MKB-Nederland[1]
Registration number: 05673984520-73

VNO-NCW[2]
Registration number: 13255254129-80

Data Protection Regulation **Amendments proposed by VNO-NCW and MKB Nederland**	
Original Text	Amendment and Explanation
Recital (1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty lay down that everyone has the right to the protection of personal data concerning him or her.	
Recital (2) The processing of personal data is designed to serve man; the principles and rules on the protection of individuals with regard to the processing of their personal data should, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably their right to the protection of personal data. It should contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, the strengthening and the convergence of the economies within the internal market, and the well-being of individuals.	
Recital (3) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to guarantee the free flow of personal data between Member States.	
Recital (4) The economic and social integration resulting from the functioning of the internal market has led to a substantial increase in cross-border flows. The exchange of data between economic and social, public and private actors across the Union increased. National authorities in the Member States are being called upon by Union law to cooperate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State.	
Recital (5) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of data sharing and collecting has increased	

[1] Confederation of Netherlands Industry VNO-NCW, Bezuidenhoutseweg 12, PO Box, 93002 2509 AA The Hague, Netherlands. Contact: [redacted]

[2] Confederation of SME-Netherlands (MKB-Nederland), Bezuidenhoutseweg 12, PO Box, 93002 2509 AA The Hague, Netherlands. Contact [redacted]

spectacularly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Individuals increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and requires to further facilitate the free flow of data within the Union and the transfer to third countries and international organisations, while ensuring an high level of the protection of personal data.	
Recital (6) These developments require building a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance to create the trust that will allow the digital economy to develop across the internal market. Individuals should have control of their own personal data and legal and practical certainty for individuals, economic operators and public authorities should be reinforced.	
Recital (7) The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the way data protection is implemented across the Union, legal uncertainty and a widespread public perception that there are significant risks for the protection of individuals associated notably with online activity. Differences in the level of protection of the rights and freedoms of individuals, notably to the right to the protection of personal data, with regard to the processing of personal data afforded in the Member States may prevent the free flow of personal data throughout the Union. These differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. This difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC.	
Recital (8) In order to ensure consistent and high level of protection of individuals and to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union.	
Recital (9) Effective protection of personal data throughout the Union requires strengthening and detailing the rights of data subjects and the obligations of those who process and determine the processing of personal data, but also equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for offenders in the Member States.	
Recital (10) Article 16(2) of the Treaty mandates the European	

Parliament and the Council to lay down the rules relating to the protection of individuals with regard to the processing of personal data and the rules relating to the free movement of personal data.	
Recital (11) In order to ensure a consistent level of protection for individuals throughout the Union and to prevent divergences hampering the free movement of data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide individuals in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective co-operation by the supervisory authorities of different Member States. To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a number of derogations. In addition, the Union institutions and bodies, Member States and their supervisory authorities are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation. The notion of micro, small and medium-sized enterprises should draw upon Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises.	**Recital (11)** In order to ensure a consistent level of protection for individuals throughout the Union and to prevent divergences hampering the free movement of data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide individuals in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective co-operation by the supervisory authorities of different Member States. ~~**To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a number of derogations**~~ **The level of protection of personal data and the measures to be taken by the controller or the processor should not be dependent on the size of the enterprise processing the personal data, but on the risk posed by such processing**. ~~**In addition**~~ **However**, the Union institutions and bodies, Member States and their supervisory authorities are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation. The notion of micro, small and medium-sized enterprises should draw upon Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises. *Justification:* *This amendment speaks for itself. It also matches the risk-based approach as proposed by VNO-NCW in the relevant articles. The special needs of SME's should be taken into account when applying the Regulation, not in the Regulation itself.*
Recital (12) The protection afforded by this Regulation concerns natural persons, whatever their nationality or place of residence, in relation to the processing of personal data. With regard to the processing of data which concern legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person, the protection of this Regulation should not be claimed by any person. This should also apply where the name of the legal person contains the names of one or more natural persons.	**Recital (12)** The protection afforded by this Regulation concerns natural persons, whatever their nationality or place of residence, in relation to the processing of personal data. With regard to the processing of data which concern **enterprises** ~~**legal persons and in particular undertakings established as legal persons**~~, including the name and the form of the ~~**legal person**~~ **enterprise** and the contact details of the ~~**legal person**~~ **enterprise**, the protection of this Regulation should not be claimed by any person. This should also apply where the name of the ~~**legal person**~~ **enterprise** contains the names of one or more natural persons. *Justification:* *The protection of data relating to a business, such as turn-over, profit, details about business operations or business assets, place of business, business contact details, etc., should not be dependent on the legal form of the business.*
Recital (13) The protection of individuals should be technologically	

neutral and not depend on the techniques used; otherwise this would create a serious risk of circumvention. The protection of individuals should apply to processing of personal data by automated means as well as to manual processing, if the data are contained or are intended to be contained in a filing system. Files or sets of files as well as their cover pages, which are not structured according to specific criteria, should not fall within the scope of this Regulation.	
Recital (14) This Regulation does not address issues of protection of fundamental rights and freedoms or the free flow of data related to activities which fall outside the scope of Union law, nor does it cover the processing of personal data by the Union institutions, bodies, offices and agencies, which are subject to Regulation (EC) No 45/2001, or the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union.	
Recital (15) This Regulation should not apply to processing of personal data by a natural person, which are exclusively personal or domestic, such as correspondence and the holding of addresses, and without any gainful interest and thus without any connection with a professional or commercial activity. The exemption should also not apply to controllers or processors which provide the means for processing personal data for such personal or domestic activities.	**Recital (15)** This Regulation should not apply to processing of personal data by a natural person, which are ~~exclusively~~ personal or domestic, such as correspondence and the holding of addresses, ~~and without any gainful interest and thus without any connection with a professional or commercial activity~~ **or to processing of personal data in the context of activities, which cannot be considered to constitute an enterprise, such as the (occasional) selling of goods or the provision of (occasional) services for a fee without the intention of making a profit**. The exemption should ~~also~~ not apply to controllers or processors which provide the means for processing personal data for such personal or domestic activities. *Justification:* *This amendment matches the amendment to Article 2(2).*
Recital (16) The protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, is subject of a specific legal instrument at Union level. Therefore, this Regulation should not apply to the processing activities for those purposes. However, data processed by public authorities under this Regulation when used for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties should be governed by the more specific legal instrument at Union level (Directive XX/YYY).	
Recital (17) This Regulation should be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.	
Recital (18) This Regulation allows the principle of public access to official documents to be taken into account when applying	

the provisions set out in this Regulation.	
Recital (19) Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union or not. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in this respect.	**Recital (19)** Any processing of personal data in the context of the activities of an establishment of a controller, ~~or~~ a processor **or an enterprise** in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union or not. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in this respect. *Justification:* *This amendment matches the amendment to article 3.1.*
Recital (20) In order to ensure that individuals are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects residing in the Union by a controller not established in the Union should be subject to this Regulation where the processing activities are related to the offering of goods or services to such data subjects, or to the monitoring of the behaviour of such data subjects.	**Recital (20)** In order to ensure that individuals are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects residing in the Union by a controller not established in the Union should be subject to this Regulation where the processing activities are related to the offering of goods or services **directed** to such data subjects, or to the monitoring of the behaviour of such data subjects. *Justification:* *This amendment matches the amendment to Article 3(2).*
Recital (21) In order to determine whether a processing activity can be considered to 'monitor the behaviour' of data subjects, it should be ascertained whether individuals are tracked on the internet with data processing techniques which consist of applying a 'profile' to an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.	
Recital (22) Where the national law of a Member State applies by virtue of public international law, this Regulation should also apply to a controller not established in the Union, such as in a Member State's diplomatic mission or consular post.	
Recital (23) The principles of protection should apply to any information concerning an identified or identifiable person. To determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the individual. The principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.	**Recital (23)** The principles of protection should apply to any information concerning an identified or identifiable person. To determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller ~~**or by any other person**~~ to identify the individual. The principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer **directly** identifiable **by the controller, the processor, or a third party, which accesses the data, including, where possible, the use of measures shielding the data subject's identity or the encryption of the data.** *Justification:* *This amendment matches the amendment to Article 4(1). 'Or by any other person' is too broad. It would mean that*

	data, which cannot be identified by the controller using reasonable means, still have to be treated as personal data because there might be a person out there who could identify the data subject. This would put an unreasonable compliance burden on the 'controller'. *Furthermore, the Regulation should also not apply to the processing of encrypted data or data which have been pseudomised, if the party processing the data has no reasonable means to directly identify the individual from the data. For instance because such party does not have access to the key. This allows for controller to engage high-secure service providers and high-security technologies, such as providers of encrypted cloud storage, without having to deal with the burden of compliance with the Regulation with regard to the use of such services.*
Recital (24) When using online services, individuals may be associated with online identifiers provided by their devices, applications, tools and protocols, such as Internet Protocol addresses or cookie identifiers. This may leave traces which, combined with unique identifiers and other information received by the servers, may be used to create profiles of the individuals and identify them. It follows that identification numbers, location data, online identifiers or other specific factors as such need not necessarily be considered as personal data in all circumstances.	
Recital (25) Consent should be given explicitly by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or inactivity should therefore not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.	**Recital (25)** Consent should be given ~~**explicitly by any appropriate method enabling a**~~ freely **given, and should constitute a** specific and informed indication of the data subject's ~~**wishes**~~ **will with respect to the data processing**, either by a statement or by ~~**a clear affirmative**~~ **an** action by the data subject. **Where appropriate, consent should be given by a method, which** ~~**ensuring**~~ **ensures** that individuals are aware that they give their consent to the processing of personal data, including**, but not limited to,** by ticking a box when visiting an Internet website or by any other statement or conduct**,** which clearly indicates in ~~**this**~~ **the** context **and the circumstances of the case at the time consent is required** the data subject's acceptance of the ~~**proposed**~~ processing of ~~**their**~~ **his** personal data. Silence or inactivity**, such as not opting out from the data processing,** should therefore not constitute consent. Consent ~~**should cover**~~ **covers** all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided. ***Justification:*** *This amendment matches the amendment to article 4(8). It leaves open the possibility of 'implied consent', which can be deferred from the data subject's actions, where relevant based on the circumstances and the information available to the data subject at the time consent is required.* *Examples of implied consent to the processing of personal data are:* - *submitting an online registration form,* - *sending an e-mail to a customer service centre,* - *exchanging business cards,*

	- *submitting a photo for use in a directory,* - *posting a CV on a job search website.* *In such situations, it would be unreasonably burdensome to require explicit consent, as proposed by the Commission.* *Implied consent does not include silence, such as not unticking pre-ticked boxes or not responding to a possibility to opt-out.*
Recital (26) Personal data relating to health should include in particular all data pertaining to the health status of a data subject; information about the registration of the individual for the provision of health services; information about payments or eligibility for healthcare with respect to the individual; a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; any information about the individual collected in the course of the provision of health services to the individual; information derived from the testing or examination of a body part or bodily substance, including biological samples; identification of a person as provider of healthcare to the individual; or any information on e.g. a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, such as e.g. from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test.	
Recital (27) The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes, conditions and means of processing through stable arrangements. This criterion should not depend whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore no determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union.	**Recital (27)** The main establishment of ~~**a controller**~~ **a group of undertakings** in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the ~~**purposes, conditions and means of**~~ **data** processing through stable arrangements. This criterion **shall apply to both data controllers and data processors and** should not depend whether the processing of personal data is actually carried out at that location; the presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute such main establishment and are therefore no determining criteria for a main establishment. **Where the global or European headquarters of a group of undertakings is established on the territory of the European Union, such headquarters shall be deemed the main establishment for the purposes of this Regulation. Alternatively, where an entity established on the territory of the European Union has delegated data protection responsibilities with respect to data processing within the group of undertakings, such group company shall be deemed the main establishment for the purposes of this Regulation. Delegated data protection responsibilities may be inferred from formal arrangements between group companies as well as management decisions or other measures indicating the intention to centralise data protection responsibilities within the enterprise or group of undertakings, such as the appointment of a group data protection officer or the designation of group compliance responsibilities. Alternatively, the legal entity, which takes the most decisions in terms of purposes and means of data processing in group companies established in**

	multiple Member States or the group company which is best placed (in terms of management function, administrative burden etc.) to deal with the application and to enforce the group's compliance framework, like the group's binding corporate rules, may be deemed the main establishment for the purposes of this Regulation. Priority should be given to the place of establishment of the global or European headquarters of the group of undertakings on the territory of the European Union. ~~**The main establishment of the processor should be the place of its central administration in the Union.**~~ *Justification:* - *It's not the controller (which is term defined by this Regulation), but a group of undertakings which has a main establishment in the EU.* - *The relevant criteria to determine the main establishment under the BCR-regime (WP 107) have been inserted into the recital for purpose of clarity.* - *By inserting the BCR-criteria, there is no need for a specific definition of main establishment of the processor.*
Recital (28) A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exercise a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented.	
Recital (29) Children deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data. To determine when an individual is a child, this Regulation should take over the definition laid down by the UN Convention on the Rights of the Child.	**Recital (29)** Children deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data. ~~**To determine when an individual is a child, this Regulation should take over**~~ **At the same time, given the higher average use of communication technologies by younger generations, a distinction shall be made between** the definition laid down by the UN Convention on the Rights of the Child **and the "minor age" criterion.** *Justification:* *Children, especially adolescents, are using the Internet, often in a very tech-savvy way. The protection sought after by the Commission's proposal should apply to the very young children. This amendment reflects the amendment to article 8.*
Recital (30) Any processing of personal data should be lawful, fair and transparent in relation to the individuals concerned. In particular, the specific purposes for which the data are processed should be explicit and legitimate and determined at the time of the collection of the data. The data should be adequate, relevant and limited to the minimum necessary for the purposes for which the data are processed; this requires in particular ensuring that the data collected are not excessive and that the period for which the data are stored is limited to a strict minimum. Personal data should only be processed if the purpose of the processing could not be fulfilled by other means. Every reasonable step	**Recital (30)** Any processing of personal data should be lawful, fair and transparent in relation to the individuals concerned. In particular, the specific purposes for which the data are processed should be explicit and legitimate and determined at the time of the collection of the data. The data should be adequate, relevant and limited to the minimum necessary for the purposes for which the data are processed; this requires in particular ensuring that the data collected are not excessive and that the period for which the data are stored is limited to a strict minimum. Personal data should only be processed if the purpose of the processing could not be fulfilled by other means. Every reasonable step

should be taken to ensure that personal data which are inaccurate are rectified or deleted. In order to ensure that the data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.	should be taken to ensure that personal data which are inaccurate are rectified or deleted. In order to ensure that the data are not kept longer than necessary, time limits should be established by the controller for erasure ~~or for a periodic review~~**, where possible**. *Justification:* *As data retention depends on the purposes of the processing and the often the controller does not know upfront how long such purposes will continue to exist (e.g., in case of a customer relationship or employment relationship), it is also not possible to establish time limits for the retention of the data in all cases.*
Recital (31) In order for processing to be lawful, personal data should be processed on the basis of the consent of the person concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation.	**Recital (31)** In order for processing to be lawful, personal data should be processed on the basis of ~~the consent of the person concerned or some other~~ **a** legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation. *Justification:* *Consent is only one of six basis to process personal data, which are all equal. The deletion removes the impression that consent would be more important than the other processing grounds mentioned in art. 6.1 (quod non).*
Recital (32) Where processing is based on the data subject's consent, the controller should have the burden of proving that the data subject has given the consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware that and to what extent consent is given.	**Recital (32)** Where processing is based on the data subject's consent, the controller should have the burden of proving that the data subject has given the consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware that and to what extent consent is given**, such as the capitalising or highlighting of the relevant provision in online terms and conditions**. *Justification:* *The information available to the data subject at the time consent is required, is an important factor whether or not the controller may rely on consent. This addition provides a practical example how to achieve the clarity of the consent clause in any Terms & Conditions.*
Recital (33) In order to ensure free consent, it should be clarified that consent does not provide a valid legal ground where the individual has no genuine and free choice and is subsequently not able to refuse or withdraw consent without detriment.	
Recital (34) Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context. Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the	**Recital (34)** Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context. Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the

consent cannot be deemed as freely given, taking into account the interest of the data subject.	consent cannot be deemed as freely given, taking into account the interest of the data subject. **However, consent should always be a valid legal ground where Union or Member State law has made the data subject's consent a specific condition for a specific type of processing of the personal data or set of processing operations or where the purpose or purposes of the processing of the personal data is in the interest of the data subject, regardless of any imbalance between the parties.** *Justification:* *The imbalance should not be a problem in case the processing is required by Union or Member State law as a specific condition for the processing (other than article 6.1). E.g., the Dutch Medical Examinations Act requires employee consent for the disclosure of a medical report prepared by the company doctor to the employer.* *Furthermore, consent should be possible where the purpose of the processing is in the interest of the data subject. E.g., an employer should be allowed to ask the consent of an expat to disclose his personal data to a tax advisor or moving company, paid for by the employer. In this example, the tax advisor or moving company are controllers of the personal data as they render their services directly to the employee. This means that the disclosure needs a basis in article 6.1 of this Regulation. Because the use of such services cannot be made a condition of the expat contract under labour law and the disclosure cannot be based on any other processing basis as mentioned in article 6.1 except consent, the expat's consent would be required in such case.*
Recital (35) Processing should be lawful where it is necessary in the context of a contract or the intended entering into a contract.	**Recital (35)** Processing should be lawful where it is necessary in the context of a contract or the intended entering into a contract. **In such case, (additional) consent of the data subject for the same processing shall not be required.** *Justification:* *Often, controllers ask data subject for their consent for the processing of the personal data in the context of a service in order to be sure they have a basis for the processing of the personal data. This happens especially in online environments. In such situation, consent is neither legally required per Article 6.1(b), nor is it sound business practice, as for example a withdrawal of consent to process the personal data would in most cases also imply the termination of the contract. However, termination of contracts is and should not be subject to the legal basis for processing of personal data, but is governed by the terms & conditions of the service and applicable contract law. To avoid that controllers make such mistakes and to avoid false expectations with data subjects, this amendment clarifies that consent is not required if the data are processed in the context of a contract.*
Recital (36) Where processing is carried out in compliance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority, the processing should have a legal basis in Union law, or in a Member State law which meets the requirements of the Charter of Fundamental Rights of the	

European Union for any limitation of the rights and freedoms. It is also for Union or national law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public administration or another natural or legal person governed by public law, or by private law such as a professional association.	
Recital (37) The processing of personal data should equally be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's life.	
Recital (38) The legitimate interests of a controller may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding. This would need careful assessment in particular where the data subject is a child, given that children deserve specific protection. The data subject should have the right to object the processing, on grounds relating to their particular situation and free of charge. To ensure transparency, the controller should be obliged to explicitly inform the data subject on the legitimate interests pursued and on the right to object, and also be obliged to document these legitimate interests. Given that it is for the legislator to provide by law the legal basis for public authorities to process data, this legal ground should not apply for the processing by public authorities in the performance of their tasks.	**Recital (38)** The legitimate interests of a controller may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding. This would need careful assessment in particular where the data subject is a child, given that children deserve specific protection. The data subject should have the right to object **to** the processing, on grounds relating to their particular situation and free of charge. To ensure transparency, the controller should be obliged to ~~**explicitly**~~ inform the data subject on the legitimate interests pursued and on the right to object, and also be obliged to document these legitimate interests **insofar the processing poses a high risk to the interests and fundamental rights and freedoms of the data subject**. Given that it is for the legislator to provide by law the legal basis for public authorities to process data, this legal ground should not apply for the processing by public authorities in the performance of their tasks. *Justification:* - *The addition of 'to' is a technical addition.* - *The deletion of 'explicit' is mean to ensure that controller may inform the data subjects via the publication of privacy notices without having to verify whether the data subject has actually accessed or read them.* - *The addition matches the risk-based approach proposed by VNO-NCW in article 28.*
Recital (39) The processing of data to the extent strictly necessary for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, and the security of the related services offered by, or accessible via, these networks and systems, by public authorities, Computer Emergency Response Teams – CERTs, Computer Security Incident Response Teams – CSIRTs, providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the concerned data controller. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.	**Recital (39)** The processing of data to the extent strictly necessary for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, and the security of the related services offered by, or accessible via, these networks and systems, by public authorities, Computer Emergency Response Teams – CERTs, Computer Security Incident Response Teams – CSIRTs, providers of electronic communications networks and services and by providers of security technologies and services, constitutes**, among others,** a legitimate interest of the ~~**concerned**~~ data controller. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.

	Justification: *- The addition clarifies that the interests described in Recital 39 are not the only legitimate interests of the controller, which allow processing on the basis of article 6.1(f).* *- The deletion clarifies that this is not about controllers who are worried.*
Recital (40) The processing of personal data for other purposes should be only allowed where the processing is compatible with those purposes for which the data have been initially collected, in particular where the processing is necessary for historical, statistical or scientific research purposes. Where the other purpose is not compatible with the initial one for which the data are collected, the controller should obtain the consent of the data subject for this other purpose or should base the processing on another legitimate ground for lawful processing, in particular where provided by Union law or the law of the Member State to which the controller is subject. In any case, the application of the principles set out by this Regulation and in particular the information of the data subject on those other purposes should be ensured.	**Recital (40)** The processing of personal data for other purposes should be ~~only~~ allowed where the processing is compatible with those purposes for which the data have been initially collected **('further processing')**, in particular where the processing is necessary for historical, statistical**,** scientific **or applies** research purposes. **When determining the compatibility between the purpose for which the data were collected and the purposes of the further processing, the controller shall take into account: the relationship between the purpose of the intended processing and the purpose for which the data were obtained, the nature of the data concerned, the consequences of the further processing for the data subject, and the extent to which appropriate measures and safeguards have been put in place to protect the interests of the data subject.** ~~**Where the other purpose is not compatible with the initial one for which the data are collected, the controller should obtain the consent of the data subject for this other purpose or should base the processing on another legitimate ground for lawful processing, in particular where provided by Union law or the law of the Member State to which the controller is subject.**~~ **The further processing of personal data for non-compatible purposes shall only be allowed if the further processing is based on the consent of the data subject, is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract, is necessary for compliance with a legal obligation to which the controller is subject, or is necessary in order to protect the vital interests of the data subject.** In any case, the application of the principles set out by this Regulation and in particular the information of the data subject on those other purposes should be ensured. **Where the personal data are collected for two or more non-compatible purposes, such processing shall be allowed, provided such processing meets the requirements of this Regulation.** *Justification:* *- 'Only' has been transferred to the part of non-compatible purposes (former Article 6.4).* *- This Amendment provides the criteria for assessing compatibility between the purpose for which the data were collected and the purposes of the further processing. Such criteria are part of the current Dutch Personal Data Protection Act and have proven to be a very useful instrument to determine compatibility in practice.* *- Furthermore, as Article 6.4 makes clear, it is understood that further processing of personal data for non-compatible purposes is also allowed in case the further processing is based on consent, contact, compliance and vital interests. This is already implicitly understood in the Directive. VNO-NCW support the Commission in making this explicit in the Regulation. However, it should not be part of Article 6, but*

	of Article 5. Contrary to the Commission's proposal, VNO-NCW believes that further processing in the interest of public tasks of the controller should not be mentioned in the list of non-compatible purposes; instead such further processing should always meet the test of 'compatibility' as mentioned in the beginning of this Recital. *- The final sentence clarifies that it is possible to collect data for two or more non-compatible purposes.*
Recital (41) Personal data which are, by their nature, particularly sensitive and vulnerable in relation to fundamental rights or privacy, deserve specific protection. Such data should not be processed, unless the data subject gives his explicit consent. However, derogations from this prohibition should be explicitly provided for in respect of specific needs, in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.	
Recital (42) Derogating from the prohibition on processing sensitive categories of data should also be allowed if done by a law, and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where grounds of public interest so justify and in particular for health purposes, including public health and social protection and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for historical, statistical and scientific research purposes.	**Recital (42)** Derogating from the prohibition on processing sensitive categories of data should also be allowed if done by a law, and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where grounds of public interest so justify and in particular for health purposes, including public health and social protection and the management of health-care services, **such as IT, administration or financial services**, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the ~~**health**~~ insurance system, or for historical, statistical and scientific research purposes. **Healthcare management service providers, such as IT, administration or financial services, which require data concerning health for the purpose of providing their services to a healthcare professional or healthcare organisation, such as a hospital, may process such data on the basis of a processor contract.** *Justification:* *Insurers need and can process health data for the management of health care services and settling claims for the benefits and services in the health insurance system, as stated in this recital. However collecting and processing health data for other insurance purposes, such as personal injury, life, accident, and third party liabilities insurance is also necessary. The limitation to 'health insurance' is therefore too restrictive to serve the need of the insurance sector. This is explained further in article 9 paragraph 2(h). Furthermore, the requirement that health data may only be processed if authorized by law should not apply to processors in the healthcare sector. This amendment clarifies that the basis of their processing of health data is the processor contract. This means that healthcare management services are to be treated as the 'long arm' of the healthcare professional or healthcare organization and that the specific conditions of Article 81.1 do not apply to them.*
Recital (43) Moreover, the processing of personal data by official	

authorities for achieving aims, laid down in constitutional law or international public law, of officially recognised religious associations is carried out on grounds of public interest.	
Recital (44) Where in the course of electoral activities, the operation of the democratic system requires in a Member State that political parties compile data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established.	
Recital (45) If the data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. In case of a request for access, the controller should be entitled to ask the data subject for further information to enable the data controller to locate the personal data which that person seeks.	
Recital (46) The principle of transparency requires that any information addressed to the public or to the data subject should be easily accessible and easy to understand, and that clear and plain language is used. This is in particular relevant where in situations, such as online advertising, the proliferation of actors and the technological complexity of practice makes it difficult for the data subject to know and understand if personal data relating to them are being collected, by whom and for what purpose. Given that children deserve specific protection, any information and communication, where processing is addressed specifically to a child, should be in such a clear and plain language that the child can easily understand.	
Recital (47) Modalities should be provided for facilitating the data subject's exercise of their rights provided by this Regulation, including mechanisms to request, free of charge, in particular access to data, rectification, erasure and to exercise the right to object. The controller should be obliged to respond to requests of the data subject within a fixed deadline and give reasons, in case he does not comply with the data subject's request.	
Recital (48) The principles of fair and transparent processing require that the data subject should be informed in particular of the existence of the processing operation and its purposes, how long the data will be stored, on the existence of the right of access, rectification or erasure and on the right to lodge a complaint. Where the data are collected from the data subject, the data subject should also be informed whether they are obliged to provide the data and of the consequences, in cases they do not provide such data.	**Recital (48)** The principles of fair and transparent processing require that the data subject should be informed in particular of the existence of the processing operation and its purposes, **and of any other information, which guarantees a fair processing taking into account the circumstances. Such information may include, where appropriate,** how long the data will be stored, on the existence of the right of access, rectification or erasure and on the right to lodge a complaint. Where the data are collected from the data subject, the data subject should also be informed whether they are obliged to provide the data and of the consequences, in cases they do not provide such data.

