Art / par.	draft regulation provision	amendment proposal	explanation
Art. 1 *Subject matter and objectives*	1. […]. 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.	1. […]. 2. This Regulation protects the fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data. 3. **[new]** This Regulation aims at fostering economical growth and innovation throughout Europe, taking into account the growing economic importance of data based businesses. 4. 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.	• The European commission has repeatedly stated that the regulations shall foster economic growth. This goal hence should be explicitly included in the general framework of objectives to better balance the interests throughout the material provisions of the regulation.
Art. 2 / 2 *Material scope*	2. This Regulation does not apply to the processing of personal data: (a) [….]; (b) by the Union institutions, bodies, offices and agencies; (c) […]; (d) by a natural person without any gainful interest in the course of its own exclusively personal or household activity; (e) […]. 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.	2. This Regulation does not apply to the processing of personal data: (a) […]; ~~(b) by the Union institutions, bodies, offices and agencies;~~ (c) [….]; (d) by a natural person without any gainful interest in the course of its own ~~exclusively~~ primarily personal or household activity; (e) [….]. 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.	• The proposed exemption of European Union bodies leads to fragmentation of the DP framework particularly against the background of the inclusion of national public bodies. The regulation should aim at a maximum harmonization of the DP framework, including all public bodies. • In practice it may be difficult to detect whether an activity is “exclusively (and absolutely) personal”. For example using a social network or a blog system may mainly involve personal statements and activities but could touch professional aspects – such borderline cases should be covered by the exemption. • Important clarification, which systematically also could be included in Art. 88 ff.

Art. 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. 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 behavior 3. […].	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. This includes processing of personal data outside the Union by a controller located 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, regardless whether paid or free of charge, to such data subjects in the Union; or (b) the monitoring of their behavior 3. […].	• Clarification that situations are covered, where a controller is established in the Union but processing of personal data related to data subjects residing in the Union takes place on servers outside the Union. • In light of the goal of maximum harmonization the transition towards a "marketplace principle" is a fundamental pillar, which should be rendered as clear as possible to prevent loopholes. Thus Art 2 (a) should be clarified by an amendment clarifying that the marketplace principle applies regardless whether a service is offer free of charge or not.

Art. 4 / 1,2 *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;	For the purposes of this Regulation: (1) personal data means information able to, ~~directly or indirectly~~ identifiy a natural person (data subject) by means reasonably likely to be used by the controller or a processor supervised by the controller. ~~or natural or legal person to which the controller. in particular, the identification on 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;~~	• The split between the data subject and the personal data definition seems artificial and contradicts the approach of many existing national data protection laws. For a better understanding, the term personal data hence should be the central one. • Moreover it is of upmost importance for a practical handling of data protection law, the definition of personal data strictly refers to the practical means at the controller's disposal, but not the means of any (theoretical) third party. • Otherwise from the controllers perspective any information was personal data, since a controller could never rule out the possibility that any third party has the means to aggregate data with other data in order to identify a data subject. • In particular, the definition is hindering controllers to take technical protection measures such as anonymization and pseudonymization as there is always some natural or legal person holding a key. • The general reference to identification numbers, online identifiers etc. in the current draft produces a high degree of legal uncertainty, since it is not clear, whether the reference weakens the general requirement of identification of a data subject. Since the Recital 24 states, that not every reference to such an abstract mark makes data personal, we recommend a deletion of this part, which should be outlined more precisely in the Recital.
Art. 4 / 2 [new]		[2] anonymous data' means data that has been collected or altered so that it cannot be attributed to a data subject	• The regulation should introduce the term "anonymized data" to clarify that such data is (no longer) personal data. This is consistent with the approach of member states law, e.g. the German Law. • The introduction of anonymized data does not alter the existing legal situation, since anonymized data already is regarded as non-personal. • Introducing the term would, however, help to implement specific incentives within the framework, in particular in the context of the privacy by design approach.

Art. 4 / 3 [new]		[4] "pseudonymous data' means personal data, that has been altered by replacement of the identifying fields with an artificial mark, so that it cannot be attributed to the data subject or that such attribution would require a disproportionate amount of time, expense or effort.	• Pseudonymisation of data is a specific form of privacy by design, which should be fostered across Europe by specific regulatory incentives. • Pseudonymization is a procedure by which identifying fields within a data record are replaced by one or more artificial identifiers. The purpose is to render the data record less identifying relating to a data subject. • Pseudonymized data means a subcategory of personal data for which less strict rules could apply under specific circumstances to be defined within the regulation. • Art. 15 III of the German Telemedia-Act my serve as an example. • The process of (sufficient) pseudonymization can be made subject to certification by independent authorities.
Art. 4 / 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;	'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;	**General comment:** *The proposed definition of processing is very broad. This causes problems in the context of the general obligation to document all processing operations. Thus either the definition of processing has to be adjusted or the obligation to document processing operations must be limited to specific processing operations.*
Art. 4 / 7	'recipient' means a natural or legal person, public authority, agency or any other body to which the personal data are disclosed;	'recipient' means a natural or legal person, public authority, agency or any other body other than the data subject, the data controller or the data processor to which the personal data are disclosed;	• Clarification is needed, since the current definition could be interpreted so that a recipient may also be the data subject, the data controller or the data processor.
Art. 4 / 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;	'the data subject's consent' means any freely given specific, informed and ~~explicit~~ provable 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;	• The core goal of Art. 4 (8) is to ensure that a data subject makes a conscious decisions whether data should be processed or not and to render this decision verifiably. • To reach this goal implicit consent can be considered as valid as well, since an implicit action may demonstrate the data subjects will equally clear like an explicit one. • In this context it should be noted that the UK DPA recently – after intensive discussions with all stakeholders – decided to allow for implicit consent in the context of "cookie-regulation" based on the E-Privacy directive. This decision is based on the insight, that an overly strict explicit-consent requirement ist simply not practicable.

