controller are responsible for the personal data breach* ***Justification (par. 5 new)*** *This amendment clarifies which supervisory authority must be notified. This amendment is especially important in cases where persons in multiple member states are affected by the data breach, as to avoid that the some breach must be notified in multiple member states, thus reducing the administrative burden.* ***Justification (par. 6 new)*** *- ad A. As the actual number of data records is often unknown, the controller should only notify an estimated number. This is especially important in view of the fact that incomplete notification may be fined pursuant to Article 79.* *- ad B. In case of a personal data breach, the supervisory authority should always contact the controller, and not bypass the controller and go directly to the DPO. However, if the controller so chooses, the DPO could be mentioned as contact person for the controller. However, this should not be codified.* Alternatief
Article 32 **Communication of a personal data breach to the data subject** 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.	**Article 32** **Communication of a personal data breach to the data subject** 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**~~ **unreasonable** delay, **unless this is factually impossible or would require a disproportionate effort on the part of the controller.** **2. In case of joint controllers or where the controller is part of a group of undertakings, the personal data breach may be communicated by the main establishment, if any, or by any other controller or undertaking designated by**

Commen[redacted]
Ingeval het amendement op 22(5) sneuvelt zou een apart amendement voor de melding van security breaches door regulated sectors kunnen worden overwogen:

Article 32b:
Regulated sectors
Articles 31 and 32 do not apply if and insofar as the controller is subject to an obligation to notify an independent sectorial supervisory authority by virtue of legislation based on sector specific Union law.

Justification
By virtue of Union Law, the national legislator, taking in to account the specific requirements for such a sector, may designate an independent sectorial supervisory authority as the competent authority to deal with security breaches in a specific sector. The proposal also aims at preventing overlapping obligations and conflicts between different supervisory authorities.

	the joint controllers or group of undertakings.
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).	**3.** 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~~**5**).
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.	4. **(deleted in favour of art. 31.3 new)**
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.	**5.** 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.
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.	**6.** 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.
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).	**7.** 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). *Justification (par.1):* *This amendment in the first sentence corresponds with the amendment to article 31(1). Furthermore, the controller should not be required to inform the data subjects in case the data subjects are unknown to the controller (e.g., in case of a loss of a security video tape) or in case of the notification would require a disproportionate effort on the part of the controller (e.g , in case the controller does not dispose of the contact details of the data subjects).* *Justification (par.2):* *(see justification to Article 31(4) new).* *Justification (par.4 new)* *As the notification to the data subject follows the notification to the supervisory authority per paragraph 32(1), the exception is no longer required if the amendment to Article 31(3)new is accepted*
Article 33 **Data protection impact assessment** 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	**Article 33** **~~Data protection~~ Privacy impact assessment** **1.** Where processing operations **are likely to** present **~~specific~~ high degree of risks** to the rights and freedoms of data subjects by virtue of their nature, their scope or their

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.	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~~ **the rights and freedoms of the data subjects, especially their right to privacy.**
2. The following processing operations in particular present specific risks referred to in paragraph 1: (a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual; (b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale; (c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale; (d) personal data in large scale filing systems on children, genetic data or biometric data; (e) other processing operations for which the consultation of the supervisory authority is required pursuant to point (b) of Article 34(2).	2. The following processing operations in particular present ~~specific~~ **high** risks referred to in paragraph 1: (a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual; (b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale; (c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale; (d) personal data in large scale filing systems on children, genetic data or biometric data; (e) **(deleted in view of amendment to article 34(2)(b).)**
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.	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.
4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.	**4. (deleted)**
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.	4. Where the controller is a public authority or body and where the processing results from a legal obligation pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing operations and regulated by Union law, paragraphs 1 to 4 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.
6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro,	5. 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.~~ **encourage, in particular at the** European

small and medium-sized enterprises. 7. The Commission may specify standards and procedures for carrying out and verifying and auditing the assessment referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	**level, the establishment of common criteria for privacy impact assessments, taking into account the specific features of the various sectors, the size of the enterprises and the different processing operations. ~~In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.~~** 6. 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). *Justification (par. 1):* *The amendments to Articles 28 and 35 introduce a risk-based approach to the obligation to document data processing operations and the appointment of a data protection officer. Only in case of high risk to the rights and freedoms of the data subject, those obligations are triggered. Therefore, Article 33(1) is amended to reflect those changes.* *Moreover, unlike the Commission proposed, the assessment should be on the risk to the rights and freedoms of the data subject and not on the personal data, as the risk assessment with respect to the personal data would be part of a security risk assessment to determine the safeguards pursuant to Article 30. Furthermore, given the changes made to paragraph 1, the risk assessment should be performed by the controller and cannot be performed by the processor. Also, any risk is "specific", but what is important is whether the risk is high. The factor "likely to present" is added as the risks may be mitigated following the conclusions of the PIA. The factor assumes that risks exist irrespective of any mitigation.* *See also the amendments to articles 28, 34 and 35.* ***Justification (par. 4 - deleted)*** *In many cases it is factually impossible to seek the views of the data subjects (e.g., in case the controller starts something from scratch and does not already dispose of the personal data). Therefore, the requirement is deleted. Of course, in some cases, the intent of paragraph 4 is accomplished via other legally required procedures, such as the consultation of works councils with regard to employee privacy issues subject to labour law requirements. In such cases, the paragraph 4 would not add any value.* ***Justification (par. 5 new)*** *As data processing operations may differ from sector to sector and from organisation to organisation, a lot of flexibility is needed with regard to the way privacy impact assessments are performed. However, in order to ensure that the PIAs in the various sectors and organisations are comparable with respect to their quality (especially in view of the amendments to articles 28 and 35), the Commission should encourage the development of standards rather than have the power to adopt delegated acts. Standards may be developed as part of self-regulation in sectors or organisations, and the Commission should provide guidance as to the criteria for PIAs.*