	Justification: *This amendment matches the amendment to Article 14.1. Given the differences in data processing between sectors and well as processing situations, this amendment allows for some flexibility to provide an appropriate pallet of information to the data subject in order for him to be able to assess if he is subject to fair processing.*
Recital (49) The information in relation to the processing of personal data relating to the data subject should be given to them at the time of collection, or, where the data are not collected from the data subject, within a reasonable period, depending on the circumstances of the case. Where data can be legitimately disclosed to another recipient, the data subject should be informed when the data are first disclosed to the recipient.	
Recital (50) However, it is not necessary to impose this obligation where the data subject already disposes of this information, or where the recording or disclosure of the data is expressly laid down by law, or where the provision of information to the data subject proves impossible or would involve disproportionate efforts. The latter could be particularly the case where processing is for historical, statistical or scientific research purposes; in this regard, the number of data subjects, the age of the data, and any compensatory measures adopted may be taken into consideration.	
Recital (51) Any person should have the right of access to data which has been collected concerning them, and to exercise this right easily, in order to be aware and verify the lawfulness of the processing. Every data subject should therefore have the right to know and obtain communication in particular for what purposes the data are processed, for what period, which recipients receive the data, what is the logic of the data that are undergoing the processing and what might be, at least when based on profiling, the consequences of such processing. This right should not adversely affect the rights and freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of these considerations should not be that all information is refused to the data subject.	**Recital (51)** Any person should have the right of access to data which has been collected concerning them, and to exercise this right easily, in order to be aware and verify the lawfulness of the processing. Every data subject should therefore have the right to know and obtain communication in particular **the categories of personal data that are processed,** for what purposes the data are processed, for what period, which recipients receive the data, what is the logic of the data that are undergoing the processing and what might be, at least when based on profiling, the consequences of such processing. **The controller should not be required to provide a copy of the raw data or meta data.** This right should not adversely affect the rights and freedoms of others, including **the privacy rights of others, confidentiality in business operations,** trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of these considerations should not be that all information is refused to the data subject. **Where the request is vexatious, e.g. an abuse of right, or where the requests are manifestly excessive, the controller should have the right to deny a request**. *Justification:* *Raw data or meta data (like a raw dump of a database or technical log information) doesn't provide data subjects with added value in assessing if the processing is in accordance with the principles for data processing. Furthermore, the right of access should also be restricted if such access would infringe the privacy rights of others (e.g.,*

	if the data subject seeks access to a surveillance tape) or if the business operation requires confidentiality (e.g., promotion decisions or mergers & acquisitions). Moreover, controllers should be protected from abusive use of the right of access and therefore should in some cases have the right to deny certain requests.
Recital (52) The controller should use all reasonable measures to verify the identity of a data subject that requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the unique purpose of being able to react to potential requests.	
Recital (53) Any person should have the right to have personal data concerning them rectified and a 'right to be forgotten' where the retention of such data is not in compliance with this Regulation. In particular, data subjects should have the right that their personal data are erased and no longer processed, where the data are no longer necessary in relation to the purposes for which the data are collected or otherwise processed, where data subjects have withdrawn their consent for processing or where they object to the processing of personal data concerning them or where the processing of their personal data otherwise does not comply with this Regulation. This right is particularly relevant, when the data subject has given their consent as a child, when not being fully aware of the risks involved by the processing, and later wants to remove such personal data especially on the Internet. However, the further retention of the data should be allowed where it is necessary for historical, statistical and scientific research purposes, for reasons of public interest in the area of public health, for exercising the right of freedom of expression, when required by law or where there is a reason to restrict the processing of the data instead of erasing them.	**Recital (53)** Any person should have the right to have personal data concerning them rectified and **~~a 'right to be forgotten'~~ the right to have such personal data erased** where the retention of such data is not in compliance with this Regulation. In particular, data subjects should have the right that their personal data are erased and no longer processed, where the data are no longer necessary in relation to the purposes for which the data are collected or otherwise processed, where data subjects have withdrawn their consent for processing, **~~or~~** where they object to the **~~processing~~ collection or retention** of personal data concerning them or where the processing of their personal data **~~otherwise does not comply with this Regulation~~ is illegal. ~~This right is particularly relevant, when the data subject has given their consent as a child, when not being fully aware of the risks involved by the processing, and later wants to remove such personal data especially on the Internet.~~** However, the further retention of the data should be allowed where it is necessary for historical, statistical, and scientific research purposes, **for purposes of proof,** for reasons of public interest in the area of public health, for exercising the right of freedom of expression, when required by law or where there is a reason to restrict the processing of the data instead of erasing them. *Justification:* *This amendment reflect the amendments to art. 17.*
Recital (54) To strengthen the 'right to be forgotten' in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform third parties which are processing such data that a data subject requests them to erase any links to, or copies or replications of that personal data. To ensure this information, the controller should take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible. In relation to a third party publication of personal data, the controller should be considered responsible for the publication, where the controller has authorised the publication by the third party.	**Recital (54)** To strengthen the **~~'right to be forgotten'~~ right to erasure** in the online environment, the right to erasure should also be extended **to information society service providers via whose services the personal data have been published. Such information society service providers should provide the data subject with easily accessible means to request the personal data to be removed from their services ('notice and take down procedure'). This right is particularly relevant, when the data subject has given their consent as a child, when not being fully aware of the risks involved by the processing, and later wants to remove such personal data from the Internet. ~~in such a way that a controller who has made the personal data public should be obliged to inform third parties which are processing such data that a data subject requests them to erase any links to, or copies or replications of that personal data. To ensure this information, the controller should take all reasonable steps, including technical measures, in relation to data for the publication of which~~**

	~~the controller is responsible. In relation to a third party publication of personal data, the controller should be considered responsible for the publication, where the controller has authorised the publication by the third party.~~ *Justification:* *This amendment matches the amendment to Article 17 and 17a.*
Recital (55) To further strengthen the control over their own data and their right of access, data subjects should have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain a copy of the data concerning them also in commonly used electronic format. The data subject should also be allowed to transmit those data, which they have provided, from one automated application, such as a social network, into another one. This should apply where the data subject provided the data to the automated processing system, based on their consent or in the performance of a contract.	**Recital (55)** To further strengthen the control over their own data and their right of access, data subjects should have the right, where ~~personal data are~~ **user-generated content is** processed by electronic means and in a structured and commonly used format, to obtain a copy of the data concerning them ~~also in commonly used electronic format~~ **which allows the further use of such data by them,** ~~The data subject should also be allowed to transmit~~ **such as the transmission of** ~~those data, which they have provided~~ **such user-generated content** from one automated application, such as a social network, into another one. ~~This should apply where the data subject provided the data to the automated processing system, based on their consent or in the performance of a contract.~~ **This right should be without prejudice to the continued processing of user-generated content by the controller, where necessary, such as the continuation of services provided to the data subject, compliance with Union or Member State law or proof.** *Justification:* *This amendment matches the amendment to article 18.* *The requirement of a 'commonly used format' is already part of the requirement 'allows for further use by the data subject'. Therefore, it is superfluous.* *The right of data portability should be restricted to user-generated content only (see new definition in article 4), because:* *a) not all personal data are suitable for data portability (e.g., employee data or customer payment history),* *b) the right of data portability implies a obligation to accept the data on the part of the next controller, which is only logical for user-generated content,* *c) companies may have invested considerably in building databases, which are protected under intellectual property rights. The right to move data to the database of another controller would infringe such intellectual property rights.* *Unlike number portability in the telecom sector, data portability in the online environment does not mean that the data may not be processed anymore by the controller. After the data have been made available to the data subject, the controller might still have legitimate ground for continued processing, for example if the data subject continues to use the service, where the data are necessary for compliance with law or where the data are necessary for purposes of proof of illegal behaviour on the part of the data subject in the online environment or to solve contractual issues.*
Recital (56)	**Recital (56)**

In cases where personal data might lawfully be processed to protect the vital interests of the data subject, or on grounds of public interest, official authority or the legitimate interests of a controller, any data subject should nevertheless be entitled to object to the processing of any data relating to them. The burden of proof should be on the controller to demonstrate that their legitimate interests may override the interests or the fundamental rights and freedoms of the data subject.	In cases where personal data might lawfully be processed ~~to protect the vital interests of the data subject, or~~ on grounds of public interest, official authority or the legitimate interests of a controller, any data subject should nevertheless be entitled to object to the processing of any data relating to them. The burden of proof should be on the controller to demonstrate that their legitimate interests may override the interests or the fundamental rights and freedoms of the data subject. *Justification:* *This amendment matches the amendment to Article 19. The right to object is not practically relevant in case the data are processed to protect the vital interests of the data subject (life and death situations).*
Recital (57) Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing free of charge and in a manner that can be easily and effectively invoked.	
Recital (58) Every natural person should have the right not to be subject to a measure which is based on profiling by means of automated processing. However, such measure should be allowed when expressly authorised by law, carried out in the course of entering or performance of a contract, or when the data subject has given his consent. In any case, such processing should be subject to suitable safeguards, including specific information of the data subject and the right to obtain human intervention and that such measure should not concern a child.	**Recital (58)** ~~Every natural person should have the right not to be subject to a measure which is based on profiling by means of automated processing. However, such measure should be allowed when expressly authorised by law, carried out in the course of entering or performance of a contract, or when the data subject has given his consent.~~ **In accordance with Recommendation CM/Rec(2010)13 of the Council of Europe, the profiling of data subjects by automated processing should be allowed, provided the controller can demonstrate sufficient legal grounds for such profiling, including, but not limited to, the consent of the data subject, or where the profiling is necessary for entering into a contract with the data subject or for any other legitimate interests of the controller, which are not overridden by the interests of the data subject.** In any case, such processing should be subject to suitable safeguards, including specific information of the data subject and the right to obtain human intervention, and that such measure should not concern a child. *Justification:* *This amendment matches the Amendment to Article 20. According to the Recommendation on profiling of the Council of Europe, all grounds mentioned in Article 6.1 may provide a basis for profiling.*
Recital (59) Restrictions on specific principles and on the rights of information, access, rectification and erasure or on the right to data portability, the right to object, measures based on profiling, as well as on the communication of a personal data breach to a data subject and on certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or man-made disasters, the prevention, investigation and prosecution of criminal offences or of breaches of ethics for regulated professions, other public interests of the Union or of a Member State, in particular	**Recital (59)** Restrictions on specific principles and on the rights of information, access, rectification and erasure or on the right to data portability, the right to object, measures based on profiling, as well as on the communication of a personal data breach to a data subject and on certain related obligations of the controllers may be imposed by ~~**Union or Member State law**~~ **controllers**, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or man-made disasters, the prevention, investigation and prosecution of criminal offences or of breaches of ethics for regulated professions, other public interests of the Union or of a Member State, in particular

an important economic or financial interest of the Union or of a Member State, or the protection of the data subject or the rights and freedoms of others. Those restrictions should be in compliance with requirements set out by the Charter of Fundamental Rights of the European Union and by the European Convention for the Protection of Human Rights and Fundamental Freedoms.	an important economic or financial interest of the Union or of a Member State, **the protection of health, safety and security of individuals; the overriding business interests of the controller, in particular the protection of intellectual property rights, trade secrets or reputation or the preservation of confidentiality in business transactions;** or the protection of the data subject or the rights and freedoms of others. Those restrictions should be in compliance with requirements set out by the Charter of Fundamental Rights of the European Union and by the European Convention for the Protection of Human Rights and Fundamental Freedoms. *Justification:* *This amendment matched the amendment to Article 21. The basis for this amendment is the BCR-model agreed with the supervisory authorities, which includes these grounds. Furthermore, unlike the Directive, the Regulation does not need to be implemented. Therefore, controllers should be able to directly apply Article 21 and not have to wait for Member States to re-establish the grounds mentioned in Article 21 in national law.*
Recital (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.	**Recital (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. *Justification:* *This amendment matches the risk-based approach proposed by VNO-NCW in the relevant articles.*
Recital (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 principles of data protection by design and data protection by default.	**Recital (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 **and the processor** should adopt internal policies and implement appropriate measures, which meet in particular the principle~~**s of data protection by design and**~~ data protection by default. *Justification:* *This amendment matches the amendment to Article 23 and Recital 66.*
Recital (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.	

Recital (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.	**Recital (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 **directed** 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. *Justification* *Technical addition. The addition of the word 'directed' exempts controllers established outside the Union that are not targeting their services at data subjects residing in the EU. This way a non-EU website offering services to non-EU data subjects but is occasionally visited by EU data subjects should not designate a representative. As soon as any targeting occurs (by for instance offering a service in a specific EU-language or otherwise), the controller will have to apply EU data protection regime. (See also ECJ in Alpenhof v Heller).*
Recital (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.	**Recital (64)** **(deleted)** *Justification* *By using the word 'directed' in the previous recital, the case law of the ECJ in Alpenhof v. Heller makes this recital superfluous.*
Recital (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.	**Recital (65)** In order to demonstrate compliance with this Regulation, the controller ~~**or processor**~~ should document ~~**each**~~ processing operation**s, which following a risk assessment pose a high degree of risk to the fundamental rights of the data subjects, in particular their right to privacy**. 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. **Each processor should provide the controller with all information necessary to meet his obligations under this Regulation.** *Justification:* *This amendment matches the amendments to Article 28. The Regulation removes administrative burdens of Directive 95/46, such as notification of data processing to the supervisory authority. However, it replaces those with costly mandatory compliance burdens. Such compliance burdens should are only justifiable for high-risk data processing. Similar Directive 95/46, the Regulation should have exemptions from such burdens. However, the size of organizations is not the right criterion for such exemptions. Exemptions should be risk-based.* *Data processors should only have derivative obligations with respect to documentation of data processing.*

	Therefore, they should be required to provide all information necessary for the controller to meet his obligations under this Regulation.
Recital (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.	**Recital (66)** In order to maintain security and to prevent processing in breach of this Regulation, the controller ~~or~~ **and the** processor should evaluate the **security** 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. *Justification:* *Both the controller and the processor should evaluate security risks.*
Recital (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 achieved within 24 hours, an explanation of the reasons for the delay should accompany the notification. The individuals whose personal data could be adversely affected by the breach should be notified without undue delay in order to allow them to take the necessary precautions. A breach should be considered as adversely affecting the personal data or privacy of a data subject where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation. The notification should describe the nature of the personal data breach as well as recommendations as well as recommendations for the individual concerned to mitigate potential adverse effects. Notifications to data subjects should be made as soon as reasonably feasible, and in close cooperation with the supervisory authority and respecting guidance provided by it or other relevant authorities (e.g. law enforcement authorities). For example, the chance for data subjects to mitigate an immediate risk of harm would call for a prompt notification of data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify a longer delay.	**Recital (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 **personal data** breach**, which is likely to have a significant adverse effect on the rights and freedoms of the data subject, especially his right to privacy,** has occurred, the controller should notify the breach to the supervisory authority without ~~undue~~ **unreasonable** delay**.** ~~**and, where feasible, within 24 hours. Where this cannot achieved within 24 hours, an explanation of the reasons for the delay should accompany the notification.**~~ **Where the controller has taken technical measures, which prevent the individual from being directly identified from the data or which make it reasonably unlikely that the individual can be identified from the data, such as having made the data unintelligible through the use of encryption or having the data pseudomised, the obligation to notify the supervisory authority should not exist.** **Where the data subjects can be identified from the data, the individuals data subjects whose personal data could be adversely affected by the breach should be notified without undue unreasonable delay in order to allow them to take the necessary precautions. However, the controller should not be required to communicate a personal data breach to the data subject where the obligation to notify the supervisory authority does not exist, as well as where contacting the data subject is factually impossible or where contacting the data subject would require a disproportionate effort on the part of the controller.** 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 prompt notification of data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify a longer delay. **In order to avoid multiple notifications or communication for the same breach, joint controllers or groups of undertakings should be able to designate a controller or undertaking responsible for the notification or communication on their behalf.** **Where a notification of a personal data breach to the data subjects would likely result in a disruption of society, such as a significant impact on the trust financial market stability, the controller should not be required to notify the data subject.** *Justification* *This amendment matches the amendment to Articles 31 and 32.*
Recital (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.	**Recital (68)** **(deleted, in favour of the amendment to recital 67)**
Recital (69) In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of the breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. Moreover, such rules and procedures should take into account the legitimate interests of law enforcement authorities in cases where early disclosure could unnecessarily hamper the investigation of the circumstances of a breach.	**Recital (69)** In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of the breach, ~~**including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse**~~. Moreover, such rules and procedures should take into account the legitimate interests of law enforcement authorities in cases where early disclosure could unnecessarily hamper the investigation of the circumstances of a breach. *Justification* *This amendment matches the amendment to Recital 67.*
Recital (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	**Recital (70)** Directive 95/46/EC provided for a general obligation to notify processing of personal data to the supervisory authorities **allowing the Member States to exempt**

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 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.	**processing, which were unlikely to pose risks to the data subjects from this obligation. ~~While~~ T**his obligation produces administrative and financial burdens, **and** 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~~ high degree of** 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~~ privacy** impact assessment should be carried out by 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. *Justification:* *This amendment matches the amendment to Article 33 and the risk-based approach proposed by VNO-NCW. Furthermore, reference is made to the possibility under article 18 of Directive 95/46/EC to exempt low-risk processing from the notification obligation. The Commission's proposal did not contain such exemption. The risk-based approach proposed by VNO-NCW, especially the amendments to Articles 28 and 33 re-inserts this exemption.*
Recital (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.	
Recital (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.	**Recital (72)** There are circumstances under which it may be sensible and economic that the subject of a **~~data protection~~ privacy** 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. *Justification:* *This amendment matches the amendment to Article 33.*
Recital (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.	**Recital (73)** **~~Data protection~~ Privacy** 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. *Justification:* *This amendment matches the amendment to Article 33.*
Recital (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	**Recital (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.	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.~~ **controller should document the privacy impact assessment and make such assessment available to the supervisory authority upon request.** ~~**Such**~~ **The supervisory authority should be** ~~**consultation should equally take place**~~ **consulted** 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. *Justification:* *This amendment matches the amendments to Article 34.*
Recital (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.	**Recital (75)** Where the processing is carried out in the public sector or where~~, in the private sector,~~ processing is carried out by a**n** ~~**large**~~ enterprise~~, or where its core activities, regardless of the size of the enterprise, involve processing operations which require regular and systematic monitoring~~ **which relates to its core activities and poses a high degree of risk to the rights and freedoms of data subjects especially their right to privacy, such as the regular and systematic monitoring of data subjects, irrespective of the measures taken to mitigate such risks**, 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. **In any other case, the appointment of such a person should be optional. The data protection officer should be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil his or her tasks. The necessary level of expert knowledge should be determined in particular according to the data processing carried out and the protection required for the personal data processed by the controller.** *Justification:* *This amendment matches the amendments to Article 35.*
Recital (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.	
Recital (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.	
Recital (78) Cross-border flows of personal data are necessary for the expansion of international trade and international co-operation. The increase in these flows has raised new	

challenges and concerns with respect to the protection of personal data. However, when personal data are transferred from the Union to third countries or to international organisations, the level of protection of individuals guaranteed in the Union by this Regulation should not be undermined. In any event, transfers to third countries may only be carried out in full compliance with this Regulation.	
Recital (79) This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects.	
Recital (80) The Commission may decide with effect for the entire Union that certain third countries, or a territory or a processing sector within a third country, or an international organisation, offer an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third countries or international organisations which are considered to provide such level of protection. In these cases, transfers of personal data to these countries may take place without needing to obtain any further authorisation.	
Recital (81) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, take into account how a given third country respects the rule of law, access to justice as well as international human rights norms and standards.	
Recital (82) The Commission may equally recognise that a third country, or a territory or a processing sector within a third country, or an international organisation offers no adequate level of data protection. Consequently the transfer of personal data to that third country should be prohibited. In that case, provision should be made for consultations between the Commission and such third countries or international organisations.	**Recital (82)** The Commission may equally recognise that a third country, or a territory or a processing sector within a third country, or an international organisation offers no adequate level of data protection. Consequently the transfer of personal data to that third country should be prohibited. In that case, provision should be made for consultations between the Commission and such third countries or international organisations. **Such decision should not apply to transfers based on a derogation pursuant to this Regulation, as well as to personal data which originated in such country. The Commission should seek the views of relevant stakeholders prior to taking such decision.** *Justification:* *- The economic interests of companies or sectors may be significantly impacted by such decision. Therefore, such companies or sectors should be given the possibility to express their views.* *- Furthermore, for clarity, the exception mentioned in article 41.6 has been added to the Recital.* *- Moreover, where companies store the data of their employees or customers residing in such country in a datacenter in the EU, the prohibition would prohibit such companies from transferring such data back to such country. Therefore, such re-transfers should be excluded from the prohibition, unless trade with such country is also prohibited.*

Recital (83) In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority, or other suitable and proportionate measures justified in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations and where authorised by a supervisory authority.	
Recital (84) The possibility for the controller or processor to use standard data protection clauses adopted by the Commission or by a supervisory authority should neither prevent the possibility for controllers or processors to include the standard data protection clauses in a wider contract nor to add other clauses as long as they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects.	
Recital (85) A corporate group should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same corporate group of undertakings, as long as such corporate rules include essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.	**Recital (85)** A corporate group should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same corporate group of undertakings, **including an alliance,** as long as such corporate rules include essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data. *Justification* *This amendment matches the amendment to Article 4.17. It clarifies that the group of undertakings, which may adopt BCRs, can be – under certain conditions – fluid. In such case, it is likely that the BCRs will apply to one or a few processings which are essential to the alliance (e.g., a shared customer database).*
Recital (86) Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal claim, where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In this latter case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients.	**Recital (86)** Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal claim, where important grounds of public interest ~~**laid down by Union or Member State law**~~ so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In this latter case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients. *Justification* *This amendment matches the amendment to Article 44.5.*

	The fact that the data processing is necessary in the public interest may also be assessed by the controller. The delegated acts of the Commission pursuant to Article 44.7 should ensure that no misuse of this ground is made.
Recital (87) These derogations should in particular apply to data transfers required and necessary for the protection of important grounds of public interest, for example in cases of international data transfers between competition authorities, tax or customs administrations, financial supervisory authorities, between services competent for social security matters, or to competent authorities for the prevention, investigation, detection and prosecution of criminal offences.	
Recital (88) Transfers which cannot be qualified as frequent or massive, could also be possible for the purposes of the legitimate interests pursued by the controller or the processor, when they have assessed all the circumstances surrounding the data transfer. For the purposes of processing for historical, statistical and scientific research purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration.	**Recital (88)** Transfers which cannot be qualified as ~~**frequent**~~ **structural** or massive, could also be possible for the purposes of the legitimate interests pursued by the controller or the processor, when they have assessed all the circumstances surrounding the data transfer. For the purposes of processing for historical, statistical and scientific research purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration. *Justification:* *This amendment matches the amendment to Article 44.1(h)*
Recital (89) In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with a guarantee that they will continue to benefit from the fundamental rights and safeguards as regards processing of their data in the Union once this data has been transferred.	**Recital (89)** In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller ~~**or processor**~~ should **assess the adequacy of the country, sector or recipient or** ~~**make use of**~~ solutions **should be used** that provide data subjects with a guarantee that they will continue to benefit from the fundamental rights and safeguards as regards processing of their data in the Union once this data has been transferred. *Justification:* *This amendment matches the amendment to Article 41. Furthermore, it means that processors may not conduct such an assessment.*
Recital (90) Some third countries enact laws, regulations and other legislative instruments which purport to directly regulate data processing activities of natural and legal persons under the jurisdiction of the Member States. The extraterritorial application of these laws, regulations and other legislative instruments may be in breach of international law and may impede the attainment of the protection of individuals guaranteed in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may inter alia be the case where the disclosure is necessary for an important ground of public interest recognised in Union law or in a Member State law to which the controller is subject. The conditions under which an important ground of public interest exists should be further specified by the Commission in a delegated act.	
Recital (91)	

When personal data moves across borders it may put at increased risk the ability of individuals to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. Therefore, there is a need to promote closer co-operation among data protection supervisory authorities to help them exchange information and carry out investigations with their international counterparts.	
Recital (92) The establishment of supervisory authorities in Member States, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of their personal data. Member States may establish more than one supervisory authority, to reflect their constitutional, organisational and administrative structure.	
Recital (93) Where a Member State establishes several supervisory authorities, it should establish by law mechanisms for ensuring the effective participation of those supervisory authorities in the consistency mechanism. That Member State should in particular designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the mechanism, to ensure swift and smooth co-operation with other supervisory authorities, the European Data Protection Board and the Commission.	
Recital (94) Each supervisory authority should be provided with the adequate financial and human resources, premises and infrastructure, which is necessary for the effective performance of their tasks, including for the tasks related to mutual assistance and cooperation with other supervisory authorities throughout the Union.	
Recital (95) The general conditions for the members of the supervisory authority should be laid down by law in each Member State and should in particular provide that those members should be either appointed by the parliament or the government of the Member State, and include rules on the personal qualification of the members and the position of those members.	
Recital (96) The supervisory authorities should monitor the application of the provisions pursuant to this Regulation and contribute to its consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the internal market. For that purpose, the supervisory authorities should co-operate with each other and the Commission.	
Recital (97)	**Recital (97)**

Where the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union takes place in more than one Member State, one single supervisory authority should be competent for monitoring the activities of the controller or processor throughout the Union and taking the related decisions, in order to increase the consistent application, provide legal certainty and reduce administrative burden for such controllers and processors.	Where the processing of personal data in the context of the activities of an establishment of ~~a controller or a processor~~ **an enterprise** in the Union takes place in more than one Member State, one single supervisory authority should be competent for monitoring the activities of the ~~controller or processor~~ **enterprise** throughout the Union and taking the related decisions, in order to increase the consistent application, provide legal certainty and reduce administrative burden for such controllers and processors. *Justification* *Technical. The term controller and processor are defined terms. The term enterprise is more neutral, as the controller of a particular cross-border processing operation may not be the parent company of the entity in the other Member State.*
Recital (98) The competent authority, providing such one-stop shop, should be the supervisory authority of the Member State in which the controller or processor has its main establishment.	**Recital (98)** The competent authority, providing such one-stop shop, should be the supervisory authority of the Member State in which the ~~controller or processor~~ **enterprise** has its main establishment. *Justification* *Technical. The term controller and processor are defined terms. The term enterprise is more neutral, as the controller of a particular cross-border processing operation may not be the parent company of the entity in the other Member State.*
Recital (99) While this Regulation applies also to the activities of national courts, the competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of judges in the performance of their judicial tasks. However, this exemption should be strictly limited to genuine judicial activities in court cases and not apply to other activities where judges might be involved in, in accordance with national law.	
Recital (100) In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same duties and effective powers, including powers of investigation, legally binding intervention, decisions and sanctions, particularly in cases of complaints from individuals, and to engage in legal proceedings. Investigative powers of supervisory authorities as regards access to premises should be exercised in conformity with Union law and national law. This concerns in particular the requirement to obtain a prior judicial authorisation.	
Recital (101) Each supervisory authority should hear complaints lodged by any data subject and should investigate the matter. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case	

requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject.	
Recital (102) Awareness raising activities by supervisory authorities addressed to the public should include specific measures directed at controllers and processors, including micro, small and medium-sized enterprises, as well as data subjects.	
Recital (103) The supervisory authorities should assist each other in performing their duties and provide mutual assistance, so as to ensure the consistent application and enforcement of this Regulation in the internal market.	
Recital (104) Each supervisory authority should have the right to participate in joint operations between supervisory authorities. The requested supervisory authority should be obliged to respond to the request in a defined time period.	
Recital (105) In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for co-operation between the supervisory authorities themselves and the Commission should be established. This mechanism should in particular apply where a supervisory authority intends to take a measure as regards processing operations that are related to the offering of goods or services to data subjects in several Member States, or to the monitoring such data subjects, or that might substantially affect the free flow of personal data. It should also apply where any supervisory authority or the Commission requests that the matter should be dealt with in the consistency mechanism. This mechanism should be without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties.	
Recital (106) In application of the consistency mechanism, the European Data Protection Board should, within a determined period of time, issue an opinion, if a simple majority of its members so decides or if so requested by any supervisory authority or the Commission.	
Recital (107) In order to ensure compliance with this Regulation, the Commission may adopt an opinion on this matter, or a decision, requiring the supervisory authority to suspend its draft measure.	
Recital (108) There may be an urgent need to act in order to protect the interests of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded. Therefore, a supervisory authority should be able to adopt provisional measures with a specified period of validity when applying the consistency mechanism.	
Recital (109)	

The application of this mechanism should be a condition for the legal validity and enforcement of the respective decision by a supervisory authority. In other cases of cross-border relevance, mutual assistance and joint investigations might be carried out between the concerned supervisory authorities on a bilateral or multilateral basis without triggering the consistency mechanism.	
Recital (110) At Union level, a European Data Protection Board should be set up. It should replace the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by Directive 95/46/EC. It should consist of a head of a supervisory authority of each Member State and of the European Data Protection Supervisor. The Commission should participate in its activities. The European Data Protection Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the Commission and promoting cooperation of the supervisory authorities throughout the Union. The European Data Protection Board should act independently when exercising its tasks.	
Recital (111) Every data subject should have the right to lodge a complaint with a supervisory authority in any Member State and have the right to a judicial remedy if they consider that their rights under this Regulation are infringed or where the supervisory authority does not react on a complaint or does not act where such action is necessary to protect the rights of the data subject.	
Recital (112) Any body, organisation or association which aims to protects the rights and interests of data subjects in relation to the protection of their data and is constituted according to the law of a Member State should have the right to lodge a complaint with a supervisory authority or exercise the right to a judicial remedy on behalf of data subjects, or to lodge, independently of a data subject's complaint, an own complaint where it considers that a personal data breach has occurred.	
Recital (113) Each natural or legal person should have the right to a judicial remedy against decisions of a supervisory authority concerning them. Proceedings against a supervisory authority should be brought before the courts of the Member State, where the supervisory authority is established.	
Recital (114) In order to strengthen the judicial protection of the data subject in situations where the competent supervisory authority is established in another Member State than the one where the data subject is residing, the data subject may request any body, organisation or association aiming to protect the rights and interests of data subjects in relation to the protection of their data to bring on the data subject's behalf proceedings against that supervisory authority to the competent court in the other Member State.	

Recital (115) In situations where the competent supervisory authority established in another Member State does not act or has taken insufficient measures in relation to a complaint, the data subject may request the supervisory authority in the Member State of his or her habitual residence to bring proceedings against that supervisory authority to the competent court in the other Member State. The requested supervisory authority may decide, subject to judicial review, whether it is appropriate to follow the request or not.	
Recital (116) For proceedings against a controller or processor, the plaintiff should have the choice to bring the action before the courts of the Member States where the controller or processor has an establishment or where the data subject resides, unless the controller is a public authority acting in the exercise of its public powers.	
Recital (117) Where there are indications that parallel proceedings are pending before the courts in different Member States, the courts should be obliged to contact each other. The courts should have the possibility to suspend a case where a parallel case is pending in another Member State. Member States should ensure that court actions, in order to be effective, should allow the rapid adoption of measures to remedy or prevent an infringement of this Regulation.	
Recital (118) Any damage which a person may suffer as a result of unlawful processing should be compensated by the controller or processor, who may be exempted from liability if they prove that they are not responsible for the damage, in particular where he establishes fault on the part of the data subject or in case of force majeure.	
Recital (119) Penalties should be imposed to any person, whether governed by private or public law, who fails to comply with this Regulation. Member States should ensure that the penalties should be effective, proportionate and dissuasive and should take all measures to implement the penalties.	
Recital (120) In order to strengthen and harmonise administrative sanctions against infringements of this Regulation, each supervisory authority should have the power to sanction administrative offences. This Regulation should indicate these offences and the upper limit for the related administrative fines, which should be fixed in each individual case proportionate to the specific situation, with due regard in particular to the nature, gravity and duration of the breach. The consistency mechanism may also be used to cover divergences in the application of administrative sanctions.	
Recital (121) The processing of personal data solely for journalistic purposes, or for the purposes of artistic or literary expression should qualify for exemption from the requirements of certain provisions of this Regulation in order to reconcile the right to the protection of personal	

data with the right to freedom of expression, and notably the right to receive and impart information, as guaranteed in particular by Article 11 of the Charter of Fundamental Rights of the European Union. This should apply in particular to processing of personal data in the audiovisual field and in news archives and press libraries. Therefore, Member States should adopt legislative measures, which should lay down exemptions and derogations which are necessary for the purpose of balancing these fundamental rights. Such exemptions and derogations should be adopted by the Member States on general principles, on the rights of the data subject, on controller and processor, on the transfer of data to third countries or international organisations, on the independent supervisory authorities and on co-operation and consistency. This should not, however, lead Member States to lay down exemptions from the other provisions of this Regulation. In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly. Therefore, Member States should classify activities as "journalistic" for the purpose of the exemptions and derogations to be laid down under this Regulation if the object of these activities is the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them. They should not be limited to media undertakings and may be undertaken for profit-making or for non-profit making purposes.	
Recital (122) The processing of personal data concerning health, as a special category of data which deserves higher protection, may often be justified by a number of legitimate reasons for the benefit of individuals and society as a whole, in particular in the context of ensuring continuity of cross-border healthcare. Therefore this Regulation should provide for harmonised conditions for the processing of personal data concerning health, subject to specific and suitable safeguards so as to protect the fundamental rights and the personal data of individuals. This includes the right for individuals to have access to their personal data concerning their health, for example the data in their medical records containing such information as diagnosis, examination results, assessments by treating physicians and any treatment or interventions provided.	
Recital (123) The processing of personal data concerning health may be necessary for reasons of public interest in the areas of public health, without consent of the data subject. In that context, 'public health' should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work, meaning all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Such processing of personal data concerning health for reasons of public interest should not result in personal data	

being processed for other purposes by third parties such as employers, insurance and banking companies.	
Recital (124) The general principles on the protection of individuals with regard to the processing of personal data should also be applicable to the employment context. Therefore, in order to regulate the processing of employees' personal data in the employment context, Member States should be able, within the limits of this Regulation, to adopt by law specific rules for the processing of personal data in the employment sector.	**Recital (124)** The general principles on the protection of individuals with regard to the processing of personal data should also be applicable to the employment context. ~~**Therefore, in order to regulate the processing of employees' personal data in the employment context**~~ **However, in recognition of the differences in labour relations between Member States,** Member States should be able, within the limits of this Regulation, to adopt by law specific rules for the ~~**processing**~~ **collection, use or dissemination** of personal data in the employment **and staffing** sector. **Moreover, such a law should not impact the full harmonization across Member States with respect to HR-operations or other processing of employee data, such as the processing of such data by processors, the security measures required for such data, data breach notifications, or any international transfers of such data. Those issues should be exclusively governed by Union law.** *Justification:* *This amendment matches the amendment to article 82.*
Recital (125) The processing of personal data for the purposes of historical, statistical or scientific research should, in order to be lawful, also respect other relevant legislation such as on clinical trials.	
Recital (126) Scientific research for the purposes of this Regulation should include fundamental research, applied research, and privately funded research and in addition should take into account the Union's objective under Article 179(1) of the Treaty on the Functioning of the European Union of achieving a European Research Area.	
Recital (127) As regards the powers of the supervisory authorities to obtain from the controller or processor access personal data and access to its premises, Member States may adopt by law, within the limits of this Regulation, specific rules in order to safeguard the professional or other equivalent secrecy obligations, in so far as necessary to reconcile the right to the protection of personal data with an obligation of professional secrecy.	
	Recital (127a) **The obligation to inform the data subject about the purposes of the processing, the right to erasure, the right to data portability, the right to objection, the obligation to take measures to ensure compliance as well as the prohibition to transfer data to countries outside the Union, should not apply to the processing of information relating to the professional capacity of an individual, such as such individual's employer, job title, function, business address, business phone or fax number, business e-mail address or other organizational details. However, data subjects should have the right to request from the controller not to have such professional information disclosed to third parties. Such blocking should not be required where the blocking proves impossible or would involve a disproportionate effort on the part of the**

	controller. *Justification:* *Professional data (see definition in Article 4) are frequently collected or disclosed in commercial settings, often as part of communication between companies (e.g., a letter head or e-mail signature). Professional data poses hardly any risk to the privacy of the data subject and is often meant to be freely disseminated (e.g., business cards, business phone numbers and business e-mail addresses). This amendment aims to reduce the burden of compliance with regard to such data.*
Recital (128) This Regulation respects and does not prejudice the status under national law of churches and religious associations or communities in the Member States, as recognised in Article 17 of the Treaty on the Functioning of the European Union. As a consequence, where a church in a Member State applies, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of individuals with regard to the processing of personal data, these existing rules should continue to apply if they are brought in line with this Regulation. Such churches and religious associations should be required to provide for the establishment of a completely independent supervisory authority.	
Recital (129) In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement of personal data within the Union, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission. In particular, delegated acts should be adopted in respect of lawfulness of processing; specifying the criteria and conditions in relation to the consent of a child; processing of special categories of data; specifying the criteria and conditions for manifestly excessive requests and fees for exercising the rights of the data subject; criteria and requirements for the information to the data subject and in relation to the right of access; the right to be forgotten and to erasure; measures based on profiling; criteria and requirements in relation to the responsibility of the controller and to data protection by design and by default; a processor; criteria and requirements for the documentation and the security of processing; criteria and requirements for establishing a personal data breach and for its notification to the supervisory authority, and on the circumstances where a personal data breach is likely to adversely affect the data subject; the criteria and conditions for processing operations requiring a data protection impact assessment; the criteria and requirements for determining a high degree of specific risks which require prior consultation; designation and tasks of the data protection officer; codes of conduct; criteria and requirements for certification mechanisms; criteria and requirements for transfers by way of binding corporate rules; transfer derogations; administrative sanctions; processing for health purposes; processing in the employment context and processing for historical,	**Recital (129)** **[to be changed in accordance with the deletions in other articles]**

statistical and scientific research purposes. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing-up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and Council.	
Recital (130) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission for: specifying standard forms in relation to the processing of personal data of a child; standard procedures and forms for exercising the rights of data subjects; standard forms for the information to the data subject; standard forms and procedures in relation to the right of access; the right to data portability; standard forms in relation to the responsibility of the controller to data protection by design and by default and to the documentation; specific requirements for the security of processing; the standard format and the procedures for the notification of a personal data breach to the supervisory authority and the communication of a personal data breach to the data subject; standards and procedures for a data protection impact assessment; forms and procedures for prior authorisation and prior consultation; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation; disclosures not authorized by Union law; mutual assistance; joint operations; decisions under the consistency mechanism. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers. In this context, the Commission should consider specific measures for micro, small and medium-sized enterprises.	**Recital (130)** **[to be changed in accordance with the deletions in other articles]**
Recital (131) The examination procedure should be used for the adoption of specifying standard forms in relation to the consent of a child; standard procedures and forms for exercising the rights of data subjects; standard forms for the information to the data subject; standard forms and procedures in relation to the right of access;, the right to data portability; standard forms in relation to the responsibility of the controller to data protection by design and by default and to the documentation; specific requirements for the security of processing; the standard format and the procedures for the notification of a personal data breach to the supervisory authority and the communication of a personal data breach to the data subject; standards and procedures for a data protection impact assessment; forms and procedures for prior authorisation and prior consultation; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation; disclosures not authorized by Union law; mutual assistance; joint operations; decisions	**Recital (131)** **[to be changed in accordance with the deletions in other articles]**

under the consistency mechanism, given that those acts are of general scope.	
Recital (132) The Commission should adopt immediately applicable implementing acts where, in duly justified cases relating to a third country or a territory or a processing sector within that third country or an international organisation which does not ensure an adequate level of protection and relating to matters communicated by supervisory authorities under the consistency mechanism, imperative grounds of urgency so require.	
Recital (133) Since the objectives of this Regulation, namely to ensure an equivalent level of protection of individuals and the free flow of data throughout the Union, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.	
Recital (134) Directive 95/46/EC should be repealed by this Regulation. However, Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC should remain in force.	
Recital (135) This Regulation should apply to all matters concerning the protection of fundamental rights and freedom vis-à-vis the processing of personal data, which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC, including the obligations on the controller and the rights of individuals. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, the latter Directive should be amended accordingly.	
Recital (136) As regards Iceland and Norway, this Regulation constitutes a development of provisions of the Schengen acquis to the extent that it applies to the processing of personal data by authorities involved in the implementation of that acquis, as provided for by the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen acquis.	
Recital (137) As regards Switzerland, this Regulation constitutes a development of provisions of the Schengen acquis to the extent that it applies to the processing of personal data by authorities involved in the implementation of that acquis, as provided for by the Agreement between the European Union, the European Community and the Swiss Confederation concerning the association of the Swiss Confederation with the implementation, application and	

development of the Schengen acquis.	
Recital (138) As regards Liechtenstein, this Regulation constitutes a development of provisions of the Schengen acquis to the extent that it applies to the processing of personal data by authorities involved in the implementation of that acquis, as provided for by the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen acquis.	
Recital (139) In view of the fact that, as underlined by the Court of Justice of the European Union, the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society and be balanced with other fundamental rights, in accordance with the principle of proportionality, this Regulation respects all fundamental rights and observes the principles recognised in the Charter of Fundamental Rights of the European Union as enshrined in the Treaties, notably the right to respect for private and family life, home and communications, the right to the protection of personal data, the freedom of thought, conscience and religion, the freedom of expression and information, the freedom to conduct a business, the right to an effective remedy and to a fair trial as well as cultural, religious and linguistic diversity.	**Recital (139)** In view of the fact that, as underlined by the Court of Justice of the European Union, the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society and be balanced with other fundamental rights, in accordance with the principle of proportionality, this Regulation respects all fundamental rights and observes the principles recognised in the Charter of Fundamental Rights of the European Union as enshrined in the Treaties, notably the right to respect for private and family life, home and communications, the right to the protection of personal data, the freedom of thought, conscience and religion, the freedom of expression and information, the freedom to conduct a business, the right to an effective remedy and to a fair trial ~~as well as,~~ cultural, religious and linguistic diversity **as well as the fundamental rights and freedoms of enterprises, including but not limited to their freedom to conduct a business**. *Justification* *The proposal builds on paragraph 3.3 of the explanatory memorandum to the Regulation. Recalling the Charter of human rights, the amendment strikes a balance between individuals rights/freedoms and companies rights/freedoms. E.g. contract data represent information about the contracting individual as well as the contracting company.*
Article 1 **Subject matter and objectives** 1. This Regulation lays down rules relating to the protection of individuals with regard to the processing of personal data and rules relating to the free movement of personal data. 2. This Regulation protects the fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data. 3. The free movement of personal data within the Union shall neither be restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data.	
Article 2 **Material scope**	**Article 2** **Material scope**

1. This Regulation applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.	1. This Regulation applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.
2. This Regulation does not apply to the processing of personal data: (a) in the course of an activity which falls outside the scope of Union law, in particular concerning national security; (b) by the Union institutions, bodies, offices and agencies; (c) by the Member States when carrying out activities which fall within the scope of Chapter 2 of the Treaty on European Union; (d) by a natural person without any gainful interest in the course of its own exclusively personal or household activity; (e) by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.	2. This Regulation does not apply to the processing of personal data: (a) in the course of an activity which falls outside the scope of Union law, in particular concerning national security; (b) by the Union institutions, bodies, offices and agencies; (c) by the Member States when carrying out activities which fall within the scope of Chapter 2 of the Treaty on European Union; (d) by a natural person ~~**without any gainful interest**~~ in the course of ~~**its own exclusively**~~ **a** personal or household activity**, or in the context of gainful activities, which cannot be considered to constitute an enterprise**; (e) by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.
3. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.	3. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive. *Justification:* - *The deletion of 'exclusively' is technical and tries to avoid that personal data which are shared in a personal setting (e.g., providing a friend with another friends phone number) falls within the scope of this Regulation.* - *The deletion of 'own' is intended to avoid that personal activities which involve multiple persons, e.g., an activity with family or friends, falls within the scope of this Regulation.* - *Furthermore, private persons often conduct activities with the intention to earn some money, but such activities cannot be considered a commercial enterprise under commercial law (e.g., teenagers providing baby-sitting services, or people selling their car on eBay). Applying the Regulation to such activities would be unreasonable. Therefore, the Commission's proposal for the exclusion of 'personal or domestic' activities is too narrow. The amendment clarifies that such 'commercial' activities do not fall within the scope of this Regulation.*
Article 3 **Territorial scope** 1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union.	**Article 3** **Territorial scope** 1. This Regulation applies to the processing of personal data in the context of the activities of **a public authority or public body, or of** an establishment of ~~**a controller, or a processor**~~ **an enterprise or any other entity acting as a controller or processor** in the Union**, as well as by a natural person residing in the Union**.
2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to: (a) the offering of goods or services to such data subjects in the Union; or (b) the monitoring of their behaviour.	2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established **or residing** in the Union, where the processing activities are related to: (a) the offering of goods or services **directed** to such data subjects in the Union; or (b) the monitoring of their behaviour.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.	3. This Regulation applies to the processing of personal data by a controller not established **or residing** in the Union, but in a place where the national law of a Member State applies by virtue of public international law. *Justification 3.1* *Technical change to repair a mistake made in Directive 95/46 with regard to term 'establishment of the controller', which was too simplistic.* *First of all, the terms 'controller' and 'processor' have a data protection specific meaning (see definitions in art. 4). This means that – within a multinational enterprise – the controller for a particular processing may often not be the parent company of the establishment in another Member State, and therefore has no 'establishments' other than his own establishment. The term 'enterprise' better fits the objective of Art. 3.1., as all establishments in the Union belong to the same enterprise.* *Furthermore, Art. 3.1 should also mention 'natural persons' as they don't have an 'establishment', but 'reside'.* *The terms 'public authority' and 'public body' have been added for sake of completeness. The term 'any other entity acting as a controller or processor' includes foundations and associations.* *Justification 3.2* *The addition of the words 'directed' exempts controllers established outside the Union that are not targeting their services at data subjects residing in the EU. This way a non-EU website offering services to non-EU data subjects but is occasionally visited by EU data subjects should not comply with the regime. As soon as any targeting occurs (for instance, by offering a service in a specific EU-language or otherwise), the controller will have to apply EU data protection regime.*
Article 4 **Definitions** For the purposes of this Regulation: (1) 'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person; (2) 'personal data' means any information relating to a data subject; (3) 'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction;	**Article 4** **Definitions** For the purposes of this Regulation: (1) 'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller ~~**or by any other natural or legal person**~~, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person; **if identification, in view of the measures taken by the controller to prevent identification, requires disproportionate effort, time or resources, the natural person shall not be considered identifiable.** (2) 'personal data' means any information relating to a data subject; (3) 'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction;

(4) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;	(4) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;
(5) 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the processing of personal data; where the purposes, conditions and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;	(5) 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the processing of personal data; where the purposes, conditions and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;
(6) 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;	(6) 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;
(7) 'recipient' means a natural or legal person, public authority, agency or any other body to which the personal data are disclosed;	(7) 'recipient' means a natural or legal person, public authority, agency or any other body to which the personal data are disclosed. **The term does not include staff of the controller, the processor or processors, or the data subject, including the data subject's representative or legal guardian**;
(8) 'the data subject's consent' means any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;	(8) 'the data subject's consent' means any free, specific**,** **and** informed **~~and explicit~~ expression of will, either by a statement or an action, which, in view of the context and circumstances at the time consent is required, signifies the data subject's agreement to the processing of the personal data** ~~**indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being 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;
(10) 'genetic data' means all data, of whatever type, concerning the characteristics of an individual which are inherited or acquired during early prenatal development;	(10) 'genetic data' means all data, of whatever type, concerning the characteristics of an individual which are inherited or acquired during early prenatal development;
(11) 'biometric data' means any data relating to the physical, physiological or behavioural characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data;	(11) 'biometric data' means any data relating to the physical, physiological or behavioural characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data;
(12) 'data concerning health' means any information which relates to the physical or mental health of an individual, or to the provision of health services to the individual;	(12) 'data concerning health' means any information which relates to the physical or mental health of an individual, or to the provision of health services to the individual;
(13) 'main establishment' means as regards the controller, the place of its establishment in the Union where the main decisions as to the purposes, conditions and means of the processing of personal data are taken; if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the Union, the main establishment is the place where the main processing activities in the context of the activities of an establishment of a controller in the Union take place. As regards the	(13) 'main establishment' means ~~**as regards the controller,**~~ the place of ~~its~~ establishment **of a group of companies** in the Union where the main decisions as to the ~~**purposes, conditions and means of**~~ the processing of personal data are taken; ~~**if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the Union, the main establishment is the place where the main processing activities in the context of the activities of an establishment of a controller in the Union take place.**~~

processor, 'main establishment' means the place of its central administration in the Union;	~~As regards the processor, 'main establishment' means the place of its central administration in the Union;~~ **the global or European headquarters or the group company with delegated data protection responsibilities shall be deemed the main establishment. Alternatively, the legal entity, which takes most or the most significant decisions with respect to the purposes and means of data processing in the group or the group company which is best placed to enforce the group's compliance framework, including the group's binding corporate rules, may be deemed the main establishment.**
(14) 'representative' means any natural or legal person established in the Union who, explicitly designated by the controller, acts and may be addressed by any supervisory authority and other bodies in the Union instead of the controller, with regard to the obligations of the controller under this Regulation;	(14) 'representative' means any natural or legal person established in the Union who, explicitly designated by the controller, acts and may be addressed by any supervisory authority and other bodies in the Union instead of the controller, with regard to the obligations of the controller under this Regulation;
(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;
(16) 'group of undertakings' means a controlling undertaking and its controlled undertakings;	(16) 'group of undertakings' means a controlling undertaking and its controlled undertakings;
(17) 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State of the Union for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings;	(17) 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State of the Union for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings**, a part thereof, or another form of cooperation between undertakings, such as an alliance**;
(18) 'child' means any person below the age of 18 years;	**~~(18)~~ Deleted in favour of amendment to article 8.**
(19) 'supervisory authority' means a public authority which is established by a Member State in accordance with Article 46.	(19) 'supervisory authority' means a public authority which is established by a Member State in accordance with Article 46. **(20) 'professional information' means any personal data relating to the professional capacity of the data subject, such as name, employer, job title, function, business address, business phone or fax number, business e-mail address or other organizational details.** **(21) 'user-generated content' means any content published by the data subject through an information society service, including, but not limited to, personal profile information, digital images, video, blogs, postings on forums, and audio files.** **(22) 'Scientific research' means fundamental research, applied research, and privately funded research.** *Justification 4.1* *The suggested definitions of 'data subject' and 'personal data' outline the techniques used to identify data subjects, whilst they should emphasise the principle of identification and the context of processing, similar to the definition in the 95/46 Directive. Article 4 (1) of the proposal defines the*

	data subject by providing a list of data that are considered personal, such as online identifiers, geolocation data and identification numbers. This contradicts Article 10 and recitals 23 and 24 of the proposal which argue that certain data do not necessarily permit to identify a data subject and that 'principles of protection should apply to any information concerning an identified or identifiable person'. *Moreover, data that is used by a controller in identifying individuals is often processed in a pseudonymised way by a different controller or by a different department within the company (data minimisation). The accounting department will use personal data for billing purposes, whilst research and development use aggregated data to identify buying trends.* *In light of developing technologically neutral and broadly applicable legislation which stimulates the data minimisation, privacy by design, and adequate security measures the definition of personal data and data subject should focus on the on the principle of identifiabillity.* ***Justification 4.7*** *To reduce the burden of obligations of the controller with respect to disclosures to recipients, the scope of the definition has been reduced to third-party controllers. Third party data controllers are the most relevant from a privacy perspective, as they are not a natural part of the data processing. The processor is excluded, as under data protection principles the processor is considered to be "part of the organization of the controller".* ***Justification 4.8*** *Consent should be able to be given in various ways, dependent on the context and circumstances, as long as it is reasonable to assume that it has been given free, specifically and informed. When entering a television studio through a door that states 'you might be recorded behind this door', a data subject consents by entering through the door. This is not 'an explicit indication of wishes', but context and circumstances (television studio, door, sign) make it likely enough for the data subject to have consented.* ***Justification 4.13*** *To clarify the concept of main establishment, the relevant criteria of determining the lead authority in the Binding Corporate Rules approval procedure has been added (see Article 29 Working Party document WP 107).* ***Justification 4.18 (deleted)*** *The concept of child is irrelevant to the Regulation from a legal perspective. Therefore, it is not necessary to define it.* ***Justification 4.20 (new):*** *A definition of 'professional information' needs to be included in the regulation, in order to be able to exclude personal data being professional information from certain articles. Without these exclusions (art 85a) normal business processes will be choked.* ***Justification 4.21 (new):*** *A definition of 'user-generated content' needs to be included in the regulation, in order to be able to use it in the*