Article 34 **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.	**Article 34** **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.
2. The controller or processor acting on the controller's behalf shall consult the supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where: (a) a data protection impact assessment as provided for in Article 33 indicates that processing operations are by virtue of their nature, their scope or their purposes, likely to present a high degree of specific risks; or (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.	2. The controller ~~or processor acting on the controller's behalf~~ shall ~~consult~~ **obtain from** the supervisory authority **authorisation** prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where: (a) a ~~data protection~~ **privacy** 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, **which cannot be mitigated.** ~~; or~~ (b) **(deleted, as it is impacts the European level playing field).**
3. Where the supervisory authority is of the opinion that the intended processing does not comply with this Regulation, in particular where risks are insufficiently identified or mitigated, it shall prohibit the intended processing and make appropriate proposals to remedy such incompliance.	3. Where the supervisory authority is of the opinion that the intended processing does not comply with this Regulation, in particular where risks are insufficiently identified or mitigated, it shall prohibit the intended processing and make appropriate proposals to remedy such incompliance.
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. (deleted in view of deletion art. 2(b))**
5. Where the list provided for in paragraph 4 involves processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour, or may substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57 prior to the adoption of the list.	**5. (deleted in view of deletion par. 2(b))**
6. The controller or processor shall provide the supervisory authority with the data protection impact assessment provided for in Article 33 and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.	6. The controller ~~or processor~~ shall provide the supervisory authority with the data protection impact assessment provided for in Article 33 and, 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.
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	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

Comment [redacted]: V&J suggereert om dit lid helemaal te schrappen.

legislative measure, which defines the nature of the processing, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects. 8. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for determining the high degree of specific risk referred to in point (a) of paragraph 2. 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).	legislative measure, which defines the nature of the processing, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects. 8. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for determining the high degree of specific risk referred to in point (a) of paragraph 2. 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). *Justification (par 1):* *Deleted wording is superfluous.* *Justification (par. 2):* *The requirement to 'consult' with the supervisory authority has undesired consequences, as a consultation bears no legal meaning nor does it create legal certainty. In theory, a controller would be allowed to disregard the advice of the supervisory authority, but in practice such decision would be impossible. Furthermore, the supervisory authority is not a consultant. Therefore, the obligation to consult has been amended to an obligation to obtain an authorization. Furthermore, in order to reduce the administrative burden, the authorisation should only be sought in cases where the controller cannot mitigate the risks. In other words, the residual risks are high. Normally, in risk management procedures residual risks are accepted by management, but Article 34(2) requires such risk acceptance to be performed by the supervisory authority in the form of an authorisation (e.g., a permit) instead.* *Paragraph 2(b) has been deleted in order to maintain a level playing field between the Member States as well as to reduce the administrative burden with regard to ex-ante enforcement.*
Article 35 **Designation of the data protection officer** 1. The controller and the processor shall designate a data protection officer in any case where: (a) the processing is carried out by a public authority or body; or (b) the processing is carried out by an enterprise employing 250 persons or more; or (c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.	**Article 35** **Designation of the data protection officer** 1. The controller **~~and the processor~~** shall designate a data protection officer in any case where: (a) the processing is carried out by a public authority or body; or (b) the processing is carried out by an **enterprise ~~employing 250 persons or more~~ and the outcome of any privacy impact assessment as referred to in article 33, has indicated that a high degree of risk to the rights and freedoms of data subjects especially their right to privacy, exists**; or (c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects. **In all other cases, the designation of a data protection officer is optional.**

2. In the case referred to in point (b) of paragraph 1, a group of undertakings may appoint a single data protection officer.	2. In the case referred to in point (b) of paragraph 1, a group of undertakings may appoint a single data protection officer.
3. Where the controller or the processor is a public authority or body, the data protection officer may be designated for several of its entities, taking account of the organisational structure of the public authority or body.	3. Where the controller or the processor is a public authority or body, the data protection officer may be designated for several of its entities, taking account of the organisational structure of the public authority or body.
4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may designate a data protection officer.	4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may designate a data protection officer.
5. The controller or processor shall designate the data protection officer on the basis of professional qualities and, in particular, expert knowledge of 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. (deleted, move to recitals)**
6. The controller or the processor shall ensure that any other professional duties of the data protection officer are compatible with the person's tasks and duties as data protection officer and do not result in a conflict of interests.	6. The controller or the processor shall ensure that any other professional duties of the data protection officer are compatible with the person's tasks and duties as data protection officer and do not result in a conflict of interests.
7. The controller or the processor shall designate a data protection officer for a period of at least two years. The data protection officer may be reappointed for further terms. During their term of office, the data protection officer may only be dismissed, if the data protection officer no longer fulfils the conditions required for the performance of their duties.	7. ~~The controller or the processor shall designate a data protection officer for a period of at least two years. The data protection officer may be reappointed for further terms.~~ During their term of office, the data protection officer may only be dismissed, if the data protection officer no longer fulfils the conditions required for the performance of their duties.
8. The data protection officer may be employed by the controller or processor, or fulfil his or her tasks on the basis of a service contract.	8. The data protection officer may be employed by the controller ~~or processor,~~ or fulfil his or her tasks on the basis of a service contract.
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~~.
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. (deleted)**
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.	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. ***Justification (par 1):*** *VNO-NCW believes that the organisational size criterion (>250 employees) is not useful to differentiate between organisations with respect to the scope of this article. Instead, a risk-based approach in Article 35 would be better suited to achieve the goals of this Regulation. Therefore, the*