	relevant articles. *Justification 4.22 (new)* *This definition incorporates Recital 126 into the definitions of Article 4.*
Article 5 **Principles relating to personal data processing** Personal data must be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject; (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; (c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data; (d) accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay; (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the data will be processed solely for historical, statistical or scientific research purposes in accordance with the rules and conditions of Article 83 and if a periodic review is carried out to assess the necessity to continue the storage; (f) processed under the responsibility and liability of the controller, who shall ensure and demonstrate for each processing operation the compliance with the provisions of this Regulation.	**Article 5** **Principles relating to personal data processing** **1.** Personal data must be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject; (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; (c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data; (d) accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay; (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the data will be processed solely for historical, statistical or scientific research purposes in accordance with the rules and conditions of Article 83 **as well as for dispute resolution purposes ~~and if a periodic review is carried out to assess the necessity to continue the storage~~**; (f) processed under the responsibility and liability of the controller, who shall ensure and demonstrate for each processing operation the compliance with the provisions of this Regulation. **2. Notwithstanding paragraph 5.1(b), further processing of personal data for purposes not compatible with the purpose or purposes for which the data were collected only be allowed if the further processing has a legal basis in one of the grounds referred to in Article 6(1)(a) to (d).** **3. In order to determine whether the further processing is compatible with the purposes for which the personal data were collected, the controller shall take into account:** **(a) the relationship between the purpose of the further processing and the purpose for which the data were collected;** **(b) the nature of the data concerned;** **(c) the consequences of the further processing for the data subject; and** **(d) the extent to which appropriate measures and safeguards have been put in place to protect the interests of the data subject.** *Justification 5.2 (new):* *Article 6(4) introduces the possibility of further processing of data for incompatible purposes in cases where another legal basis can be found in grounds for legitimate processing in points (a) to (d) of article 6(1). This paragraph should be added to article 5(2) as it is an exception to a principle of processing as reflected in art. 5(1)(b). The*

	ground 'public task' has been deleted from the Commission's proposal as such processing should meet the compatibility test of article 5.3(new). ***Justification 5.3 (new):*** *Article 5(3) provides the criteria for assessing compatible use of data, similar to the current criteria provided for in the Dutch Personal Data Protection Act.*
Article 6 **Lawfulness of processing** 1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of their personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks. 2. Processing of personal data which is necessary for the purposes of historical, statistical or scientific research shall be lawful subject to the conditions and safeguards referred to in Article 83. 3. The basis of the processing referred to in points (c) and (e) of paragraph 1 must be provided for in: (a) Union law, or (b) the law of the Member State to which the controller is subject. The law of the Member State must meet an objective of public interest or must be necessary to protect the rights and freedoms of others, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued. 4. Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract. 5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in point (f) of paragraph 1 for various sectors and data processing situations, including as regards the processing of personal	**Article 6** **Lawfulness of processing** 1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of their personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by ~~a~~ **the** controller **or a third party**, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks. 2. Processing of personal data which is necessary for the purposes of historical, statistical or scientific research shall be lawful subject to the conditions and safeguards referred to in Article 83. 3. The basis of the processing referred to in points (c) and (e) of paragraph 1 must be provided for in: (a) Union law, or (b) the law of the Member State to which the controller is subject. The law of the Member State must meet an objective of public interest or must be necessary to protect the rights and freedoms of others, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued. **4. (transferred to art. 5.2)** 5. **Deleted**

data related to a child.	*Justification 6.1* *Although this was already allowed under the wording of the Commission ("a controller"), the amendment restores the wording of Directive 95/46 and clarifies that the data may be disclosed to a third party.* *Justification 6.4 (moved):* *This paragraph should be moved to article 5(2) as it provides an exception to a principle of processing as stated in Article 5(1)(b).* *Justification 6.5 (deleted):* *There is no need for such power, as further specifications would hamper changes and innovation.*
Article 7 **Conditions for consent** 1. The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes. 2. If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter. 3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. 4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.	**Article 7** **Conditions for consent** 1. The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes. 2. If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter. 3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. **4. (deleted in favour of alternative below)** *Justification 7.4 (deleted):* *The assumption that when there is significant imbalance, consent is not be given freely, and therefore not valid, is too simplistic. Only when it is unlikely that the consent is given freely because of such imbalance, consent should not provide legal basis. Recital 34, including the proposed Amendment thereto, is sufficient to get the point of possible imbalance and its consequences for consent across. There is no need to have it incorporated in Article 7.*
Article 8 **Processing of personal data of a child** 1. For the purposes of this Regulation, in relation to the offering of information society services directly to a child, the processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that consent is given or authorised by the child's parent or custodian. The controller shall make reasonable efforts to obtain verifiable consent, taking into consideration available technology.	**Article 8** **Processing of personal data of a child** 1. For the purposes of this Regulation, in relation to the offering of information society services **directed** to a child **below the age of 13 years**, the processing of **the child's** personal data ~~**of a child below the age of 13 years**~~ shall only be lawful if and to the extent that consent **for the processing of the child's personal data** is given or **the child's use of the service has been** authorised by ~~**the**~~ **a** ~~**child's**~~ parent or custodian **of the child**. The controller shall make reasonable efforts to obtain ~~**verifiable**~~ **such** consent **in a verifiable manner**, taking into consideration available technology. **When relying on the authorisation of the parent or custodian, the information society service provider shall provide such parent or custodian with the information as referred to in Article 14(1) in a clear and conspicuous manner. Such information shall at least**

	contain information as to the consequences of the processing of the personal data for the child and the method of objecting to the processing pursuant to Article 19(1). **1a. Paragraph 1 shall not apply in case:** **(a) the controller merely answers a question of a child;** **(b) the data are processed in order to obtain the consent of the parent or guardian.**
2. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.	2. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.
3. 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 methods to obtain verifiable consent referred to in paragraph 1. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.	3. 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 methods to obtain verifiable consent referred to in paragraph 1. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.
4. The Commission may lay down standard forms for specific methods to obtain verifiable consent referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	4. The Commission may lay down standard forms for specific methods to obtain verifiable consent referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2). *Justification 8.1* *The addition of the word 'directed' is more appropriate. Controllers not targeting their services to a child should not be subject to an extended form of consent. Since this is not the intention of the information society service to target a child, but only a consequence of the internet being open for everyone, the controller should not bear an extra burden.* *Justification 8.1a (new):* *This addition reflects justified processing of children's data, similar to the exceptions mentioned in the US Children Online Privacy Protection Act (COPPA). Furthermore, VNO-NCW takes the view that parents should supervise the use of the internet by their (young) children. To avoid that controllers and parents run into practical problems as a consequence of the requirement to obtain consent, VNO-NCW proposes to use some form of 'implied consent' by requiring ISSP's to put emphasis on clear and conspicuous information to the parents (e.g., by putting a clearly visible link to **Information for Parents**) rather than obtaining consent, where the parents are OK with the use of the website or service. Such information should, apart from the information described in Article 14.1, detail at least the consequences of the processing of the child's data for the child and the method of objecting to the processing pursuant to Article 19(1).*
Article 9 **Processing of special categories of personal data** 1. The processing of personal data, revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions or related security measures shall be prohibited.	**Article 9** **Processing of special categories of personal data** 1. The processing of personal data, revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or **offences and** criminal convictions or related security measures shall be prohibited.

2. Paragraph 1 shall not apply where: (a) the data subject has given consent to the processing of those personal data, subject to the conditions laid down in Articles 7 and 8, except where Union law or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; or (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller in the field of employment law in so far as it is authorised by Union law or Member State law providing for adequate safeguards; or (c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent; or (d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other non-profitseeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed outside that body without the consent of the data subjects; or (e) the processing relates to personal data which are manifestly made public by the data subject; or (f) processing is necessary for the establishment, exercise or defence of legal claims; or (g) processing is necessary for the performance of a task carried out in the public interest, on the basis of Union law, or Member State law which shall provide for suitable measures to safeguard the data subject's legitimate interests; or (h) processing of data concerning health is necessary for health purposes and subject to the conditions and safeguards referred to in Article 81; or (i) processing is necessary for historical, statistical or scientific research purposes subject to the conditions and safeguards referred to in Article 83; or (j) processing of data relating to criminal convictions or related security measures is carried out either under the control of official authority or when the processing is necessary for compliance with a legal or regulatory obligation to which a controller is subject, or for the performance of a task carried out for important public interest reasons, and in so far as authorised by Union law or Member State law providing for adequate safeguards. A complete register of criminal convictions shall be kept only under the control of official authority.	2. Paragraph 1 shall not apply where: (a) the data subject has given consent to the processing of those personal data, subject to the conditions laid down in Articles 7 and 8, except where Union law or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; or (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller in the field of employment law in so far as it is authorised by Union law or Member State law providing for adequate safeguards; or (c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent; or (d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other non-profitseeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed outside that body without the consent of the data subjects; or (e) the processing relates to personal data which are manifestly made public by the data subject; or (f) processing is necessary for the establishment, exercise or defence of legal claims; or (g) processing is necessary for the performance of a task carried out in the public interest, on the basis of Union law, or Member State law which shall provide for suitable measures to safeguard the data subject's legitimate interests; or (h) processing of data concerning health is necessary for health purposes and subject to the conditions and safeguards referred to in Article 81; or (i) processing is necessary for historical, statistical or scientific research purposes subject to the conditions and safeguards referred to in Article 83~~; or~~ ~~(j) processing of data relating to criminal convictions or related security measures is carried out either under the control of official authority or when the processing is necessary for compliance with a legal or regulatory obligation to which a controller is subject, or for the performance of a task carried out for important public interest reasons, and in so far as authorised by Union law or Member State law providing for adequate safeguards. A complete register of criminal convictions shall be kept only under the control of official authority~~. **3. Paragraph 1 shall also not apply** where processing of data relating to **offences,** criminal convictions or related security measures is carried out: (a) under the control of official authority; (b) when the processing is necessary for compliance with a legal or regulatory obligation to which a controller is subject; (c) when the processing is necessary for the performance of a task carried out for important public interest reasons, and in so far as authorised by Union law or Member State law providing for adequate safeguards; **(d) when the processing is necessary for the assessment of a request of the data subject to provide a service to him or**

	the assessment of an application of the data subject to take a decision against him, and insofar the controller has provided for adequate safeguards to protect the interests of the data subject; **(e) when the processing is necessary for the protection of the legitimate interests of a controller or a group company or to prevent harm to his employees, customers, or persons for which the controller has a duty of care, and insofar the controller has provided for adequate safeguards to protect the interests of the data subject.** **The processing of other data mentioned in paragraph 1 shall be allowed insofar as such processing is necessary in addition to the processing of offences, criminal convictions or related security measures as specified in this paragraph.** A complete register of criminal convictions shall be kept only under the control of official authority.
3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria, conditions and appropriate safeguards for the processing of the special categories of personal data referred to in paragraph 1 and the exemptions laid down in paragraph 2.	**4.** The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria, conditions and appropriate safeguards for the processing of the special categories of personal data referred to in paragraph 1 and the exemptions laid down in paragraph 2 and 3. *Justification 9.1* *To ensure that data about criminal activity may be processed by the controller, the wording 'offences' has been added (see also art. 8 Directive 95/46). The justified processing of data about criminal activity by the controller (e.g., theft, fraud, bribery, etc) is mentioned in paragraph 3 (new).* *Justification 9.2* *Paragraph 2 sub(j) is given a separate paragraph to be able to provide more detail.* *Justification 9.3* *Paragraph 3 sub (d) and (e) provide organizations with possibilities to protect themselves from for instance fraud or violence against employees. Data relating to offences, criminal convictions or security measures is required by the financial sector in order to detect and prevent fraud. In the insurance sector, for example, data relating to offences, criminal convictions or security measures is indispensable in order to execute a proper risk assessment during the acceptance procedure, determining the coverage and for claims handling. Furthermore, any controller may process data about criminal activity by using surveillance camera's or by detecting hacking activities on its network.*
Article 10 **Processing not allowing identification** If the data processed by a controller do not permit the controller to identify a natural person, the controller shall not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation.	
Article 11 **Transparent information and communication** 1. The controller shall have transparent and easily accessible policies with regard to the processing of personal data and for the exercise of data subjects' rights.	**Article 11** **Transparent information and communication** The controller shall ~~**have**~~ **provide** in a transparent and easily accessible **manner** ~~**policies**~~ **the information referred to in Article 14** ~~**with regard to the processing of personal**~~

	~~data~~ and **information on** ~~for~~ the exercise of data subjects' rights.
2. The controller shall provide any information and any communication relating to the processing of personal data to the data subject in an intelligible form, using clear and plain language, adapted to the data subject, in particular for any information addressed specifically to a child.	2. The controller shall, **having regard to the state of the art, the cost of the implementation , the risks of the processing and the nature of the data to be protected**, provide ~~any~~ **appropriate** information and ~~any~~ communication relating to the processing of personal data to the data subject in an intelligible form, using clear and plain language, adapted to the data subject, in particular for any information addressed specifically to a child. *Justification (11 par 1):* *The changes are technical. One does not provide 'policies', but information in a 'notice', which reflect the policies.* *Justification (11 par 2):* *The information should be appropriate to the risks, the costs and the nature of the data.*
Article 12 **Procedures and mechanisms for exercising the rights of the data subject** 1. The controller shall establish procedures for providing the information referred to in Article 14 and for the exercise of the rights of data subjects referred to in Article 13 and Articles 15 to 19. The controller shall provide in particular mechanisms for facilitating the request for the actions referred to in Article 13 and Articles 15 to 19. Where personal data are processed by automated means, the controller shall also provide means for requests to be made electronically. 2. The controller shall inform the data subject without delay and, at the latest within one month of receipt of the request, whether or not any action has been taken pursuant to Article 13 and Articles 15 to 19 and shall provide the requested information. This period may be prolonged for a further month, if several data subjects exercise their rights and their cooperation is necessary to a reasonable extent to prevent an unnecessary and disproportionate effort on the part of the controller. The information shall be given in writing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject. 3. If the controller refuses to take action on the request of the data subject, the controller shall inform the data subject of the reasons for the refusal and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy. 4. The information and the actions taken on requests referred to in paragraph 1 shall be free of charge. Where requests are manifestly excessive, in particular because of their repetitive character, the controller may charge a fee for providing the information or taking the action requested, or the controller may not take the action requested. In that case, the controller shall bear the burden of proving the manifestly excessive character of the request.	**Article 12** **Procedures and mechanisms for exercising the rights of the data subject** 1. The controller shall establish procedures for providing the information referred to in Article 14 and for the exercise of the rights of data subjects referred to in Article 13 and Articles 15 to 19. The controller shall provide in particular mechanisms for facilitating the request for the actions referred to in Article 13 and Articles 15 to 19. ~~Where personal data are processed by automated means, the controller shall also provide means for requests to be made electronically.~~ 2. The controller shall inform the data subject without delay and, at the latest within ~~one month~~ **four weeks** of receipt of the request, whether or not any action has been taken pursuant to Article 13 and Articles 15 to 19 and shall provide the requested information. This period may be prolonged for a further ~~month~~ **4 weeks**, if several data subjects exercise their rights and their cooperation is necessary to a reasonable extent to prevent an unnecessary and disproportionate effort on the part of the controller. The information shall be given in writing. ~~Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.~~ 3. If the controller refuses to take action on the request of the data subject, the controller shall inform the data subject of the reasons for the refusal and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy. 4. The information and the actions taken on requests referred to in paragraph 1 shall be free of charge. Where requests are **vexatious or** manifestly excessive, in particular because of their repetitive character, **or where the request requires a disproportionate effort on the part of the controller,** the controller may charge a fee for providing the information or taking the action requested, or the controller may not take the action requested. In that case, the controller shall bear the burden of proving the manifestly excessive **or unfounded** character of the

	request.
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 manifestly excessive requests and the fees referred to in paragraph 4.	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 manifestly excessive requests and the fees referred to in paragraph 4.
6. The Commission may lay down standard forms and specifying standard procedures for the communication referred to in paragraph 2, including the electronic format. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized enterprises. 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 and specifying standard procedures for the communication referred to in paragraph 2, including the electronic format. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized enterprises. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2). *Justification 12.1* *Art 12.1 already obliges controllers to establish procedures for providing the information referred to in Article 14 and for the exercise of the rights of data subjects referred to in Article 13 and Articles 15 to 19. The choice of how to provide the information should be left to the controller.* *Justification 12.2* *See justification under 12.1.* *Furthermore, as months have different lengths, it is more practical to use a fixed deadline of 4 weeks.* *Justification 12.4* *Controllers should be protected from abusive use of the rights of data subjects referred to in Article 13 and Articles 15 to 19.*
Article 13 **Rights in relation to recipients** The controller shall communicate any rectification or erasure carried out in accordance with Articles 16 and 17 to each recipient to whom the data have been disclosed, unless this proves impossible or involves a disproportionate effort.	**Article 13** **Rights in relation to recipients** 1. The controller shall communicate any rectification ~~**or erasure**~~ carried out in accordance with Articles 16 ~~**and 17**~~ to each recipient to whom the data have been disclosed, unless this proves impossible, involves a disproportionate effort, **or where the disclosure was based on a legal obligation**. **2. Paragraph 1 shall not apply to the publication of user-generated content by information society service providers.** *Justification 13.1* *The erasure of the data with controller A does not influence the erasure with controller B, as the processing by controller B is not dependent on the lawfulness or the purposes of the processing by controller A. Therefore, the reference to article 17 should be removed.* *Most disclosures to third party controllers (e.g., government agencies, social security organizations, etc) take place on the basis of a legal obligation. To lower the burden of compliance with article 13.1, such disclosures should be excluded.* *Justification 13.2 (new)* *If personal data have been published, e.g., on social networks or websites, the service provider operating the service should not be required to comply with article 13.1.*
Article 14	**Article 14**

Information to the data subject 1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information: (a) the identity and the contact details of the controller and, if any, of the controller's representative and of the data protection officer; (b) the purposes of the processing for which the personal data are intended, including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1); (c) the period for which the personal data will be stored; (d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data; (e) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority; (f) the recipients or categories of recipients of the personal data; (g) where applicable, that the controller intends to transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission; (h) any further information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected.	**Information to the data subject** 1. Where personal data relating to a data subject are collected, the controller shall ~~**provide**~~ **make available to** the data subject ~~**with**~~ at least the following information: (a) the identity and the contact details of the controller ~~**and**~~ **or**, if any, of the controller's representative ~~**and of the data protection officer**~~; (b) the purposes of the processing for which the personal data are intended, ~~**including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1)**~~; ~~**(c) the period for which the personal data will be stored;**~~ ~~**(d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data;**~~ ~~**(e) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;**~~ ~~**(f) the recipients or categories of recipients of the personal data;**~~ ~~**(g) where applicable, that the controller intends to transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission;**~~ (**c**) any further information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected.
2. Where the personal data are collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, whether the provision of personal data is obligatory or voluntary, as well as the possible consequences of failure to provide such data.	**2. (deleted)**
3. Where the personal data are not collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, from which source the personal data originate.	**2**. Where the personal data are not collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, from which source the personal data originate.
4. The controller shall provide the information referred to in paragraphs 1, 2 and 3: (a) at the time when the personal data are obtained from the data subject; or (b) where the personal data are not collected from the data subject, at the time of the recording or within a reasonable period after the collection, having regard to the specific circumstances in which the data are collected or otherwise processed, or, if a disclosure to another recipient is envisaged, and at the latest when the data are first disclosed.	**3**. The controller shall provide the information referred to in paragraphs 1, 2 and 3: (a) at the time when the personal data are obtained from the data subject; or (b) where the personal data are not collected from the data subject, at the time of the recording or within a reasonable period after the collection, having regard to the specific circumstances in which the data are collected or otherwise processed, or, if a disclosure to another recipient is envisaged, and at the latest when the data are first disclosed.
5. Paragraphs 1 to 4 shall not apply, where: (a) the data subject has already the information referred to in paragraphs 1, 2 and 3; or (b) the data are not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort; or	**4**. Paragraphs 1 to 4 shall not apply, where: (a) the data subject has already the information referred to in paragraphs 1, 2 and 3; or (b) the data are not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort; or

(c) the data are not collected from the data subject and recording or disclosure is expressly laid down by law; or (d) the data are not collected from the data subject and the provision of such information will impair the rights and freedoms of others, as defined in Union law or Member State law in accordance with Article 21.	(c) the data are not collected from the data subject and recording or disclosure is expressly laid down by law; or (d) the data are not collected from the data subject and the provision of such information will impair the rights and freedoms of others, as defined in Union law or Member State law in accordance with Article 21.
6. In the case referred to in point (b) of paragraph 5, the controller shall provide appropriate measures to protect the data subject's legitimate interests.	**5**. In the case referred to in point (b) of paragraph 5, the controller shall provide appropriate measures to protect the data subject's legitimate interests.
7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria for categories of recipients referred to in point (f) of paragraph 1, the requirements for the notice of potential access referred to in point (g) of paragraph 1, the criteria for the further information necessary referred to in point (h) of paragraph 1 for specific sectors and situations, and the conditions and appropriate safeguards for the exceptions laid down in point (b) of paragraph 5. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized-enterprises.	**6. (deleted)**
8. The Commission may lay down standard forms for providing the information referred to in paragraphs 1 to 3, taking into account the specific characteristics and needs of various sectors and data processing situations where necessary. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	**6. (deleted)** ***Justification 14.1*** *The complexity and variety of data processing situations demands flexibility with regard to the information provided at certain instances. Furthermore, requiring such detailed specifications would be against the consumer-friendly nature of "layered privacy notices", which have successfully been introduced by many businesses under the current Directive.* *The controller should be able to provide a data subject with information, but the current text literally forces the controller to pro-actively take action. Therefore we choose to support the wording 'make available'.* *Moreover sub (b) to (g) should be removed: if applicable they already follow from sub (h).* ***Justification 14.2*** *Should be deleted: This is a strange article, since the principle of data minimization is in place. If there is no ground for asking for information, the information should not be asked for. Furthermore, please note that 'mandatory data' on registration forms are there to ensure that the proper follow-up can be given to the registration. But every data element on the registration form should serve a purpose.* ***Justification 14.7 and 14.8 (deleted)*** *The complexity and variety of data processing situations demands flexibility with regard to the information provided at certain instances and the way such information is provided. Additional regulation would only reduce that flexibility.*

Article 15 **Right of access for the data subject** 1. The data subject shall have the right to obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed. Where such personal data are being processed, the controller shall provide the following information: (a) the purposes of the processing; (b) the categories of personal data concerned; (c) the recipients or categories of recipients to whom the personal data are to be or have been disclosed, in particular to recipients in third countries; (d) the period for which the personal data will be stored; (e) the existence of the right to request from the controller rectification or erasure of personal data concerning the data subject or to object to the processing of such personal data; (f) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority; (g) communication of the personal data undergoing processing and of any available information as to their source; (h) the significance and envisaged consequences of such processing, at least in the case of measures referred to in Article 20.	**Article 15** **Right of access for the data subject** 1. The data subject shall have the right to obtain from the controller at ~~**any time**~~ **reasonable intervals**, on request, confirmation as to whether or not personal data relating to the data subject are being processed. **The controller may ask the data subject for further information to enable the data controller to locate the personal data which that person seeks.** **2.** Where such personal data are being processed **in order to be aware and verify the lawfulness of the processing**, the controller shall provide the following information: (a) the purposes of the processing; (b) the categories of personal data concerned; (c) the recipients or categories of recipients to whom the personal data are to be or have been disclosed, in particular to recipients in third countries; (d) the **intended** period for which the personal data will be stored, **insofar such information is available**; (e) the existence of the right to request from the controller rectification or erasure of personal data concerning the data subject or to object to the processing of such personal data; ~~**(f) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;**~~ (g) communication of the personal data undergoing processing and of any available information as to their source; (h) the significance and envisaged consequences of such processing, at least in the case of measures referred to in Article 20.
2. The data subject shall have the right to obtain from the controller communication of the personal data undergoing processing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.	**3. To the extent to verify the lawfulness of the processing,** the data subject shall have the right to obtain from the controller communication of the personal data undergoing processing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.
3. 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 communication to the data subject of the content of the personal data referred to in point (g) of paragraph 1.	3. **(deleted)**
4. The Commission may specify standard forms and procedures for requesting and granting access to the information referred to in paragraph 1, including for verification of the identity of the data subject and communicating the personal data to the data subject, taking into account the specific features and necessities of various sectors and data processing situations. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	4. The Commission may specify standard forms and procedures for requesting and granting access to the information referred to in paragraph 1, including for verification of the identity of the data subject and communicating the personal data to the data subject, taking into account the specific features and necessities of various sectors and data processing situations. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2). *Justification 15.1, 15.2 (new) and 15.3 (new)* *This amendment is related to the amendment to 51. It recalls that the access right of the data subject aims at enabling the data subject to be aware and verify the lawfulness of the processing. By specifying the purpose of*

	the access right it strikes a balance between the fundamental right of the individual and the interest of companies in preventing vexatious requests and fishing expeditions. The burden of proof remains with the controller though. *Furthermore, the controller should only be required to provide information as to the intended time for which the data will be stored and only insofar as possible. In many cases, data are collected for purposes for which have no specific data retention period, as the retention period depends on the continued existence of a purpose. E.g., customer billing data are retained for as long as the customer relationship exists. The same is true for many employee data, which are only erased after the employment term has ended.* *The reference to the supervisory authority has been deleted because 1) the supervisory authority authorized to deal with the issue may not be the supervisory authority of the Member State in which the data subject resides, 2) the information would create a false expectation with the data subject that the supervisory authority will actually hear the complaint (quod non, as the supervisory authority is not obligated to hear the complaint), and 3) the information with regard to the address may be subject to change. The addition to 15.1 refers to the last sentence of recital 45 of the Commission's proposal.* ***Justification 15.3 (deletion)*** *Delegated acts are not necessary in this case.*
Article 16 **Right to rectification** The data subject shall have the right to obtain from the controller the rectification of personal data relating to them which are inaccurate. The data subject shall have the right to obtain completion of incomplete personal data, including by way of supplementing a corrective statement.	**Article 16** **Right to rectification** **1.** The data subject shall have the right to obtain from the controller the rectification of personal data relating to them which are inaccurate. The data subject shall have the right to obtain completion of incomplete personal data, including by way of supplementing a corrective statement. **2. The controller shall restrict processing of personal data where their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data.** **3. Paragraph 1 shall not apply to user-generated content, with the exception of content, which is of a defamatory nature.** ***Justification 16.2 (new)*** *This paragraph was moved from article 17.4, since it belongs in this article 16.* ***Justification 16.3 (new)*** *User generated content (any content published by the data subject through an information society service) is out of the hands of the information society service provider. Only when content is defamatory, the service provider may have a duty to care for the data subject.*
Article 17 **Right to be forgotten and to erasure**	**Article 17** **Right to ~~be forgotten and to~~ erasure**

1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies: (a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data; (c) the data subject objects to the processing of personal data pursuant to Article 19; (d) the processing of the data does not comply with this Regulation for other reasons.	1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, ~~especially in relation to personal data which are made available by the data subject while he or she was a child~~, where one of the following grounds applies: (a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data; (c) the data subject ~~objects~~ **has successfully objected** to the ~~processing~~ **collection or retention** of personal data pursuant to Article 19; (d) the processing of the data does not comply with ~~this Regulation for other reasons~~ **Articles 5, 6, 8 and 9**.
2. Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.	**2. (deleted in favour of art. 17a new)**
3. The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary: (a) for exercising the right of freedom of expression in accordance with Article 80; (b) for reasons of public interest in the area of public health in accordance with Article 81; (c) for historical, statistical and scientific research purposes in accordance with Article 83; (d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued; (e) in the cases referred to in paragraph 4.	**2**. The controller shall carry out the erasure without **unreasonable** delay. **3. The controller may deny a request for erasure where** the ~~retention~~ **processing** of the personal data is necessary: (a) for exercising the right of freedom of expression in accordance with Article 80; (b) for reasons of public interest in the area of public health in accordance with Article 81; (c) for historical, statistical and scientific research purposes in accordance with Article 83; (d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued; (e) in the cases referred to in paragraph 4.
4. Instead of erasure, the controller shall restrict processing of personal data where: (a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data; (b) the controller no longer needs the personal data for the accomplishment of its task but they have to be maintained for purposes of proof; (c) the processing is unlawful and the data subject opposes their erasure and requests the restriction of their use instead; (d) the data subject requests to transmit the personal data into another automated processing system in accordance	**4.** Instead of erasure, the controller shall restrict processing of personal data where: ~~(a)~~ **(move to 16.2 new)** (b) the ~~controller no longer needs the personal data for the accomplishment of its task but they~~ **data** have to be maintained for purposes of proof; ~~(c)~~ **(deleted, as this is proposal does not make sense in practice)** ~~(d)~~ **(deleted, per deletion art. 18.2)** **The controller shall erase the personal data when the purpose of proof no longer exists, except where the data are necessary for other purposes.**

with Article 18(2).	**5. Where personal data have been recorded in a manner, which physically does not allow the data to be erased, and where such storage medium also contains other personal data, which should not be erased, the controller shall, instead of erasing the data, may deny the request for erasure and inform the data subject about such impossibility to erase the data.**
5. Personal data referred to in paragraph 4 may, with the exception of storage, only be processed for purposes of proof, or with the data subject's consent, or for the protection of the rights of another natural or legal person or for an objective of public interest.	~~**5. Personal data referred to in paragraph 4 may, with the exception of storage, only be processed for purposes of proof, or with the data subject's consent, or for the protection of the rights of another natural or legal person or for an objective of public interest.**~~
6. Where processing of personal data is restricted pursuant to paragraph 4, the controller shall inform the data subject before lifting the restriction on processing.	~~**6. Where processing of personal data is restricted pursuant to paragraph 4, the controller shall inform the data subject before lifting the restriction on processing.**~~
7. The controller shall implement mechanisms to ensure that the time limits established for the erasure of personal data and/or for a periodic review of the need for the storage of the data are observed.	**6**. The controller shall implement mechanisms to ensure that the time limits established for the erasure of personal data**, if any,** ~~**and/or for a periodic review of the need for the storage of the data**~~ are observed.
8. Where the erasure is carried out, the controller shall not otherwise process such personal data.	~~**8. Where the erasure is carried out, the controller shall not otherwise process such personal data.**~~
9. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying: (a) the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations; (b) the conditions for deleting links, copies or replications of personal data from publicly available communication services as referred to in paragraph 2; (c) the criteria and conditions for restricting the processing of personal data referred to in paragraph 4.	~~**9. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying:**~~ ~~**(a) the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations;**~~ ~~**(b) the conditions for deleting links, copies or replications of personal data from publicly available communication services as referred to in paragraph 2;**~~ ~~**(c) the criteria and conditions for restricting the processing of personal data referred to in paragraph 4.**~~ ***Justification 17 title*** *The text proposed by the Commission is misleading.* ***Justification 17.1*** *Only when there are no legitimate grounds for processing the data, the data can be erased. Objection to processing is not a ground for erasing data. Only successful objection provides this ground for erasure.* ***Justification 17.2 (deleted)*** *Paragraph 18(2) has been deleted in favour of article 17a new.* ***Justification 17.2 (new) and 17.3 (new)*** *For reasons of clarity par. 3 (old) has been split.* *In order to allow for some organisational flexibility in complying with this obligation, the word "reasonable" has been added.* *The changes in par. 3 (new) are technical and the result of the split.* ***Justification 17.4 (new)*** *Ad a): This section has been moved to article 16(2) new, as*

	the situation described in sub a has nothing to do with erasure. If the accuracy of the data is contested, the data should be updated if necessary, not deleted. *Ad b): These changes are technical, as , this purpose of proof are also a "need".* *Ad c): This section has been deleted as it describes an unusual situation and could be seen as an incentive to process data illegally.* *Ad d): As VNO-NCW proposes to delete article 18(2), this section is no longer needed. In any case, the fact that a data subject invokes his right to data portability does not necessarily mean that the data should be erased on the part of the original controller. The right to data portability, as drafted, could also be used to obtain copy of the data and not leave the services of the original controller.* ***Justification 17.5 (new)*** *Some storage media do not allow individual data to be erased (e.g., microfiche or back-up tapes).* ***Justification 17.5 (deleted)*** *This paragraph does not fit the system of erasure. Therefore it has been deleted.* ***Justification 17.6 (deleted)*** *This paragraph has been redrafted to reflect the proposed changes in par. 4 and moved to par. 4 last sentence.* ***Justification 17.6 (new)*** *As often the controller does not know upfront how long the data are needed and therefore has no retention schedule, the wording "if any" has been added. The deleted part of the sentence is superfluous.* ***Justification 17.8 (deleted)*** *This paragraph is superfluous.* ***Justification 17.9 (deleted)*** *It is undesirable that the Commission may adopt delegated acts with respect to article 17. This should be left to the discretion of the controller and the supervision by the supervisory authority.*
	Article 17a **Notice and take down** **Without prejudice to the laws and regulations put in place by the Member States pursuant to Article 80(1), where the personal data have been published via the service of an information society service provider, such information society service provider shall provide the data subject with easily accessible means to have the personal data be removed from the service or to request their removal from the service.** ***Justification 17a (new):*** *In order to allow data to be erased from the internet, the data subject should have the right to have personal data contained in user-generated content, like photos, videos, blogs, etc, be removed from internet platforms, such as social media and search engines. As the provider of such platform does not control the reasons of the publication, the service provider should only be required to offer a Notice and Take Down procedure. However, for reasons of*

	freedom of expression, etc, the service provider should not be put in a position to judge the basis of the request.
Article 18 **Right to data portability** 1. The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject.	**Article 18** **Right to data portability** 1. The data subject shall have the right, where ~~**personal data**~~ **his user-generated content,** ~~are processed~~ **is published** ~~**by electronic means and in a structured and commonly used format**~~ **through an information society service**, to obtain from the ~~**controller**~~ **information society service provider** a copy of **such content,** ~~**data undergoing processing in an electronic and structured format**~~ which ~~**is commonly used and**~~ allows for further use by the data subject.
2. Where the data subject has provided the personal data and the processing is based on consent or on a contract, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn.	2. **(deleted, in favour of paragraph 1)** **2. Paragraph 1 shall be without prejudice to the continued processing of the user-generated content in connection with the provision the service to the data subject by the information society service provider referred to in paragraph 1.**
3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	3. **(deleted in view of deletion in paragraph 1)** ***Justification 18.1 and 18.2*** *As the purposes of collection of personal data are determined by the controller, many personal data are not suited to be transferred to another controller (e.g., billing data, job performance records, logging info, etc). Furthermore, a data portability right implies an obligation of the next controller to collect the data. This does not fit the concept of controller.* *Therefore, in line with the Commission's intention, the right to data portability has been restricted to user-generated content only created in the context of an internet society service.*
Article 19 **Right to object** 1. The data subject shall have the right to object, on grounds relating to their particular situation, at any time to the processing of personal data which is based on points (d), (e) and (f) of Article 6(1), unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject.	**Article 19** **Right to object** 1. The data subject shall have the right to object, on grounds relating to their particular situation, at any time to the processing of personal data which is based on points ~~**(d),**~~ (e) and (f) of Article 6(1)~~**, unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject**~~. **2. Where an objection is justified, the particular processing to which the objection was made, shall be terminated, unless the legitimate grounds as referred to in**

	Article 6(1) sub (e) or (f) override the interests or fundamental rights and freedoms of the data subject. The controller shall inform the data subject of his decision and, if the request is denied, of the arguments underlying the decision.
2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object free of charge to the processing of their personal data for such marketing. This right shall be explicitly offered to the data subject in an intelligible manner and shall be clearly distinguishable from other information.	**3**. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object free of charge to the processing of their personal data for such marketing. This right shall be explicitly offered to the data subject **at the time of the collection if the data by the controller,** in an intelligible manner and ~~**shall be**~~ clearly distinguishable from other information.
3. Where an objection is upheld pursuant to paragraphs 1 and 2, the controller shall no longer use or otherwise process the personal data concerned.	3. **(deleted, see sub 2 new)** ***Justification 19.1 and 19.2*** *Technical change. The wording of the Commission is not correct, as it would mean that the legitimate interests under 6.1(f) now would need to be 'compelling', therefore effectively requiring extra weight of such interest. This should not be the case (and was not the case in Directive 95/46). The right to objection means that the general weighing of interests of Art. 6.1() now needs to be 'individualised' for the data subject concerned. This means that the same interests of the controller as the ones mentioned in Article 6.1(f) need to be taken into account. It's the interests of the data subject that need to be compelling in the sense that they should override the generic balancing of interests under Article 6.1(f). This amendment restores the system of the right of objection as mentioned in Directive 95/46.* ***Justification 9.3 (deleted)*** *Paragraph 19.3 wrongly suggests that in case the data subject objects against a certain processing of his data, the controller can no longer process the personal data concerned. The Article should recognise that the controller can no longer process data for the specific purpose the data subject has objected to. Processing is "any operation…", so the right to object can and should be applies in a granular way. For example, if the data subject objects to the use of his postal address for direct marketing, the controller should still be allowed to process the address for billing purposes. Therefore, Article 19.3 has been deleted. The correct objective has been added to Article 19.2(new).* ***Justification 19.3 (new)*** *In order to be able to implement the second sentence of Art. 19.3, it is important to determine at what moment in time the obligation exists.*
Article 20 **Measures based on profiling** 1. Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences,	**Article 20** **~~Measures~~ Decisions based on ~~profiling~~ automated processing** 1. **(deleted)**

reliability or behaviour.	
2. Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 only if the processing: (a) is carried out in the course of the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention; or (b) is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or (c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards.	**1**. Subject to the other provisions of this Regulation, **in particular Articles 14, 15 and 16**, a person may be subjected to a ~~**measure of the kind referred to in paragraph 1**~~ **decision which produces legal effects concerning this natural person and adversely affects this natural person, based solely on automated processing intended to evaluate certain personal aspects relating to this person or to analyse or predict in particular the person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour, is lawful** only if ~~**the processing:**~~ ~~**(a) is carried out in the course of the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where**~~ suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention.~~**; or**~~ ~~**(b) is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or**~~ ~~**(c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards;**~~
3. Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be based solely on the special categories of personal data referred to in Article 9.	**2**. Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be based solely on the special categories of personal data referred to in Article 9.
4. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject.	**3**. In the cases referred to in paragraph ~~**2**~~ **1**, the information to be provided by the controller under Article 14 shall include information as to the existence of processing ~~**for a measure**~~ **following a decision** of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject.
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 suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2.	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 suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2. ***Justification - Title*** *The title of the provision should be 'Decisions based on automated processing', as is the case in Article 15 of the 95/46 Directive.* ***Justification 20.1 (deletion)*** *The Commission's proposal takes a negative approach to profiling, which ignores the fact that profiling may also have positive effects on individuals. The deletion and subsequent amendment of Article 20.2 takes a more neutral approach. Profiling is allowed if the data subject is aware of it (art. 14) and has the possibility to access the personal information used (art. 15) and change them if wrong (art. 16). This has been addressed in the amendment to article 20.2.* ***Justification 20.2*** *The deletion of a) to c) is based on the Recommendation CM/Rec(2010)13 of the Council of Europe, which allows*

	profiling to be based on all six grounds mentioned in article 6.1 of this Regulation, not only consent, contract and law. VNO-NCW does not see any justification to deviate from the Council of Europe's Recommendation and to limit the grounds for profiling to the ones proposes by the Commission. Therefore, the amendment to Article 20.2 restores the system that article 6.1 applies to all data processing, so also to profiling and now only requires that in such case suitable safeguards are taken.
Article 21 **Restrictions** 1. Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in points (a) to (e) of Article 5 and Articles 11 to 20 and Article 32, when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard: (a) public security; (b) the prevention, investigation, detection and prosecution of criminal offences; (c) other public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters and the protection of market stability and integrity; (d) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions; (e) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (a), (b), (c) and (d); (f) the protection of the data subject or the rights and freedoms of others. 2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least as to the objectives to be pursued by the processing and the determination of the controller.	**Article 21** **Restrictions** 1. ~~**Union or Member State law may restrict by way of a legislative measure the scope of the.**~~ **The controller may restrict the** obligations and rights provided for in points (a) to (e) of Article 5 and Articles 11 to 20 and Article 32, when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard: (a) public security; (b) the prevention, investigation, detection and prosecution of criminal offences; (c) other public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters and the protection of market stability and integrity; (d) the prevention, investigation, detection and prosecution of breaches of ethics **or confidentiality obligations** ~~**for regulated professions;**~~ (e) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (a), (b), (c) and (d); **(f) the protection of health, safety and security of individuals;** **(g) the overriding business interests of the controller, in particular the protection of intellectual property rights, trade secrets or reputation or the preservation of confidentiality in business transactions;** (**h**) the protection of the data subject or the rights and freedoms of others. 2. ~~**In particular, any**~~ **The Union or Member States may adopt** legislative measure **restricting the rights** referred to in paragraph 1 **for the purposes referred to in paragraph 1 section (a) to (h), which** shall contain specific provisions at least as to the objectives to be pursued by the processing and the determination of the controller. ***Justification 21.1*** *Because the Regulation does not need to be implemented into national law, the wording of Directive 95/46, which was copied in this article and which required implementation into national law, should be changed into a direct right. This allows controllers to apply Article 21.1 without having to wait for national law to be created. Furthermore, the circumstances as allowed in binding corporate rules based on the implementation of Directive 95/46 and which have been thoroughly negotiated with the members of the Article 29 Working Party, have been added in (d), (f) and (g).* ***Justification 21.2*** *This allows the Union and Member States to adopt*

	legislative measures as originally intended by the Commission's proposal.
Article 22 **Responsibility of the controller** 1. The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.	**Article 22** **Responsibility of the controller** 1. The controller shall adopt **appropriate** policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.
2. The measures provided for in paragraph 1 shall in particular include: (a) keeping the documentation pursuant to Article 28; (b) implementing the data security requirements laid down in Article 30; (c) performing a data protection impact assessment pursuant to Article 33; (d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2); (e) designating a data protection officer pursuant to Article 35(1).	2. The measures provided for in paragraph 1 shall in particular include: (a) keeping the documentation pursuant to Article 28; (b) implementing the data security requirements laid down in Article 30; (c) performing a data protection impact assessment pursuant to Article 33; (d) complying with the requirements for prior authorisation ~~**or prior consultation**~~ of the supervisory authority pursuant to Article 34(1) and (2); (e) designating a data protection officer pursuant to Article 35(1).
3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors.	3. The controller shall implement **appropriate** mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors.
	4. Paragraphs 1, 2 and 3 of this article, do not apply to controllers, which are part of a group of undertakings, provided such group of undertakings, through its main establishment or otherwise, has implemented a common framework of policies and measures as referred to in paragraphs 1 and 2, which cover the processing of personal data by such controllers.
	5. Paragraphs 1 and 3 shall also not apply if and insofar as the controller is subject to a similar obligation by virtue of Union law and under supervision of an independent sectorial supervisory authority.
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.	6. **(deleted)** *Justification 22.1* *This allows for a risk-based approach.* *Justification 22.2* *In view of the deletion of Article 34.2 the reference to prior consultation has been deleted.* *Justification 22.3* *This allows for a risk-based approach.* *Justification 22.4 (new)* *Where controllers are part of a group, it is expected that the*

	group, most probably through its main establishment, has implemented a common framework of policies and measures to comply with this Regulation (e.g., by adopting Binding Corporate Rules as referred to in article 43). Where such common framework exists, the controllers are shall not have the obligation to implement their own policies and measures pursuant to Article 22(1) and (2), but should be allowed to comply with the common framework instead. ***Justification 22.5 (new)*** *In some regulated sectors, such as the financial sector, the national legislator has imposed similar obligations as listed in this article 22 by virtue of Union or Member State law. Independent sectorial supervisory authorities such as bank regulators deal with compliance issues related to such sector. The proposal also aims to prevent overlapping obligations and conflicts between various supervisory authorities.* ***Justification 22.4 (deleted)*** *There is no need for such powers.*
Article 23 **Data protection by design and by default** 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.	**Article 23** **Data protection by design and by default** 1. **(deleted)**
2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.	2. 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**, other than user-generated content,** are not made accessible to an indefinite number of individuals**, unless justified pursuant to Article 5(a), (b) and (c)**.
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.	3. **(deleted)**
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).	**3**. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2). ***Justification 23.1 (deleted)*** *The obligation in 23.1 is 'compliance by design' rather than 'privacy by design'. As this is obvious, it has been deleted.* ***Justification 23.2*** *- The way user-generated content is disclosed, should be*

	determined by the user, not the controller or ISSP. *- Sometimes the disclosure of data to an indefinite number of people is justified (e.g., in newspaper articles). Therefore, an exception has been added.* ***Justification 23.3 (deleted)*** *There is no need for such powers.*
Article 24 **Joint controllers** 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.	**Article 24** **Joint controllers** **1.** 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. **2. Where no arrangement has been established, the data subject may exercise his rights as referred to in Articles 15 to 20 against any of the controllers involved in the processing.** **3. Paragraph 1 shall not apply where all controllers involved in the processing belong to the same group of undertakings.** ***Justification 24.2*** *The addition would only be logical in view of the protection of the interests of the data subject.* ***Justification 24.3*** *The obligation of par. 23.1 makes no sense in case of joint controllers belonging to the same group (e.g., a multinational), as the group will deal with data protection matters internally on a policy or management basis without formal arrangements between the entities.*
Article 25 **Representatives of controllers not established in the Union** 1. In the situation referred to in Article 3(2), the controller shall designate a representative in the Union. 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 (b) an enterprise employing fewer than 250 persons; or (c) a public authority or body; or (d) a controller offering only occasionally goods or services to data subjects residing in the Union. 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. 4. The designation of a representative by the controller shall be without prejudice to legal actions which could be initiated against the controller itself.	**Article 25** **Representatives of controllers not established in the Union** 1. In the situation referred to in Article 3(2), the controller shall designate a representative in the Union. 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 (b) an enterprise employing fewer than 250 persons; or (c) a public authority or body; or (d) a controller**, who does not direct** ~~**offering only occasionally**~~ goods or services to data subjects residing in the Union. 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. 4. The designation of a representative by the controller shall be without prejudice to legal actions which could be initiated against the controller itself.

	Justification: *See justification to article 3(2).*
Article 26 **Processor** 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.	**Article 26** **Processor** 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.
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: (a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited; (b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality; (c) take all required measures pursuant to Article 30; (d) enlist another processor only with the 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; (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; (h) make available to the controller and the supervisory authority all information necessary to control compliance with the obligations laid down in this Article.	2. The carrying out of processing by a processor shall be governed by a contract or other ~~legal~~ act, **documented in writing,** binding the processor to the controller. ~~and, where appropriate, 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;~~ ~~(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;~~ ~~(c) take all required measures pursuant to Article 30;~~ ~~(d) enlist another processor only with the 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;~~ ~~(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;~~ ~~(h) make available to the controller and the supervisory authority all information necessary to control compliance with the obligations laid down in this Article.~~
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 processor shall provide the controller with all information necessary for the controller to meet his obligations under this Regulation.**
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, the processor shall be considered to be a controller in respect of that processing and **where relevant** shall be subject to the rules on joint controllers laid down in Article 24.
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	**5. (deleted)**

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.	*Justification 26.1* *The deleted text is superfluous.* *Justification 26.2* *It's important that the act 1) is binding, and 2) has been documented in writing. The amendment reflects these requirements.* *Furthermore, not all processor contracts require all elements of par.26.2. The content of processor contracts should be left to legal best practice. Alternatively, the wording "where appropriate" should be added to Art. 26.2.* *Justification 26.3 (deleted)* *This section is superfluous in view of Art. 26.1.* *Justification 26.3 (new)* *It is very important that processors provide the controller with all information necessary for the controller to meet his obligations under the Regulation. Such information may include: information about the security measures taken by the processor, information about any subcontractors working for the processor, information about internal policies and instructions to employees of the processor, the locations of the processing, etc.* *Article 26.4* *There may be cases where the processor processes personal data contrary to the controller's instructions. In such cases, the processor should be the only controller for such (illegal) processing. The requirement of Art. 24 should not apply to such situation.* *Article 26.5* *There is no need for such powers.*
Article 27 **Processing under the authority of the controller and processor** The processor and any person acting under the authority of the controller or of the processor who has access to personal data shall not process them except on instructions from the controller, unless required to do so by Union or Member State law.	**Article 27** **Confidentiality of processing** The processor and any person acting under the authority of the controller or of the processor who has access to personal data shall **keep the personal data confidential and shall** not process them except on instructions from the controller, unless required to do so by Union or Member State law. *Justification 27* *The obligation to keep the data confidential was missing in the Regulation. This obligation provides an important basis for disciplinary measures or termination of the processor contract.*
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.	**Article 28** **Documentation** 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 person**s** 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. **(deleted)**
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 28.1*** *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 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 allowed 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 therefore consistent to allow also for a similar risk-based exemption with regard to the*

	documentation requirements under article 28 and to limit those to processing that pose a high degree of risk for the data subject. *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 department 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.* ***Justification 28.2*** *- the contact details of the controller are known to the controller and irrelevant for the purpose of documentation;* *- the name and contract details of the DPO are known to the controller. Having to document them per set of processing operations would put an unreasonable compliance burden on the controller, as DPO's change.* ***Justification 28.3*** *In all cases, the controller should make the documentation available to the supervisory authority. A corresponding obligation for the processor has been proposed in Art. 26(3) (new).* ***Justification 28.4*** *As size is not relevant, Art. 28.4(b) can be deleted.* ***Justification 28.5*** *There is no need for such powers.*
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	**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.	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 29.3 (new)* *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-á-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 30.1* *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 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 30.2*** *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. 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.	**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 interests, 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),**~~ **T**he 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, 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 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.	**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 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.** **8. Where a personal data breach should be notified pursuant to the breach notification procedure of Directive 2002/58/EC, as amended by Directive 2009/136/EC, paragraph 1 shall not apply.**
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.	**9. (deleted)**
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 31.1*** *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 31.3 (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 31.4 (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 31.5 (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 same breach must be notified in multiple member states, thus reducing the administrative burden.* ***Justification 31.6 (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.* ***Justification 31.8 (new)*** *Telecom providers are already subject to a breach*

	notification procedure pursuant to Directive 2002/58/EC, as amended by Directive 2009/136. To avoid duplication of obligations and notifications to data subjects, this amendment implies that the sector-specific notification procedure takes preference. ***Justification 31.5 (deleted)*** *There is no need for such powers.*
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 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~~**6**).
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. (deleted)**
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).	**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).

	Justification 32.1 *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 32.2* *(see justification to Article 31(4) new).* *Justification 32.4 (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.* *Justification 32.6* *There is no need for such powers.*
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 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.	**Article 33** ~~**Data protection**~~ **Privacy impact assessment** 1. Where processing operations **are likely to** present ~~**specific**~~ **high degree of risk**s 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**~~ **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	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

Opmerking [redacted]: In view of the proposal on 33.5 (new), it should be considered to deleted 32.2 alltogether.

rights and legitimate interests of data subjects and other persons concerned.	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, small and medium-sized enterprises.	**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 level, the establishment of common criteria for determining the level of risk of the processing operations as well as the execution of privacy impact assessments, taking into account the specific features of the various sectors, the size of the controller, the nature of the data, the consequences of the processing for the data subjects and the nature of the processing operations.** ~~**In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.**~~
7. The Commission may specify standards and procedures for carrying out and verifying and auditing the assessment referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	**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 33.1* *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 33.4 (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 33.5 (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. 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. 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	**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. **(deleted)** 3. **(moved to par. 2 – new)**

Opmerking [redacted]: Alternative proposal: the controller should obtain an **authorisation** from the supervisory authority, as consultation does not provide sufficient legal protection for the controller against the position of the supervisory authority.
Furthermore, in order to reduce the administrative burden, such 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 - *alternative*) should require such risk acceptance to be performed by the supervisory authority in the form of an authorisation (e.g., a permit) instead.
Paragraph 2(b) should be 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.

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 par. 2)**
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)**
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.	**2**. The controller ~~**or processor**~~ shall provide the supervisory authority with the ~~**data protection**~~ **privacy** impact assessment ~~**provided for**~~ **as referred to** 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. **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**.
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.	**3**. Member States shall consult the supervisory authority in the preparation of a legislative measure to be adopted by the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects.
8. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for determining the high degree of specific risk referred to in point (a) of paragraph 2.	8. **(deleted)**.
9. The Commission may set out standard forms and procedures for prior authorisations and consultations referred to in paragraphs 1 and 2, and standard forms and procedures for informing the supervisory authorities pursuant to paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	9. The Commission may set out 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 **2**. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2). *Justification 34.1* *Deleted wording is superfluous.* *Justification 34.2 (deleted)* *The requirement to consult with the supervisory authority as proposed by the Commission does not provide sufficient legal protection for controllers against the position of the supervisory authority. Therefore, in order to further reduce the administrative burden, and in view of the information*

	provision of par. 34.6 (old), the provision has been deleted. ***Justification 34.3 (deleted)*** *This provision has been moved to par. 34.2 (new).* ***Justification 34.4 and 34.5 (deleted)*** *These paragraphs are not relevant anymore after the deletion of par. 34.2 (old).* ***Justification 34.8 (deleted)*** *There is no need for such powers.*
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 **public** 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, on the processing related to its core activities, especially core activities which by virtue of their nature, scope or purposes require regular and systematic monitoring of data subjects, indicates a high degree of risk to the rights and freedoms of data subjects, especially their right to privacy, irrespective of the measures taken by the controller or processor to mitigate such risks**; 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. **(deleted in favour of amendment to 35.1)**
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. **(moved to Recital 75)**
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. **(deleted)** ***Justification 35.1*** *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 appointment of a data protection officer (DPO) should only be required if the data processing operation related to its core activities poses a high risk. Only in such high risk situation, the obligatory appointment of a DPO is justified. In any other case, the appointment of a DPO should be optional. The proposed amendment to article 33(1) also means that the obligation to appoint a DPO cannot apply to the processor. Therefore, the processor has been deleted. Nevertheless, the processor may opt to appoint a DPO.* ***Justification 35.2*** *The deletion matches the amendment to 35.1.* ***Justification 35.4 (deleted)*** *The provision has been moved to 35.1.* ***Justification 35.5 (deleted)*** *The competences of the DPO should be included in the recitals as typically DPO's learn on the job rather than already possessing such competences from the start. Furthermore, it is unlikely that all DPO's have the required competences from day 1 the Regulation is in force. Therefore, the requirement has been deleted.* ***Justification 35.7*** *In view of labour law requirements, the two 2-year term also binds the DPO. Therefore, the minimum term should be deleted, so DPO's may leave their office before the term has ended. Also, the minimum term does not provide any added*

	value to data protection. ***Justification 35.9 and 35.10*** *The role of the DPO should be internally oriented. Allocating external responsibilities to the DPO, such as proposed by par. 10 (deleted), could in some cases significantly impact the time and resources of the DPO. Furthermore, any communication between the organisation of the controller and the data subjects should in principle go via the communication channels determined by the controller. Of course, the controller may decide that the DPO is the point of contact for data protection questions, but this should not be codified.*
Article 36 **Position of the data protection officer** 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. 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.	**Article 36** **Position of the data protection officer** 1. ~~**The controller or the processor shall ensure that**~~ The data protection officer ~~**is**~~ **shall** properly and in a timely manner **be** involved in all issues which relate to the protection of personal data. 2. ~~**The controller or processor shall ensure that**~~ The data protection officer **shall** perform~~**s**~~ 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**~~. 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. *Justification* *This amendment corresponds with the amendment to Article 35(1).*
Article 37 **Tasks of the data protection officer** 1. The controller or the processor shall entrust the data protection officer at least with the following tasks: (a) to inform and advise the controller or the processor of their obligations pursuant to this Regulation and to document this activity and the responses received; (b) to monitor the implementation and application of the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, the training of staff involved in the processing operations, and the related audits; (c) to monitor the implementation and application of this Regulation, in particular as to the requirements related to data protection by design, data protection by default and data security and to the information of data subjects and their requests in exercising their rights under this Regulation; (d) to ensure that the documentation referred to in Article 28 is maintained; (e) to monitor the documentation, notification and communication of personal data breaches pursuant to Articles 31 and 32; (f) to monitor the performance of the data protection impact assessment by the controller or processor and the	**Article 37** **Tasks of the data protection officer** 1. ~~**The controller or the processor shall entrust**~~ The data protection officer **shall be entrusted with** at least ~~**with**~~ the following tasks: (a) to inform and advise the controller or the processor of their obligations pursuant to this Regulation and to document this activity and the responses received; (b) to monitor the implementation and application of the policies ~~**of**~~ **by** the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, the training of staff involved in the processing operations, and the related audits; (c) to monitor the implementation and application of this Regulation, in particular as to the requirements related to data protection by design, data protection by default and data security and to the information of data subjects and their requests in exercising their rights under this Regulation; (d) to ensure that the documentation referred to in Article 28 is maintained; (e) to monitor the documentation, notification and communication of personal data breaches pursuant to Articles 31 and 32; (f) to monitor the performance of the data protection

application for prior authorisation or prior consultation, if required 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; (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.	impact assessment by the controller or processor and the application for prior authorisation ~~**or prior consultation**~~, if required 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; (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.
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.	2. **(deleted)** *Justification 37.1* *The amendment matches the amendments to Article 35(1) and 34(2).* *Furthermore, any communication between the organisation of the controller and the supervisory authority should in principle go via management. Of course, the controller may decide that the DPO is the point of contact for the supervisory authority for a specific issue, but this should not be codified.* *Justification 37.2* *There is no need for such powers.*
Article 38 **Codes of conduct** 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: (a) fair and transparent data processing; (b) the collection of data; (c) the information of the public and of data subjects; (d) requests of data subjects in exercise of their rights; (e) information and protection of children; (f) transfer of data to third countries or international organisations; (g) mechanisms for monitoring and ensuring compliance with the code by the controllers adherent to it; (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.	**Article 38** **Codes of conduct** 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:**~~ ~~**(a) fair and transparent data processing;**~~ ~~**(b) the collection of data;**~~ ~~**(c) the information of the public and of data subjects;**~~ ~~**(d) requests of data subjects in exercise of their rights;**~~ ~~**(e) information and protection of children;**~~ ~~**(f) transfer of data to third countries or international organisations;**~~ ~~**(g) mechanisms for monitoring and ensuring compliance with the code by the controllers adherent to it;**~~ ~~**(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.**~~ **Associations and other bodies representing categories of controllers or processors in one or more Member States are encouraged to draw up codes of conduct intended to contribute to the proper application of this Regulation as appropriate for their specific sector, technology or context. Compliance with an approved code of conduct by the parties covered by such code is deemed to be compliance with this Regulation unless and until overturned by a court of law. Any issues not regulated by**

	the code are regulated by this Regulation.
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 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.	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~~ **for approval to** the supervisory authority in that Member State. The supervisory authority ~~may~~ **shall** 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.
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.	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.
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 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).
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. ***Justification 38.1*** *The creation of codes of conduct further stimulates compliance with the Regulation. However, VNO-NCW believes that the question whether a code is necessary or beneficial should be left to the appreciation of the sector at hand and not be a task of the Member States, the supervisory authorities or the Commission (as per the Commission's proposal). Furthermore, in order to stimulate the creation of codes of conduct and to avoid conflicts over the status of a code of conduct in relation to the Regulation, it is clarified that compliance with a code of conduct by the parties covered by the code is deemed to be compliance with the Regulation.* ***Justification 38.2*** *The supervisory authority should formally approve the code, not just give an opinion. This gives the submitting party judicial remedies and provides legal clarity to the data subjects whose personal data are covered by the code, therefore increasing legal certainty as to the status of the code. Furthermore, the supervisory authority should always give an opinion, regardless of the outcome of its review.*
Article 39 **Certification** 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. 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. 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).	
Article 40 **General principle for transfers** Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation may only take place if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation.	**Article 40** **General principle for transfers** Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation may only take place if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor~~, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation~~. *Justification* *The deletion of the words "including ..... organization" have been deleted because they do not add anything to or clarify in any way the main sentence.*
Article 41 **Transfers with an adequacy decision** 1. A transfer may take place where the Commission has decided that the third country, or a territory or a processing sector within that third country, or the international organisation in question ensures an adequate level of protection. Such transfer shall not require any further authorisation. 2. When assessing the adequacy of the level of protection, the Commission shall give consideration to the following elements: (a) the rule of law, relevant legislation in force, both general and sectoral, including concerning public security, defence, national security and criminal law, the professional rules and security measures which are complied with in that country or by that international organisation, as well as effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred; (b) the existence and effective functioning of one or more independent supervisory authorities in the third country or international organisation in question responsible for	**Article 41** **Transfers with an adequacy decision** 1. A transfer may take place where the Commission **or the controller** has decided that the third country, or a territory or a processing sector within that third country, or the international organisation in question ensures an adequate level of protection. Such transfer shall not require any further authorisation. 2. When assessing the adequacy of the level of protection, the Commission **or the controller** shall give consideration to the following elements: (a) **the nature of the data, the purpose and duration of the proposed processing operation or operations, and the country of origin and the country of destination of the data;** (**b**) the rule of law, relevant legislation in force, both general and sectoral, including concerning public security, defence, national security and criminal law, the professional rules and security measures which are complied with in that country or by that international organisation, as well as effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred; (**c**) the existence and effective functioning of one or more independent supervisory authorities in the third country or international organisation in question responsible for

ensuring compliance with the data protection rules, for assisting and advising the data subjects in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States; and (c) the international commitments the third country or international organisation in question has entered into.	ensuring compliance with the data protection rules, for assisting and advising the data subjects in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States; and (**d**) the international commitments the third country or international organisation in question has entered into.
3. The Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	3. The Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).
4. The implementing act shall specify its geographical and sectoral application, and, where applicable, identify the supervisory authority mentioned in point (b) of paragraph 2.	4. The implementing act shall specify its geographical and sectoral application, and, where applicable, identify the supervisory authority mentioned in point (b) of paragraph 2.
5. The Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organisation does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, in particular in cases where the relevant legislation, both general and sectoral, in force in the third country or international organisation, does not guarantee effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2), or, in cases of extreme urgency for individuals with respect to their right to personal data protection, in accordance with the procedure referred to in Article 87(3).	5. The Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organisation does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, in particular in cases where the relevant legislation, both general and sectoral, in force in the third country or international organisation, does not guarantee effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2), or, in cases of extreme urgency for individuals with respect to their right to personal data protection, in accordance with the procedure referred to in Article 87(3).
6. Where the Commission decides pursuant to paragraph 5, any transfer of personal data to the third country, or a territory or a processing sector within that third country, or the international organisation in question shall be prohibited, without prejudice to Articles 42 to 44. At the appropriate time, the Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation resulting from the Decision made pursuant to paragraph 5 of this Article.	6. Where the Commission decides pursuant to paragraph 5, any transfer of personal data to the third country, or a territory or a processing sector within that third country, or the international organisation in question**, with the exception of personal data which originated in such country,** shall be prohibited, without prejudice to Articles 42 to 44. At the appropriate time, the Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation resulting from the Decision made pursuant to paragraph 5 of this Article. **The Commission should seek the views of relevant stakeholders prior to taking such decision.**
7. The Commission shall publish in the *Official Journal of the European Union* a list of those third countries, territories and processing sectors within a third country and international organisations where it has decided that an adequate level of protection is or is not ensured.	7. The Commission shall publish in the *Official Journal of the European Union* a list of those third countries, territories and processing sectors within a third country and international organisations where it has decided that an adequate level of protection is or is not ensured.
8. Decisions adopted by the Commission on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC shall remain in force, until amended, replaced or repealed by the Commission.	8. Decisions adopted by the Commission on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC shall remain in force, until amended, replaced or repealed by the Commission. *Justification 41.1* *Certain national laws currently implementing Directive*

	95/46 leave to the experience and responsibility of the data controller the assessment of whether a country offers an adequate level of protection. This current possibility needs to get back in the text of the Regulation. ***Justification 41.6*** *Some companies store the data of their employees or customers residing in such country in a datacenter in the EU. In such case, the prohibition would prohibit such companies from re-transferring such data to such country. Therefore, such re-transfers should be excluded, unless trade with such country is also prohibited.* *Furthermore, such prohibition may significantly impact the economic interests of companies or sectors. Therefore, such companies or sectors should be given the possibility to express their views.*
Article 42 **Transfers by way of appropriate safeguards** 1. Where the Commission has taken no decision pursuant to Article 41, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has adduced appropriate safeguards with respect to the protection of personal data in a legally binding instrument. 2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by: (a) binding corporate rules in accordance with Article 43; or (b) standard data protection clauses adopted by the Commission. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2); or (c) standard data protection clauses adopted by a supervisory authority in accordance with the consistency mechanism referred to in Article 57 when declared generally valid by the Commission pursuant to point (b) of Article 62(1); or (d) contractual clauses between the controller or processor and the recipient of the data authorised by a supervisory authority in accordance with paragraph 4. 3. A transfer based on standard data protection clauses or binding corporate rules as referred to in points (a), (b) or (c) of paragraph 2 shall not require any further authorisation. 4. Where a transfer is based on contractual clauses as referred to in point (d) of paragraph 2 of this Article the controller or processor shall obtain prior authorisation of the contractual clauses according to point (a) of Article 34(1) from the supervisory authority. If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57. 5. Where the appropriate safeguards with respect to the protection of personal data are not provided for in a legally binding instrument, the controller or processor shall obtain prior authorisation for the transfer, or a set of transfers, or	**Article 42** **Transfers by way of appropriate safeguards** 1. Where the Commission has taken no decision pursuant to Article 41, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has adduced appropriate safeguards with respect to the protection of personal data in a legally binding instrument. 2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by: (a) binding corporate rules in accordance with Article 43; or (b) standard data protection clauses adopted by the Commission. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2); or (c) standard data protection clauses adopted by a supervisory authority in accordance with the consistency mechanism referred to in Article 57 when declared generally valid by the Commission pursuant to point (b) of Article 62(1); or (d) contractual clauses between the controller or processor and the recipient of the data authorised by a supervisory authority in accordance with paragraph 4. 3. A transfer based on standard data protection clauses or binding corporate rules as referred to in points (a), (b) or (c) of paragraph 2 shall not require any further authorisation. 4. Where a transfer is based on contractual clauses as referred to in point (d) of paragraph 2 of this Article the controller or processor shall obtain prior authorisation of the contractual clauses according to point (a) of Article 34(1) from the supervisory authority. If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57. 5. ~~Where the appropriate safeguards with respect to the protection of personal data are not provided for in a legally binding instrument, the controller or processor shall obtain prior authorisation for the~~ **Any other measure to adduce appropriate safeguards to a** transfer, or a set of transfers, or for provisions to be inserted into

for provisions to be inserted into administrative arrangements providing the basis for such transfer. Such authorisation by the supervisory authority shall be in accordance with point (a) of Article 34(1). If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57. Authorisations by a supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid, until amended, replaced or repealed by that supervisory authority.	administrative arrangements providing the basis for such transfer, **shall require the authorization of the supervisory authority**. Such authorisation by the supervisory authority shall be in accordance with point (a) of Article 34(1). If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57. Authorisations by a supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid, until amended, replaced or repealed by that supervisory authority. *Justification 42.5* *This amendment provides for a flexible residual category of adducing appropriate safeguards, allowing 'legal innovation', similar to the Binding Corporate Rules under Directive 95/46.*
Article 43 **Transfers by way of binding corporate rules** 1. A supervisory authority shall in accordance with the consistency mechanism set out in Article 58 approve binding corporate rules, provided that they: (a) are legally binding and apply to and are enforced by every member within the controller's or processor's group of undertakings, and include their employees; (b) expressly confer enforceable rights on data subjects; (c) fulfil the requirements laid down in paragraph 2. 2. The binding corporate rules shall at least specify: (a) the structure and contact details of the group of undertakings and its members; (b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question; (c) their legally binding nature, both internally and externally; (d) the general data protection principles, in particular purpose limitation, data quality, legal basis for the processing, processing of sensitive personal data; measures to ensure data security; and the requirements for onward transfers to organisations which are not bound by the policies; (e) the rights of data subjects and the means to exercise these rights, including the right not to be subject to a measure based on profiling in accordance with Article 20, the right to lodge a complaint before the competent supervisory authority and before the competent courts of the Member States in accordance with Article 75, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules; (f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member of the group of undertakings not established in the Union; the controller or the processor may only be exempted from this liability, in whole or in part, if he proves that that member is not responsible for the event giving rise to the damage; (g) how the information on the binding corporate rules, in	**Article 43** **Transfers by way of binding corporate rules** 1. A supervisory authority shall in accordance with the consistency mechanism set out in Article 58 approve binding corporate rules, provided that they: (a) are legally binding and apply to and are enforced by every member within the controller's or processor's group of undertakings, and include their employees; (b) expressly confer enforceable rights on data subjects; (c) fulfil the requirements laid down in paragraph 2. 2. The binding corporate rules shall at least ~~specify~~ **provide a general description of**: (a) the structure and contact details of the group of undertakings and its members; (b) the data transfers or set of transfers, ~~**including the categories of personal data, the type of processing and its purposes**~~, the type of data subjects affected and the identification of the third country or countries in question; (c) their legally binding nature, both internally and externally; (d) the general data protection principles, in particular purpose limitation, data quality, legal basis for the processing, processing of sensitive personal data; measures to ensure data security; and the requirements for onward transfers to organisations which are not bound by the policies; (e) the rights of data subjects and the means to exercise these rights, including the right not to be subject to a measure based on profiling in accordance with Article 20, the right to lodge a complaint before the competent supervisory authority and before the competent courts of the Member States in accordance with Article 75, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules; (f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member of the group of undertakings not established in the Union; the controller or the processor may only be exempted from this liability, in whole or in part, if he proves that that member is not responsible for the event giving rise to the damage;

particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in accordance with Article 11; (h) the tasks of the data protection officer designated in accordance with Article 35, including monitoring within the group of undertakings the compliance with the binding corporate rules, as well as monitoring the training and complaint handling; (i) the mechanisms within the group of undertakings aiming at ensuring the verification of compliance with the binding corporate rules; (j) the mechanisms for reporting and recording changes to the policies and reporting these changes to the supervisory authority; (k) the co-operation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, in particular by making available to the supervisory authority the results of the verifications of the measures referred to in point (i) of this paragraph.	(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in accordance with Article 11; (h) the tasks of the data protection officer designated in accordance with Article 35, including monitoring within the group of undertakings the compliance with the binding corporate rules, as well as monitoring the training and complaint handling; (i) the mechanisms within the group of undertakings aiming at ensuring the verification of compliance with the binding corporate rules; (j) the mechanisms for reporting and recording changes to the policies and reporting these changes to the supervisory authority; (k) the co-operation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, in particular by making available to the supervisory authority the results of the verifications of the measures referred to in point (i) of this paragraph. **3. The supervisory authority may authorise the transfer of personal data to other parties than the members of the group of undertakings on the basis of the binding corporate rules of such group of undertakings, provided that appropriate measures have been taken to legally bind such other party to the binding corporate rules.**
3. 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 binding corporate rules within the meaning of this Article, in particular as regards the criteria for their approval, the application of points (b), (d), (e) and (f) of paragraph 2 to binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned.	**4. (deleted)**
4. The Commission may specify the format and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).	**5**. The Commission may specify the format and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2). *Justification 43.2* *The substitution of the word "specify" for "provide a general description of" ensures that BCRs remain effective and do not become rapidly obsolete. A specification beforehand of all the aspects mentioned in a) through k) would result in that the BCRs of a company would quickly become obsolete. This would occur for example if a change in the structure of the group of undertakings takes place or other people replace those who have previously been mentioned in the BCRs as contact persons.* *The words "including" up to "purposes" of Article 43 .2 b) have been deleted since the BCRs provide for the rules according to which the controller will have to process any categories of data. It is impossible to know beforehand which categories of data will a controller process. What is important is that whatever new data category is processed,*

	such processing occurs according to the rules set out in the BCRs. The same applies to the processing and its purposes. Every time that a controller would like to process data for a new purpose, such purpose should be assessed in the light of the rules set out in the BCRs. It is not possible to think beforehand for which purposes will data controllers who are bound by BCRs will need to process data. If such purposes were listed, BCRs should be amended every time in order to accommodate the new processing or purpose. This would render BCRs very quickly obsolete. ***Justification 43.3 (new)*** *This amendment responds to the need of offering a plausible option for complicated infrastructure deals, such as the provision of services such as helpdesks, the establishment and administration of data centers, cloud storage, between controllers and processors.* ***Justification 43.3 (deleted)*** *There is no need for such powers.*
Article 44 **Derogations** 1. In the absence of an adequacy decision pursuant to Article 41, or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that: (a) the data subject has consented to the proposed transfer, after having been informed of the risks of such transfers due to the absence of an adequacy decision and appropriate safeguards; or (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; or (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; or (d) the transfer is necessary for important grounds of public interest; or (e) the transfer is necessary for the establishment, exercise or defence of legal claims; or (f) the transfer is necessary in order to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving consent; or (g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case; or (h) the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, which cannot be qualified as frequent or massive, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data,	**Article 44** **Derogations** 1. In the absence of an adequacy decision pursuant to Article 41, or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that: (a) the data subject has consented to the proposed transfer, after having been informed of the risks of such transfers due to the absence of an adequacy decision and appropriate safeguards; or (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; or (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; or (d) the transfer is necessary for important grounds of public interest; or (e) the transfer is necessary for the establishment, exercise or defence of legal claims; or (f) the transfer is necessary in order to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving consent; or (g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case; ~~or~~ (h) the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, which cannot be qualified as ~~frequent~~ **structural** or massive, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data,

where necessary.	where necessary; **or** **(i) the transfer is based on a decision of the European Commission to exempt specific categories of transfers**.
2. A transfer pursuant to point (g) of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. When the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.	2. A transfer pursuant to point (g) of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. When the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.
3. Where the processing is based on point (h) of paragraph 1, the controller or processor shall give particular consideration to the nature of the data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and adduced appropriate safeguards with respect to the protection of personal data, where necessary.	3. Where the processing is based on point (h) of paragraph 1, the controller or processor shall give particular consideration to the nature of the data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and adduced appropriate safeguards with respect to the protection of personal data, where necessary.
4. Points (b), (c) and (h) of paragraph 1 shall not apply to activities carried out by public authorities in the exercise of their public powers.	4. Points (b), (c) and (h) of paragraph 1 shall not apply to activities carried out by public authorities in the exercise of their public powers.
5. The public interest referred to in point (d) of paragraph 1 must be recognised in Union law or in the law of the Member State to which the controller is subject.	5. The public interest referred to in point (d) of paragraph 1 must be recognised in Union law or in the law of the Member State to which the controller is subject.
6. The controller or processor shall document the assessment as well as the appropriate safeguards adduced referred to in point (h) of paragraph 1 of this Article in the documentation referred to in Article 28 and shall inform the supervisory authority of the transfer.	6. The controller or processor shall document the assessment as well as the appropriate safeguards adduced referred to in point (h) of paragraph 1 of this Article in the documentation referred to in Article 28 ~~**and shall inform the supervisory authority of the transfer**~~.
7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying 'important grounds of public interest' within the meaning of point (d) of paragraph 1 as well as the criteria and requirements for appropriate safeguards referred to in point (h) of paragraph 1.	7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying 'important grounds of public interest' within the meaning of point (d) of paragraph 1 as well as the criteria and requirements for appropriate safeguards referred to in point (h) of paragraph 1. ***Justification 44.1*** *Substitution of the word "frequent" for "structural or systematic". This exception is not meant for those transfers carried out in the context of outsourcing. The words "structural or systematic" reflect without doubt the type of transfers that are excluded from falling under this particular exception.* *The addition of a new exception under 44.1.(i): certain categories of data transfers that are unlikely to adversely affect the privacy rights of data subjects and that are necessary to conduct the business of the data controller may be exempted by European Commission. The possibility for the EU Commission to make such exemptions should be included in the Regulation.* ***Justification 44.6*** *In order to reduce the administrative burden, the notification to the supervisory authority should be removed.*
Article 45	

International co-operation for the protection of personal data 1. In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to: (a) develop effective international co-operation mechanisms to facilitate the enforcement of legislation for the protection of personal data; (b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms; (c) engage relevant stakeholders in discussion and activities aimed at furthering international co-operation in the enforcement of legislation for the protection of personal data; (d) promote the exchange and documentation of personal data protection legislation and practice. 2. For the purposes of paragraph 1, the Commission shall take appropriate steps to advance the relationship with third countries or international organisations, and in particular their supervisory authorities, where the Commission has decided that they ensure an adequate level of protection within the meaning of Article 41(3).	
Article 46 **Supervisory authority** 1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application of this Regulation and for contributing to its consistent application throughout the Union, in order to protect the fundamental rights and freedoms of natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the Union. For these purposes, the supervisory authorities shall co-operate with each other and the Commission. 2. Where in a Member State more than one supervisory authority are established, that Member State shall designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the European Data Protection Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 57. 3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to this Chapter, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.	
Article 47 **Independence** 1. The supervisory authority shall act with complete independence in exercising the duties and powers entrusted to it. 2. The members of the supervisory authority shall, in the performance of their duties, neither seek nor take	

instructions from anybody. 3. Members of the supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not. 4. Members of the supervisory authority shall behave, after their term of office, with integrity and discretion as regards the acceptance of appointments and benefits. 5. Each Member State shall ensure that the supervisory authority is provided with the adequate human, technical and financial resources, premises and infrastructure necessary for the effective performance of its duties and powers, including those to be carried out in the context of mutual assistance, co-operation and participation in the European Data Protection Board. 6. Each Member State shall ensure that the supervisory authority has its own staff which shall be appointed by and be subject to the direction of the head of the supervisory authority. 7. Member States shall ensure that the supervisory authority is subject to financial control which shall not affect its independence. Member States shall ensure that the supervisory authority has separate annual budgets. The budgets shall be made public.	
Article 48 **General conditions for the members of the supervisory authority** 1. Member States shall provide that the members of the supervisory authority must be appointed either by the parliament or the government of the Member State concerned. 2. The members shall be chosen from persons whose independence is beyond doubt and whose experience and skills required to perform their duties notably in the area of protection of personal data are demonstrated. 3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement in accordance with paragraph 5. 4. A member may be dismissed or deprived of the right to a pension or other benefits in its stead by the competent national court, if the member no longer fulfils the conditions required for the performance of the duties or is guilty of serious misconduct. 5. Where the term of office expires or the member resigns, the member shall continue to exercise the duties until a new member is appointed.	
Article 49 **Rules on the establishment of the supervisory authority** Each Member State shall provide by law within the limits of this Regulation: (a) the establishment and status of the supervisory authority;	

(b) the qualifications, experience and skills required to perform the duties of the members of the supervisory authority; (c) the rules and procedures for the appointment of the members of the supervisory authority, as well the rules on actions or occupations incompatible with the duties of the office; (d) the duration of the term of the members of the supervisory authority which shall be no less than four years, except for the first appointment after entry into force of this Regulation, part of which may take place for a shorter period where this is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure; (e) whether the members of the supervisory authority shall be eligible for reappointment; (f) the regulations and common conditions governing the duties of the members and staff of the supervisory authority; (g) the rules and procedures on the termination of the duties of the members of the supervisory authority, including in case that they no longer fulfil the conditions required for the performance of their duties or if they are guilty of serious misconduct.	
Article 50 **Professional secrecy** The members and the staff of the supervisory authority shall be subject, both during and after their term of office, to a duty of professional secrecy with regard to any confidential information which has come to their knowledge in the course of the performance of their official duties.	
Article 51 **Competence** 1. Each supervisory authority shall exercise, on the territory of its own Member State, the powers conferred on it in accordance with this Regulation. 2. Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States, without prejudice to the provisions of Chapter VII of this Regulation. 3. The supervisory authority shall not be competent to supervise processing operations of courts acting in their judicial capacity.	**Article 51** **Competence** 1. Each supervisory authority shall exercise, on the territory of its own Member State, the powers conferred on it in accordance with this Regulation. 2. Where the processing of personal data takes place in the context of the activities of an establishment of ~~**a controller or a processor**~~ **an enterprise** in the Union, and the ~~**controller or processor**~~ **enterprise** is established in more than one Member State, the supervisory authority of the main establishment ~~**of the controller or processor**~~ **shall** ~~**be competent**~~ **have final competence** for the supervision of the processing activities of the ~~**controller or the processor**~~ **enterprise** in all Member States, without prejudice to the provisions of Chapter VII of this Regulation. 3. The supervisory authority shall not be competent to supervise processing operations of courts acting in their judicial capacity. *Justification 51.2* *This amendment seeks to provide clarity on how to apply the main establishment rule. Furthermore, the terms controller and processor have been replace by enterprise, as the controller or a particular processing may not be the parent company of the entity in the other Member State.*
Article 52	**Article 52**

Duties 1. The supervisory authority shall: (a) monitor and ensure the application of this Regulation; (b) hear complaints lodged by any data subject, or by an association representing that data subject in accordance with Article 73, investigate, to the extent appropriate, the matter and inform the data subject or the association of the progress and the outcome of the complaint within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary; (c) share information with and provide mutual assistance to other supervisory authorities and ensure the consistency of application and enforcement of this Regulation; (d) conduct investigations either on its own initiative or on the basis of a complaint or on request of another supervisory authority, and inform the data subject concerned, if the data subject has addressed a complaint to this supervisory authority, of the outcome of the investigations within a reasonable period; (e) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices; (f) be consulted by Member State institutions and bodies on legislative and administrative measures relating to the protection of individuals' rights and freedoms with regard to the processing of personal data; (g) authorise and be consulted on the processing operations referred to in Article 34; (h) issue an opinion on the draft codes of conduct pursuant to Article 38(2); (i) approve binding corporate rules pursuant to Article 43; (j) participate in the activities of the European Data Protection Board. 2. Each supervisory authority shall promote the awareness of the public on risks, rules, safeguards and rights in relation to the processing of personal data. Activities addressed specifically to children shall receive specific attention. 3. The supervisory authority shall, upon request, advise any data subject in exercising the rights under this Regulation and, if appropriate, co-operate with the supervisory authorities in other Member States to this end. 4. For complaints referred to in point (b) of paragraph 1, the supervisory authority shall provide a complaint submission form, which can be completed electronically, without excluding other means of communication. 5. The performance of the duties of the supervisory authority shall be free of charge for the data subject. 6. Where requests are manifestly excessive, in particular due to their repetitive character, the supervisory authority may charge a fee or not take the action requested by the data subject. The supervisory authority shall bear the burden of proving the manifestly excessive character of the request.	**Duties** 1. The supervisory authority shall: (a) monitor and ensure the application of this Regulation; (b) hear complaints lodged by any data subject, or by an association representing that data subject in accordance with Article 73, investigate, to the extent appropriate, the matter and inform the data subject or the association of the progress and the outcome of the complaint within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary; (c) share information with and provide mutual assistance to other supervisory authorities and ensure the consistency of application and enforcement of this Regulation; (d) conduct investigations either on its own initiative or on the basis of a complaint or on request of another supervisory authority, and inform the data subject concerned, if the data subject has addressed a complaint to this supervisory authority, of the outcome of the investigations within a reasonable period; (e) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices; (f) ~~be consulted by Member State institutions and bodies on legislative and administrative measures relating to the protection of individuals' rights and freedoms with regard to the processing of personal data;~~ (g) authorise and be consulted on the processing operations referred to in Article 34; (h) issue an opinion on the draft codes of conduct pursuant to Article 38(2); (i) approve binding corporate rules pursuant to Article 43; (j) participate in the activities of the European Data Protection Board. 2. Each supervisory authority shall promote the awareness of the public on risks, rules, safeguards and rights in relation to the processing of personal data. Activities addressed specifically to children shall receive specific attention. 3. The supervisory authority shall, upon request, advise any data subject in exercising the rights under this Regulation and, if appropriate, co-operate with the supervisory authorities in other Member States to this end. 4. For complaints referred to in point (b) of paragraph 1, the supervisory authority shall provide a complaint submission form, which can be completed electronically, without excluding other means of communication. 5. The performance of the duties of the supervisory authority shall be free of charge for the data subject. 6. Where requests are manifestly excessive, in particular due to their repetitive character, the supervisory authority may charge a fee or not take the action requested by the data subject. The supervisory authority shall bear the burden of proving the manifestly excessive character of the request. *Justification 51.2*

	The role of advisor on legislative issues does not match the role of supervisory authority. In the past, supervisory authorities have used this role to actively participate in and sometimes dominate the political debate by seriously lobbying pro or contra a certain bill. *Furthermore, this role 'monopolises' the expert knowledge with the supervisory authority, allowing understaffed legislators to outsource their work to the supervisory authority. VNO-NCW believes that the separation of powers requires that the supervisory authorities do not play a formal role in the legislative process.*
Article 53 **Powers** 1. Each supervisory authority shall have the power: (a) to notify the controller or the processor of an alleged breach of the provisions governing the processing of personal data, and, where appropriate, order the controller or the processor to remedy that breach, in a specific manner, in order to improve the protection of the data subject; (b) to order the controller or the processor to comply with the data subject's requests to exercise the rights provided by this Regulation; (c) to order the controller and the processor, and, where applicable, the representative to provide any information relevant for the performance of its duties; (d) to ensure the compliance with prior authorisations and prior consultations referred to in Article 34; (e) to warn or admonish the controller or the processor; (f) to order the rectification, erasure or destruction of all data when they have been processed in breach of the provisions of this Regulation and the notification of such actions to third parties to whom the data have been disclosed; (g) to impose a temporary or definitive ban on processing; (h) to suspend data flows to a recipient in a third country or to an international organisation; (i) to issue opinions on any issue related to the protection of personal data; (j) to inform the national parliament, the government or other political institutions as well as the public on any issue related to the protection of personal data; 2. Each supervisory authority shall have the investigative power to obtain from the controller or the processor: (a) access to all personal data and to all information necessary for the performance of its duties; (b) access to any of its premises, including to any data processing equipment and means, where there are	**Article 53** **Powers** 1. Each supervisory authority shall have the power: (a) to notify the controller or the processor of an alleged breach of the provisions governing the processing of personal data, and, where appropriate, order the controller or the processor to remedy that breach, in a specific manner, in order to improve the protection of the data subject; (b) to order the controller or the processor to comply with the data subject's requests to exercise the rights provided by this Regulation; (c) to order the controller and the processor, and, where applicable, the representative to provide any information relevant for the performance of its duties; (d) to ensure the compliance with prior authorisations ~~**and prior consultations**~~ referred to in Article 34; (e) to warn or admonish the controller or the processor; (f) to order the rectification, erasure or destruction of all data when they have been processed in breach of the provisions of this Regulation and the notification of such actions to third parties to whom the data have been disclosed; (g) to impose a temporary or definitive ban on processing; (h) to suspend data flows to a recipient in a third country or to an international organisation; (i) to issue opinions on any issue related to the protection of personal data; (j) to inform the national parliament, the government or other political institutions as well as the public on any issue related to the protection of personal data. **2. The supervisory authority shall not disclose information provided to it, where such disclosure could adversely affect the rights and freedoms of others, including the controller or processor. This shall apply particularly to:** **(a) information related to the economic interests and trade secrets of the controller or processor;** **(b) the security measures taken in accordance with article 30;** **(c) information, which Union or Member State law has designated as confidential; and** **(d) information, which may harm the stability or integrity of the market.** **3**. Each supervisory authority shall have the investigative power to obtain from the controller or the processor: (a) access to all personal data and to all information necessary for the performance of its duties; (b) access to any of its premises, including to any data processing equipment and means, where there are

reasonable grounds for presuming that an activity in violation of this Regulation is being carried out there. The powers referred to in point (b) shall be exercised in conformity with Union law and Member State law. 3. Each supervisory authority shall have the power to bring violations of this Regulation to the attention of the judicial authorities and to engage in legal proceedings, in particular pursuant to Article 74(4) and Article 75(2). 4. Each supervisory authority shall have the power to sanction administrative offences, in particular those referred to in Article 79(4), (5) and (6).	reasonable grounds for presuming that an activity in violation of this Regulation is being carried out there. The powers referred to in point (b) shall be exercised in conformity with Union law and Member State law. **4**. Each supervisory authority shall have the power to bring violations of this Regulation to the attention of the judicial authorities and to engage in legal proceedings, in particular pursuant to Article 74(4) and Article 75(2). **5**. Each supervisory authority shall have the power to sanction administrative offences, in particular those referred to in Article 79(4), (5) and (6). *Justification 53.1* *The amendment matches the amendment to Art. 34(2).* *Justification 53.2 (new)* *This amendment seeks to ensure that the information disclosed to the supervisory authority is kept confidential if necessary for the grounds mentioned in this amendment.*
Article 54 **Activity report** Each supervisory authority must draw up an annual report on its activities. The report shall be presented to the national parliament and shall be made be available to the public, the Commission and the European Data Protection Board.	
Article 55 **Mutual assistance** 1. Supervisory authorities shall provide each other relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective co-operation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and prompt information on the opening of cases and ensuing developments where data subjects in several Member States are likely to be affected by processing operations. 2. Each supervisory authority shall take all appropriate measures required to reply to the request of another supervisory authority without delay and no later than one month after having received the request. Such measures may include, in particular, the transmission of relevant information on the course of an investigation or enforcement measures to bring about the cessation or prohibition of processing operations contrary to this Regulation. 3. The request for assistance shall contain all the necessary information, including the purpose of the request and reasons for the request. Information exchanged shall be used only in respect of the matter for which it was requested. 4. A supervisory authority to which a request for assistance is addressed may not refuse to comply with it unless:	

(a) it is not competent for the request; or (b) compliance with the request would be incompatible with the provisions of this Regulation. 5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress or the measures taken in order to meet the request by the requesting supervisory authority. 6. Supervisory authorities shall supply the information requested by other supervisory authorities by electronic means and within the shortest possible period of time, using a standardised format. 7. No fee shall be charged for any action taken following a request for mutual assistance. 8. Where a supervisory authority does not act within one month on request of another supervisory authority, the requesting supervisory authorities shall be competent to take a provisional measure on the territory of its Member State in accordance with Article 51(1) and shall submit the matter to the European Data Protection Board in accordance with the procedure referred to in Article 57. 9. The supervisory authority shall specify the period of validity of such provisional measure. This period shall not exceed three months. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission. 10. The Commission may specify the format and procedures for mutual assistance referred to in this article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	
Article 56 **Joint operations of supervisory authorities** 1. In order to step up co-operation and mutual assistance, the supervisory authorities shall carry out joint investigative tasks, joint enforcement measures and other joint operations, in which designated members or staff from other Member States' supervisory authorities are involved. 2. In cases where data subjects in several Member States are likely to be affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in the joint investigative tasks or joint operations, as appropriate. The competent supervisory authority shall invite the supervisory authority of each of those Member States to take part in the respective joint investigative tasks or joint operations and respond to the request of a supervisory authority to participate in the operations without delay. 3. Each supervisory authority may, as a host supervisory	

authority, in compliance with its own national law, and with the seconding supervisory authority's authorisation, confer executive powers, including investigative tasks on the seconding supervisory authority's members or staff involved in joint operations or, in so far as the host supervisory authority's law permits, allow the seconding supervisory authority's members or staff to exercise their executive powers in accordance with the seconding supervisory authority's law. Such executive powers may be exercised only under the guidance and, as a rule, in the presence of members or staff from the host supervisory authority. The seconding supervisory authority's members or staff shall be subject to the host supervisory authority's national law. The host supervisory authority shall assume responsibility for their actions. 4. Supervisory authorities shall lay down the practical aspects of specific co-operation actions. 5. Where a supervisory authority does not comply within one month with the obligation laid down in paragraph 2, the other supervisory authorities shall be competent to take a provisional measure on the territory of its Member State in accordance with Article 51(1). 6. The supervisory authority shall specify the period of validity of a provisional measure referred to in paragraph 5. This period shall not exceed three months. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission and shall submit the matter in the mechanism referred to in Article 57.	
Article 57 **Consistency mechanism** For the purposes set out in Article 46(1), the supervisory authorities shall co-operate with each other and the Commission through the consistency mechanism as set out in this section.	
Article 58 **Opinion by the European Data Protection Board** 1. Before a supervisory authority adopts a measure referred to in paragraph 2, this supervisory authority shall communicate the draft measure to the European Data Protection Board and the Commission. 2. The obligation set out in paragraph 1 shall apply to a measure intended to produce legal effects and which: (a) relates to 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 (b) may substantially affect the free movement of personal data within the Union; or (c) aims at adopting a list of the processing operations subject to prior consultation pursuant to Article 34(5); or (d) aims to determine standard data protection clauses referred to in point (c) of Article 42(2); or (e) aims to authorise contractual clauses referred to in point (d) of Article 42(2); or (f) aims to approve binding corporate rules within the meaning of Article 43.	

3. Any supervisory authority or the European Data Protection Board may request that any matter shall be dealt with in the consistency mechanism, in particular where a supervisory authority does not submit a draft measure referred to in paragraph 2 or does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with Article 56. 4. In order to ensure correct and consistent application of this Regulation, the Commission may request that any matter shall be dealt with in the consistency mechanism. 5. Supervisory authorities and the Commission shall electronically communicate any relevant information, including as the case may be a summary of the facts, the draft measure, and the grounds which make the enactment of such measure necessary, using a standardised format. 6. The chair of the European Data Protection Board shall immediately electronically inform the members of the European Data Protection Board and the Commission of any relevant information which has been communicated to it, using a standardised format. The chair of the European Data Protection Board shall provide translations of relevant information, where necessary. 7. The European Data Protection Board shall issue an opinion on the matter, if the European Data Protection Board so decides by simple majority of its members or any supervisory authority or the Commission so requests within one week after the relevant information has been provided according to paragraph 5. The opinion shall be adopted within one month by simple majority of the members of the European Data Protection Board. The chair of the European Data Protection Board shall inform, without undue delay, the supervisory authority referred to, as the case may be, in paragraphs 1 and 3, the Commission and the supervisory authority competent under Article 51 of the opinion and make it public. 8. The supervisory authority referred to in paragraph 1 and the supervisory authority competent under Article 51 shall take account of the opinion of the European Data Protection Board and shall within two weeks after the information on the opinion by the chair of the European Data Protection Board, electronically communicate to the chair of the European Data Protection Board and to the Commission whether it maintains or amends its draft measure and, if any, the amended draft measure, using a standardised format.	
Article 59 **Opinion by the Commission** 1. Within ten weeks after a matter has been raised under Article 58, or at the latest within six weeks in the case of Article 61, the Commission may adopt, in order to ensure correct and consistent application of this Regulation, an opinion in relation to matters raised pursuant to Articles 58 or 61. 2. Where the Commission has adopted an opinion in accordance with paragraph 1, the supervisory authority	

concerned shall take utmost account of the Commission's opinion and inform the Commission and the European Data Protection Board whether it intends to maintain or amend its draft measure. 3. During the period referred to in paragraph 1, the draft measure shall not be adopted by the supervisory authority. 4. Where the supervisory authority concerned intends not to follow the opinion of the Commission, it shall inform the Commission and the European Data Protection Board thereof within the period referred to in paragraph 1 and provide a justification. In this case the draft measure shall not be adopted for one further month.	
Article 60 **Suspension of a draft *measure*** 1. Within one month after the communication referred to in Article 59(4), and where the Commission has serious doubts as to whether the draft measure would ensure the correct application of this Regulation or would otherwise result in its inconsistent application, the Commission may adopt a reasoned decision requiring the supervisory authority to suspend the adoption of the draft measure, taking into account the opinion issued by the European Data Protection Board pursuant to Article 58(7) or Article 61(2), where it appears necessary in order to: (a) reconcile the diverging positions of the supervisory authority and the European Data Protection Board, if this still appears to be possible; or (b) adopt a measure pursuant to point (a) of Article 62(1). 2. The Commission shall specify the duration of the suspension which shall not exceed 12 months. 3. During the period referred to in paragraph 2, the supervisory authority may not adopt the draft measure.	
Article 61 **Urgency procedure** 1. In exceptional circumstances, where a supervisory authority considers that there is an urgent need to act in order to protect the interests of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded by means of an alteration of the existing state or for averting major disadvantages or for other reasons, by way of derogation from the procedure referred to in Article 58, it may immediately adopt provisional measures with a specified period of validity. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission. 2. Where a supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion of the European Data Protection Board, giving reasons for requesting such opinion, including for the urgency of final measures. 3. Any supervisory authority may request an urgent opinion where the competent supervisory authority has not taken	

an appropriate measure in a situation where there is an urgent need to act, in order to protect the interests of data subjects, giving reasons for requesting such opinion, including for the urgent need to act. 4. By derogation from Article 58(7), an urgent opinion referred to in paragraphs 2 and 3 of this Article shall be adopted within two weeks by simple majority of the members of the European Data Protection Board.	
Article 62 **Implementing acts** 1. The Commission may adopt implementing acts for: (a) deciding on the correct application of this Regulation in accordance with its objectives and requirements in relation to matters communicated by supervisory authorities pursuant to Article 58 or 61, concerning a matter in relation to which a reasoned decision has been adopted pursuant to Article 60(1), or concerning a matter in relation to which a supervisory authority does not submit a draft measure and that supervisory authority has indicated that it does not intend to follow the opinion of the Commission adopted pursuant to Article 59; (b) deciding, within the period referred to in Article 59(1), whether it declares draft standard data protection clauses referred to in point (d) of Article 58(2), as having general validity; (c) specifying the format and procedures for the application of the consistency mechanism referred to in this section; (d) specifying the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in Article 58(5), (6) and (8). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2). 2. On duly justified imperative grounds of urgency relating to the interests of data subjects in the cases referred to in point (a) of paragraph 1, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 87(3). Those acts shall remain in force for a period not exceeding 12 months. 3. The absence or adoption of a measure under this Section does not prejudice any other measure by the Commission under the Treaties.	
Article 63 **Enforcement** 1. For the purposes of this Regulation, an enforceable measure of the supervisory authority of one Member State shall be enforced in all Member States concerned. 2. Where a supervisory authority does not submit a draft measure to the consistency mechanism in breach of Article 58(1) to (5), the measure of the supervisory authority shall not be legally valid and enforceable.	
Article 64 **European Data Protection Board** 1. A European Data Protection Board is hereby set up.	

2. The European Data Protection Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor. 3. Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, they shall nominate the head of one of those supervisory authorities as joint representative. 4. The Commission shall have the right to participate in the activities and meetings of the European Data Protection Board and shall designate a representative. The chair of the European Data Protection Board shall, without delay, inform the Commission on all activities of the European Data Protection Board.	
Article 65 **Independence** 1. The European Data Protection Board shall act independently when exercising its tasks pursuant to Articles 66 and 67. 2. Without prejudice to requests by the Commission referred to in point (b) of paragraph 1 and in paragraph 2 of Article 66, the European Data Protection Board shall, in the performance of its tasks, neither seek nor take instructions from anybody.	
Article 66 **Tasks of the European Data Protection Board** 1. The European Data Protection Board shall ensure the consistent application of this Regulation. To this effect, the European Data Protection Board shall, on its own initiative or at the request of the Commission, in particular: (a) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Regulation; (b) examine, on its own initiative or on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices addressed to the supervisory authorities in order to encourage consistent application of this Regulation; (c) review the practical application of the guidelines, recommendations and best practices referred to in point (b) and report regularly to the Commission on these; (d) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 57; (e) promote the co-operation and the effective bilateral and multilateral exchange of information and practices between the supervisory authorities; (f) promote common training programmes and facilitate personnel exchanges between the supervisory authorities, as well as, where appropriate, with the supervisory authorities of third countries or of international organisations; (g) promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide.	

2. Where the Commission requests advice from the European Data Protection Board, it may lay out a time limit within which the European Data Protection Board shall provide such advice, taking into account the urgency of the matter. 3. The European Data Protection Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 87 and make them public. 4. The Commission shall inform the European Data Protection Board of the action it has taken following the opinions, guidelines, recommendations and best practices issued by the European Data Protection Board.	
Article 67 **Reports** 1. The European Data Protection Board shall regularly and timely inform the Commission about the outcome of its activities. It shall draw up an annual report on the situation regarding the protection of natural persons with regard to the processing of personal data in the Union and in third countries. The report shall include the review of the practical application of the guidelines, recommendations and best practices referred to in point (c) of Article 66(1). 2. The report shall be made public and transmitted to the European Parliament, the Council and the Commission.	
Article 68 **Procedure** 1. The European Data Protection Board shall take decisions by a simple majority of its members. 2. The European Data Protection Board shall adopt its own rules of procedure and organise its own operational arrangements. In particular, it shall provide for the continuation of exercising duties when a member's term of office expires or a member resigns, for the establishment of subgroups for specific issues or sectors and for its procedures in relation to the consistency mechanism referred to in Article 57.	
Article 69 **Chair** 1. The European Data Protection Board shall elect a chair and two deputy chairpersons from amongst its members. One deputy chairperson shall be the European Data Protection Supervisor, unless he or she has been elected chair. 2. The term of office of the chair and of the deputy chairpersons shall be five years and be renewable.	
Article 70 **Tasks of the chair** 1. The chair shall have the following tasks: (a) to convene the meetings of the European Data Protection Board and prepare its agenda; (b) to ensure the timely fulfilment of the tasks of the European Data Protection Board, in particular in relation to the consistency mechanism referred to in Article 57.	

2. The European Data Protection Board shall lay down the attribution of tasks between the chair and the deputy chairpersons in its rules of procedure.	
Article 71 **Secretariat** 1. The European Data Protection Board shall have a secretariat. The European Data Protection Supervisor shall provide that secretariat. 2. The secretariat shall provide analytical, administrative and logistical support to the European Data Protection Board under the direction of the chair. 3. The secretariat shall be responsible in particular for: (a) the day-to-day business of the European Data Protection Board; (b) the communication between the members of the European Data Protection Board, its chair and the Commission and for communication with other institutions and the public; (c) the use of electronic means for the internal and external communication; (d) the translation of relevant information; (e) the preparation and follow-up of the meetings of the European Data Protection Board; (f) the preparation, drafting and publication of opinions and other texts adopted by the European Data Protection Board.	
Article 72 **Confidentiality** 1. The discussions of the European Data Protection Board shall be confidential. 2. Documents submitted to members of the European Data Protection Board, experts and representatives of third parties shall be confidential, unless access is granted to those documents in accordance with Regulation (EC) No 1049/2001 or the European Data Protection Board otherwise makes them public. 3. The members of the European Data Protection Board, as well as experts and representatives of third parties, shall be required to respect the confidentiality obligations set out in this Article. The chair shall ensure that experts and representatives of third parties are made aware of the confidentiality requirements imposed upon them.	
Article 73 **Right to lodge a complaint with a supervisory authority** 1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority in any Member State if they consider that the processing of personal data relating to them does not comply with this Regulation. 2. Any body, organisation or association which aims to protect data subjects' rights and interests concerning the protection of their personal data and has been properly constituted according to the law of a Member State shall have the right to lodge a complaint with a supervisory	**Article 73** **Right to lodge a complaint with a supervisory authority** 1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority in any Member State if they consider that the processing of personal data relating to them does not comply with this Regulation. 2. Any body, organisation or association which aims to protect data subjects' rights and interests concerning the protection of their personal data and has been properly constituted according to the law of a Member State shall have the right to lodge a complaint with a supervisory

authority in any Member State on behalf of one or more data subjects if it considers that a data subject's rights under this Regulation have been infringed as a result of the processing of personal data. 3. Independently of a data subject's complaint, any body, organisation or association referred to in paragraph 2 shall have the right to lodge a complaint with a supervisory authority in any Member State, if it considers that a personal data breach has occurred.	authority in any Member State on behalf of one or more data subjects if it considers that a data subject's rights under this Regulation have been infringed as a result of the processing of personal data. 3. **(deleted)** *Justification 73.3 (deleted)* *In view of the notification obligation of Article 31, the right mentioned in 73.3 is superfluous, as it does not add anything to the enforcement action of the supervisory authority towards the controller or processor concerned following a personal data breach.*
Article 74 **Right to a judicial remedy against a supervisory authority** 1. Each natural or legal person shall have the right to a judicial remedy against decisions of a supervisory authority concerning them. 2. Each data subject shall have the right to a judicial remedy obliging the supervisory authority to act on a complaint in the absence of a decision necessary to protect their rights, or where the supervisory authority does not inform the data subject within three months on the progress or outcome of the complaint pursuant to point (b) of Article 52(1). 3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established. 4. A data subject which is concerned by a decision of a supervisory authority in another Member State than where the data subject has its habitual residence, may request the supervisory authority of the Member State where it has its habitual residence to bring proceedings on its behalf against the competent supervisory authority in the other Member State. 5. The Member States shall enforce final decisions by the courts referred to in this Article.	
Article 75 **Right to a judicial remedy against a controller or processor** 1. Without prejudice to any available administrative remedy, including the right to lodge a complaint with a supervisory authority as referred to in Article 73, every natural person shall have the right to a judicial remedy if they consider that their rights under this Regulation have been infringed as a result of the processing of their personal data in non-compliance with this Regulation. 2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has its habitual residence, unless the controller is a public authority acting	**Article 75** **Right to a judicial remedy against a controller or processor** 1. Without prejudice to any available administrative remedy, including the right to lodge a complaint with a supervisory authority as referred to in Article 73, every ~~**natural person**~~ **data subject** shall have the right to a judicial remedy if they consider that their rights under this Regulation have been infringed as a result of the processing of their personal data in non-compliance with this Regulation. 2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has its habitual residence, unless the controller is a public authority acting

in the exercise of its public powers. 3. Where proceedings are pending in the consistency mechanism referred to in Article 58, which concern the same measure, decision or practice, a court may suspend the proceedings brought before it, except where the urgency of the matter for the protection of the data subject's rights does not allow to wait for the outcome of the procedure in the consistency mechanism. 4. The Member States shall enforce final decisions by the courts referred to in this Article.	in the exercise of its public powers. 3. Where proceedings are pending in the consistency mechanism referred to in Article 58, which concern the same measure, decision or practice, a court may suspend the proceedings brought before it, except where the urgency of the matter for the protection of the data subject's rights does not allow to wait for the outcome of the procedure in the consistency mechanism. 4. The Member States shall enforce final decisions by the courts referred to in this Article. *Justification 75.1* *To ensure that this right is applied in accordance with the definition of personal data, the term 'data subject' needs to be used.*
Article 76 **Common rules for court proceedings** 1. Any body, organisation or association referred to in Article 73(2) shall have the right to exercise the rights referred to in Articles 74 and 75 on behalf of one or more data subjects. 2. Each supervisory authority shall have the right to engage in legal proceedings and bring an action to court, in order to enforce the provisions of this Regulation or to ensure consistency of the protection of personal data within the Union. 3. Where a competent court of a Member State has reasonable grounds to believe that parallel proceedings are being conducted in another Member State, it shall contact the competent court in the other Member State to confirm the existence of such parallel proceedings. 4. Where such parallel proceedings in another Member State concern the same measure, decision or practice, the court may suspend the proceedings. 5. Member States shall ensure that court actions available under national law allow for the rapid adoption of measures including interim measures, designed to terminate any alleged infringement and to prevent any further impairment of the interests involved.	
Article 77 **Right to compensation and liability** 1. Any person who has suffered damage as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to receive compensation from the controller or the processor for the damage suffered. 2. Where more than one controller or processor is involved in the processing, each controller or processor shall be jointly and severally liable for the entire amount of the damage. 3. The controller or the processor may be exempted from this liability, in whole or in part, if the controller or the processor proves that they are not responsible for the	

event giving rise to the damage.	
Article 78 **Penalties** 1. Member States shall lay down the rules on penalties, applicable to infringements of the provisions of this Regulation and shall take all measures necessary to ensure that they are implemented, including where the controller did not comply with the obligation to designate a representative. The penalties provided for must be effective, proportionate and dissuasive. 2. Where the controller has established a representative, any penalties shall be applied to the representative, without prejudice to any penalties which could be initiated against the controller. 3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.	**Article 78** **Penalties** 1. Member States shall lay down the rules on penalties, applicable to infringements of the provisions of this Regulation and shall take all measures necessary to ensure that they are implemented, including where the controller did not comply with the obligation to designate a representative. The penalties provided for must be effective, proportionate and dissuasive. 2. Where the controller has established a representative, any penalties shall be applied to the representative, without prejudice to any penalties which could be initiated against the controller. 3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.
Article 79 **Administrative sanctions** 1. Each supervisory authority shall be empowered to impose administrative sanctions in accordance with this Article. 2. The administrative sanction shall be in each individual case effective, proportionate and dissuasive. The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and procedures implemented pursuant to Article 23 and the degree of cooperation with the supervisory authority in order to remedy the breach. 3. In case of a first and non-intentional non-compliance with this Regulation, a warning in writing may be given and no sanction imposed, where: (a) a natural person is processing personal data without a commercial interest; or (b) an enterprise or an organisation employing fewer than 250 persons is processing personal data only as an activity ancillary to its main activities. 4. The supervisory authority shall impose a fine up to 250 000 EUR, or in case of an enterprise up to 0,5 % of its annual worldwide turnover, to anyone who, intentionally or negligently: (a) does not provide the mechanisms for requests by data subjects or does not respond promptly or not in the required format to data subjects pursuant to Articles 12(1) and (2); (b) charges a fee for the information or for responses to the requests of data subjects in violation of Article 12(4).	**Article 79** **Administrative sanctions** 1. Each supervisory authority shall be empowered to impose administrative sanctions in accordance with this Article. 2. The administrative sanction shall be in each individual case effective, proportionate and dissuasive. The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and procedures implemented pursuant to Article 23 and the degree of cooperation with the supervisory authority in order to remedy the breach. 3. **(deleted)** 4. The supervisory authority ~~**shall**~~ **may** impose a fine up to 250 000 EUR, or in case of an enterprise up to 0,5 % of its annual worldwide turnover, to anyone who, intentionally or negligently: (a) ~~**does not provide the mechanisms for requests by data subjects or**~~ **does not respond promptly** ~~**or not in the required format**~~ to data subjects pursuant to Articles 12(1) and (2). **When determining a fine for a violation as referred to in this section, the supervisory authority shall take into account the extent to which the controller, or the main establishment as referred to in article 22(4), has put in place mechanisms to respond to data subjects' requests**; (b) charges a fee for the information or for responses to the requests of data subjects in violation of Article 12(4).

Opmerking [redacted]: VNO-NCW questions this provision for cases where the representative is not part of the same group of undertakings as the controller. Given the possible exposure for such independent 'third-party representative', this provision makes it highly unlikely that anyone would be willing to act as a representative for non-EU controllers. **Suggestion: delete.**

5. The supervisory authority shall impose a fine up to 500 000 EUR, or in case of an enterprise up to 1 % of its annual worldwide turnover, to anyone who, intentionally or negligently: (a) does not provide the information, or does provide incomplete information, or does not provide the information in a sufficiently transparent manner, to the data subject pursuant to Article 11, Article 12(3) and Article 14; (b) does not provide access for the data subject or does not rectify personal data pursuant to Articles 15 and 16 or does not communicate the relevant information to a recipient pursuant to Article 13; (c) does not comply with the right to be forgotten or to erasure, or fails to put mechanisms in place to ensure that the time limits are observed or does not take all necessary steps to inform third parties that a data subjects requests to erase any links to, or copy or replication of the personal data pursuant Article 17; (d) does not provide a copy of the personal data in electronic format or hinders the data subject to transmit the personal data to another application in violation of Article 18; (e) does not or not sufficiently determine the respective responsibilities with co-controllers pursuant to Article 24; (f) does not or not sufficiently maintain the documentation pursuant to Article 28, Article 31(4), and Article 44(3); (g) does not comply, in cases where special categories of data are not involved, pursuant to Articles 80, 82 and 83 with rules in relation to freedom of expression or with rules on the processing in the employment context or with the conditions for processing for historical, statistical and scientific research purposes.	5. The supervisory authority ~~shall~~ **may** impose a fine up to 500 000 EUR, or in case of an enterprise up to 1 % of its annual worldwide turnover, to anyone who, intentionally or negligently: (a) does not provide the information, or does provide incomplete information, or does not provide the information in a sufficiently transparent manner, to the data subject pursuant to Article 11, Article 12(3) and Article 14; (b) does not provide access for the data subject or does not rectify personal data pursuant to Articles 15 and 16 or does not communicate the relevant information to a recipient pursuant to Article 13; (c) does not comply with the right to be forgotten or to erasure, ~~or fails to put mechanisms in place to ensure that the time limits are observed~~ **or does not** ~~take all necessary steps to inform third parties that a data subjects requests to erase any links to, or copy or replication of the personal data~~ **or has not provided a mechanism** pursuant Article 17**a. When determining a fine for a violation as referred to in this section, the supervisory authority shall take into account the extent to which the controller, or the main establishment as referred to in article 22(4), has put in place mechanisms for ensuring that the time limits with respect to the retention of the personal data are observed;** (d) ~~does not provide a copy of the personal data in electronic format or~~ hinders the data subject to transmit ~~the personal data~~ **his user-generated content** to another application in violation of Article 18; ~~(e) does not or not sufficiently determine the respective responsibilities with co-controllers pursuant to Article 24;~~ ~~(f) does not or not sufficiently maintain the documentation pursuant to Article 28, Article 31(4-7), and Article 44(3);~~ (g) does not comply, in cases where special categories of data are not involved, pursuant to Articles 80, 82 and 83 with rules in relation to freedom of expression or with rules on the processing in the employment context or with the conditions for processing for historical, statistical and scientific research purposes.
6. The supervisory authority shall impose a fine up to 1 000 000 EUR or, in case of an enterprise up to 2 % of its annual worldwide turnover, to anyone who, intentionally or negligently: (a) processes personal data without any or sufficient legal basis for the processing or does not comply with the conditions for consent pursuant to Articles 6, 7 and 8; (b) processes special categories of data in violation of Articles 9 and 81; (c) does not comply with an objection or the requirement pursuant to Article 19; (d) does not comply with the conditions in relation to measures based on profiling pursuant to Article 20; (e) does not adopt internal policies or does not implement appropriate measures for ensuring and demonstrating compliance pursuant to Articles 22, 23 and 30; (f) does not designate a representative pursuant to Article 25; (g) processes or instructs the processing of personal data in violation of the obligations in relation to processing on	6. The supervisory authority ~~shall~~ **may** impose a fine up to 1 000 000 EUR or, in case of an enterprise up to 2 % of its annual worldwide turnover, to anyone who, intentionally or negligently: (a) processes personal data without any or sufficient legal basis for the processing or does not comply with the conditions for consent pursuant to Articles 6, 7 and 8; (b) processes special categories of data in violation of Articles 9 and 81; (c) does not comply with an objection or the requirement pursuant to Article 19; (d) does not comply with the conditions in relation to measures based on profiling pursuant to Article 20; ~~(e) does not adopt internal policies or does not implement appropriate measures for ensuring and demonstrating compliance pursuant to Articles 22, 23 and 30;~~ (f) does not designate a representative pursuant to Article 25; ~~(g) processes or instructs the processing of personal data in violation of the obligations in relation to processing on~~

Opmerking [redacted]: No documentation obligation in art. 44(3). Mistake in original draft ?

behalf of a controller pursuant to Articles 26 and 27; (h) does not alert on or notify a personal data breach or does not timely or completely notify the data breach to the supervisory authority or to the data subject pursuant to Articles 31 and 32; (i) does not carry out a data protection impact assessment pursuant or processes personal data without prior authorisation or prior consultation of the supervisory authority pursuant to Articles 33 and 34; (j) does not designate a data protection officer or does not ensure the conditions for fulfilling the tasks pursuant to Articles 35, 36 and 37; (k) misuses a data protection seal or mark in the meaning of Article 39; (l) carries out or instructs a data transfer to a third country or an international organisation that is not allowed by an adequacy decision or by appropriate safeguards or by a derogation pursuant to Articles 40 to 44; (m) does not comply with an order or a temporary or definite ban on processing or the suspension of data flows by the supervisory authority pursuant to Article 53(1); (n) does not comply with the obligations to assist or respond or provide relevant information to, or access to premises by, the supervisory authority pursuant to Article 28(3), Article 29, Article 34(6) and Article 53(2); (o) does not comply with the rules for safeguarding professional secrecy pursuant to Article 84.	~~**behalf of a controller pursuant to Articles 26 and 27;**~~ (h) does not alert on or notify a personal data breach or does not timely or completely notify the data breach to the supervisory authority or to the data subject pursuant to Articles 31 and 32; ~~**(i) does not carry out a data protection impact assessment pursuant or processes personal data without prior authorisation or prior consultation of the supervisory authority pursuant to Articles 33 and 34;**~~ ~~**(j) does not designate a data protection officer or does not ensure the conditions for fulfilling the tasks pursuant to Articles 35, 36 and 37;**~~ (k) misuses a data protection seal or mark in the meaning of Article 39; (l) carries out or instructs a data transfer to a third country or an international organisation that is not allowed by an adequacy decision or by appropriate safeguards or by a derogation pursuant to Articles 40 to 44; (m) does not comply with an order or a temporary or definite ban on processing or the suspension of data flows by the supervisory authority pursuant to Article 53(1); (n) does not comply with the obligations to assist or respond or provide relevant information to, or access to premises by, the supervisory authority pursuant to Article 28(3), Article 29, Article 34(6) and Article 53(~~2~~ **3**); (o) does not comply with the rules for safeguarding professional secrecy pursuant to Article 84. **A fine for violations referred to in this paragraph can only be imposed for a particular processing of personal data. When determining a fine for a violation as referred to in this paragraph, the supervisory authority shall take into account the following facts and circumstances:** **(a) the extent to which the controller, or the main establishment as referred to in Article 22(4), has adopted internal policies and has implemented the measures referred to in Articles 22, 23 and 30 with respect to such processing;** **(b) the fact whether or not the controller, or the main establishment as referred to in Article 22(4), has designated a data protection officer pursuant to Article 35;** **(c) the extent to which the controller has allowed the data protection officer, if any, to perform his tasks as referred to in Article 37 with respect to such processing;** **(d) the extent to which the data protection officer, if any, was involved in the decision making with respect to such processing or in the implementation thereof;** **(e) the fact whether or not the controller has performed a privacy impact assessment with respect to such processing;** **(f) the fact whether or not the controller, where relevant, has complied with Article 26; and** **(g) the extent to which the controller has instructed the processor, if any, pursuant to Article 27.**
7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of updating the amounts of the administrative fines referred to in paragraphs 4, 5 and 6, taking into account the criteria referred to in paragraph 2.	7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of updating the amounts of the administrative fines referred to in paragraphs 4, 5 and 6, taking into account the criteria referred to in paragraph 2. *Justification 79.3* *The supervisory should have freedom of appreciation in*

	fining organizations for violating the Regulation. ***Justification 79.5, 79.6 and 79.7*** *The 'accountability measures' should not be fined as an independent infringement. Where the absence of such measures are likely to have caused the infringement of the 'material rules' (like data security, data subject's rights, data limitation, etc), the supervisory authority should take such absence into account in determining the level of the fine (see also the US Federal Sentencing Guidelines for companies in case of non-compliance). Furthermore, instead of issuing a fine, the supervisory authority should order the controller or processor to take the necessary measures pursuant to its powers in article 53.*
Article 80 **Processing of personal data and freedom of expression** 1. Member States shall provide for exemptions or derogations from the provisions on the general principles in Chapter II, the rights of the data subject in Chapter III, on controller and processor in Chapter IV, on the transfer of personal data to third countries and international organisations in Chapter V, the independent supervisory authorities in Chapter VI and on co-operation and consistency in Chapter VII for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression in order to reconcile the right to the protection of personal data with the rules governing freedom of expression. 2. Each Member State shall notify to the Commission those provisions of its law which it has adopted pursuant to paragraph 1 by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment law or amendment affecting them.	
	Article 80a **National identification numbers** **The private sector processing of a national identification number or any other national identifier shall not be prohibited by Member States.** *Justification:* *The processing of personal data in the context of large organizations creates huge problems in identifying citizens, customers and employees. The only efficient manner to avoid false identification of individuals is the use of national identification numbers. The use of such numbers contributes to data quality and limits the risk of inaccurate processing of personal data. The extended use of national identification numbers contributes to the possibility of detecting and fighting identity fraud but also to reduction of the misuse of facilities of large organizations. It contributes to fighting organized crime. Finally it significantly reduces operational costs of large organizations. Unfortunately not all member states recognize these advantages and some of them restrict the use of the national ID by private sector enterprises. The amendment aims at creating a European level playing field, at significantly improving data quality, at significantly reducing the risk of erroneous processing and at the reduction of operational costs.*
Article 81 **Processing of personal data concerning health**	**Article 81** **Processing of personal data concerning health**

1. Within the limits of this Regulation and in accordance with point (h) of Article 9(2), processing of personal data concerning health must be on the basis of Union law or Member State law which shall provide for suitable and specific measures to safeguard the data subject's legitimate interests, and be necessary for: (a) the purposes of preventive or occupational medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject to the obligation of professional secrecy or another person also subject to an equivalent obligation of confidentiality under Member State law or rules established by national competent bodies; or (b) reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety, inter alia for medicinal products or medical devices; or (c) other reasons of public interest in areas such as social protection, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system.	1. Within the limits of this Regulation and in accordance with point (h) of Article 9(2), processing of personal data concerning health must be on the basis of Union law or Member State law which shall provide for suitable and specific measures to safeguard the data subject's legitimate interests, and be necessary for: (a) the purposes of preventive or occupational medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject to the obligation of professional secrecy or another person also subject to an equivalent obligation of confidentiality under Member State law or rules established by national competent bodies; or (b) reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety, inter alia for medicinal products or medical devices; or (c) other reasons of public interest in areas such as social protection, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the ~~health~~ insurance system.
2. Processing of personal data concerning health which is necessary for historical, statistical or scientific research purposes, such as patient registries set up for improving diagnoses and differentiating between similar types of diseases and preparing studies for therapies, is subject to the conditions and safeguards referred to in Article 83.	2. Processing of personal data concerning health which is necessary for historical, statistical or scientific research purposes, such as patient registries set up for improving diagnoses and differentiating between similar types of diseases and preparing studies for therapies, is subject to the conditions and safeguards referred to in Article 83. **3. The processing of data concerning health necessary for the purpose of the provision of healthcare management services to a healthcare professional or healthcare organisation shall be governed by a contract or other legal act as referred to in Article 26(2). Insofar consent of the data subject is required for the disclosure of the data concerning health to the healthcare management service provider, such consent shall be deemed to be given.**
3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying other reasons of public interest in the area of public health as referred to in point (b) of paragraph 1, as well as criteria and requirements for the safeguards for the processing of personal data for the purposes referred to in paragraph 1.	**4. (deleted)** *Justification 81.1* *Processing health data is an essential aspect of the insurance business. Insurers need to process health-related data to provide certain insurance products. By way of example, health data for private medical insurance is processed to ensure that consumers receive appropriate cover at a fair price for the risk that he poses, or to reimburse all or part of health care where the individual requires medical treatment covered by the insurance policy.* *Being able to access and process health data through automated processing enables insurers to process and pay claims, determine the level of cover needed, assess the risk and hence provide consumers with the appropriate premium that fairly reflects the individuals' needs and risks. Processing health data is not only crucial for health*

	insurance products but to all sorts of insurance products. Therefore the term "health" is deleted to provide in a legal basis for collecting and processing health data for insurance purposes, such as health, life, accident, third party liabilities insurance and reinsurance. *Otherwise it would prevent or delay the reimbursement of medical treatment or the compensation for car accidents, as without an appropriate assessment of the risks, insurers are unable to determine the right amounts of reimbursement or compensation.* ***Justification 81.3 (new)*** *Healthcare professionals and organizations like hospitals rely heavily on the services of healthcare management service providers, such as IT services, administration services, billing services and financial services. This amendment clarifies that healthcare management service providers are allowed to process health data as the 'long arm' of the healthcare professional or the hospital.* *Although consent is not required for disclosure of personal data to processors, healthcare sector-specific rules and regulations typically only allow the disclosure of health data to third parties on the basis of 'informed consent'. However, the processing of health data by healthcare management service providers is typically understood to be allowed on the basis of 'implied consent' (also called the "long-arm-construction"), although this is often not explicitly mentioned in the sector-specific rules and regulations. This amendment clarifies that consent shall be deemed given in order to facilitate the effective and efficient operation of healthcare management services.* ***Justification 81.3 (deleted)*** *There is no need for such powers.*
Article 82 **Processing in the employment context** 1. Within the limits of this Regulation, Member States may adopt by law specific rules regulating the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship. 2. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them. 3. 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 safeguards	**Article 82** **Processing in the employment context** 1. Within the limits of this Regulation **and Union law**, Member States may adopt by law specific rules regulating the **~~processing~~ collection, use or dissemination** of employees' personal data in the employment **and staffing** context, in particular for the purposes of the recruitment, **staffing,** the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship. **2. The rules adopted pursuant to paragraph 1 shall not cover the processing of personal data and the measures taken pursuant to Articles 26, 30 to 33, and 40 to 44.** **3**. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them. **4. (Deleted, as it contradicts the essence of par. 1, which allows Member States to introduce legislation consistent with their labour relations system)**

for the processing of personal data for the purposes referred to in paragraph 1.	*Justification 82.1* *Several areas mentioned in article 82.1 are regulated by Union law. This change reflects this.* *The addition of "staffing" reflects the fact that employment relationships may be complex (e.g., through agencies).* *Justification 82.2 (new)* *According to Article 82.1, Member States may adopt laws regulating the processing of employee data. VNO-NCW understands that this is necessary to reflect the differences in labour relations between the Member States. However, such differences should not cover the more operational requirements of this Regulation. Therefore, those laws should not provide additional rules, which may impact the harmonized implementation of HR-systems across Member States. This means that those laws should not contain any additional rules with respect to the way the data protection rights of the employees are implemented (articles 12 – 21), nor should they contain additional requirements with respect to the use of processors (art. 26), data security (art. 30), data breach notifications (articles 31 and 32), the execution of impact assessments (art. 34) or international data transfers (article 40 to 44). This allows for full harmonisation of HR-operations through shared service centres and HR-information systems, while at the same time allowing for differences in labour relations with respect to the type of personal data which are collected about employees, or the allowed uses thereof.*
Article 83 **Processing for historical, statistical and scientific research purposes** 1. Within the limits of this Regulation, personal data may be processed for historical, statistical or scientific research purposes only if: (a) these purposes cannot be otherwise fulfilled by processing data which does not permit or not any longer permit the identification of the data subject; (b) data enabling the attribution of information to an identified or identifiable data subject is kept separately from the other information as long as these purposes can be fulfilled in this manner. 2. Bodies conducting historical, statistical or scientific research may publish or otherwise publicly disclose personal data only if: (a) the data subject has given consent, subject to the conditions laid down in Article 7; (b) the publication of personal data is necessary to present research findings or to facilitate research insofar as the interests or the fundamental rights or freedoms of the data subject do not override these interests; or (c) the data subject has made the data public. 3. 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 processing of personal data for the purposes referred to in paragraph 1 and 2 as well as any necessary limitations on the rights of information to and access by the data subject and detailing	**Article 83** **Processing for historical, statistical and scientific research purposes** 1. Within the limits of this Regulation, personal data may be processed for historical, statistical or scientific research purposes only if: (a) these purposes cannot be otherwise fulfilled by processing data which does not permit or not any longer permit the identification of the data subject; (b) data enabling the attribution of information to an identified or identifiable data subject is kept separately from the other information as long as these purposes can be fulfilled in this manner. 2. Bodies conducting historical, statistical or scientific research may publish or otherwise publicly disclose personal data only if: (a) the data subject has given consent, subject to the conditions laid down in Article 7; (b) the publication of personal data is necessary to present research findings or to facilitate research insofar as the interests or the fundamental rights or freedoms of the data subject do not override these interests; or (c) the data subject has made the data public. 3. **(deleted)**

the conditions and safeguards for the rights of the data subject under these circumstances.	*Justification 83.3 (deleted)* *There is no need for such powers.*
Article 84 **Obligations of secrecy** 1. Within the limits of this Regulation, Member States may adopt specific rules to set out the investigative powers by the supervisory authorities laid down in Article 53(2) in relation to controllers or processors that are subjects under national law or rules established by national competent bodies to an obligation of professional secrecy or other equivalent obligations of secrecy, where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. These rules shall only apply with regard to personal data which the controller or processor has received from or has obtained in an activity covered by this obligation of secrecy. 2. Each Member State shall notify to the Commission the rules adopted pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.	
Article 85 **Existing data protection rules of churches and religious associations** 1. Where in a Member State, churches and religious associations or communities apply, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of individuals with regard to the processing of personal data, such rules may continue to apply, provided that they are brought in line with the provisions of this Regulation. 2. Churches and religious associations which apply comprehensive rules in accordance with paragraph 1 shall provide for the establishment of an independent supervisory authority in accordance with Chapter VI of this Regulation.	
	Article 85a **Processing of professional information** **1. Articles 14, 17, 18, 19, 22(1), 28 and 40 shall not apply to the processing of professional information.** **2. Data subjects shall have the right to request from the controller not to have their professional information disclosed to third parties. Such blocking is not required where the blocking proves impossible or would involve a disproportionate effort on the part of the controller.** *Justification:* *Professional data (see definition in Article 4) are frequently collected or disclosed in commercial settings, often as part of communication between companies (e.g., a letter head or signature). Professional data poses hardly any risk to the privacy of the data subject and is often meant to be freely disseminated (e.g., business cards, business phone numbers and business e-mail addresses).* *This amendment aims to reduce the burden of compliance*

	with regard to such data.
Article 86 **Exercise of the delegation** 1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article. 2. The delegation of power referred to in Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 336), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation. 3. The delegation of power referred to in Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force. 4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council. 5. A delegated act adopted pursuant to Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or the Council.	**Article 86** **Exercise of the delegation** **[Par. 2, 3 and 5 are to be made consistent with deletions in the Regulation]**
Article 87 **Committee procedure** 1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011. 2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.	

3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.	
Article 88 **Repeal of Directive 95/46/EC** 1. Directive 95/46/EC is repealed. 2. References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation.	
Article 89 **Relationship to and amendment of Directive 2002/58/EC** 1. This Regulation shall not impose additional obligations on natural or legal persons in relation to the processing of personal data in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC. 2. Article 1(2) of Directive 2002/58/EC shall be deleted.	
Article 90 **Evaluation** The Commission shall submit reports on the evaluation and review of this Regulation to the European Parliament and the Council at regular intervals. The first report shall be submitted no later than four years after the entry into force of this Regulation. Subsequent reports shall be submitted every four years thereafter. The Commission shall, if necessary, submit appropriate proposals with a view to amending this Regulation, and aligning other legal instruments, in particular taking account of developments in information technology and in the light of the state of progress in the information society. The reports shall be made public.	
Article 91 **Entry into force and application** 1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*. 2. It shall apply from [*two years from the date referred to in paragraph 1*]. This Regulation shall be binding in its entirety and directly applicable in all Member States.	