Art. 4 / 9	'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;	'personal data breach' means a breach of security leading to serious accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or illegal access to, personal data transmitted, stored or otherwise processed;	• Data breach notifications are a far reaching concept and should be limited from the outset to serious constellation to prevent mass notifications of minor incidents, which would exceed the resources of data protection authorities and would impose massive administrative burdens on side of controllers.
Art. 4 / 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 processor, 'main establishment' means the place of its central administration in the Union;	'main establishment' means as regards the controller, the place of its establishment in the Union where, based on objective, verifiable indications, 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 or if this place is not reasonably determinable 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 processor, 'main establishment' means the place of its central administration in the Union;	• The main establishment definition is crucial for the principle of a European one-stop shop in data protection. • However, it should be ensured, that the definition cannot be used for forum shopping just by stating that that a specific department is responsible for the main decisions regarding data protection. • Instead there should at least exist reasonable objective and verifiable indications such as the place of the legal department or the place of work of the data protection officer as to determine the main establishment. • In the absence of such indications more objective criteria should apply.

Art. 5	Personal data must be: (a) […] (b) […];	(a) […] (b) […];	
	(b) 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;	(b) 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 anonymized or pseudonymized data or information that does not involve personal data;	• Anonymization or pseudonymization may be applicable in situations where a complete waiver of processing personal data is not possible. Hence those mechanisms should be introduced to implement additional incentives for data minimization.
	(c) 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;	(c) accurate and kept up to date insofar as the controller obtains actual knowledge that the data record is incorrect or inaccurate or the data subject wishes it to be updated or rectified; ~~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;~~	• A general obligation to keep personal data accurate and up to date would lead into a permanent effort of the controller to collect new data and to verify collected data. This conflicts with principle of data harmonization as well as with a conceivable interest of a data subject to intentionally provide "wrong" personal data.
	(d) 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;	(d) 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 in the form of pseudonymized data or 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;	• Pseudonymization in terms of the proposed definition of. Art. 4 (3) [new] hinders identification of data subjects. Therefore longer storing is legitimate, as long as the additional requirement of a periodic review is reached.
	(e) 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.	(e) ~~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.~~	• The responsibilities and obligations of the controller are shaped by the specific material obligations set out in the regulation. Art. 6 (e) seems to have no additional purpose and should thus be deleted. We are afraid that the general statement made by this clause could create an excessive liability regime.

Art. 6 / 1	Processing of personal data shall be lawful only if and to the extent that at least one of the following applies: (a) […]; (b) […]; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) […]; (e) […]; (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.	Processing of personal data shall be lawful only if and to the extent that at least one of the following applies: (a) […]; (b) […]; (c) processing is allowed by Union law or necessary for compliance with a legal obligation to which the controller is subject; (d) […]; (e) […]; (f) processing is necessary for the purposes of the legitimate interests pursued by a 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. (g) **[new]:** processing is limited to pseudonymized data and the recipient of the service is given a right to object pursuant to Art. 19 (3) [new]. (h) **[new]** the processing relates to personal data which are manifestly made public by the data subject; or	• The draft regulation does not contain any saving clause for legal permissions or provisions which conclusively require processing of personal date by the controller. Since the regulation can only outline general principles such specific clauses will be needed for specific circumstances. Art. 6 [b] [new] ensures a proper dealing with such legal permissions. • The legitimate interest clause is an important element to render data protection regulation flexible in practice and to enable authorities and courts to take new technological, social and economic developments into account. • However, the draft regulation – in contrast to the current directive - limits the legitimate interest to the controller, whereas the current directive allows legitimate third party interest to be taken into account. • Given the complex structures of today's online environment, widely based on a division of labor, it is a common situation, that a legitimate interest is pursued by a third party, but not the controller. • To create incentives to use pseudonymization technologies such pseudonymized processing should be legitimate without explicit consent, unless a transparent an "easy-to-use" right to object is given to the user, the condition of the latter are set out in Art. 19 (3). This approach is – for example - in line with the current German law, in particular Art. 15 (3) of the German Telemedia Act. • Art. 6 (h) [new) is taken from the corresponding clause in Art. 9 (e). If this principle applies to specific forms of sensitive data it should all the more apply to less sensitive data.

Art. 6 / 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.	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, substantiate a legitimate interest of the controller or a third party 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.	• Art. 6 (3) has to be amended due to the inclusion of third party interest in Art. (1) f).
Art. 6 / 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.	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.	

Art. 7 / 1-4	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.	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 and a reasonable period after withdrawal, where necessary for the legitimate interest pursued by the controller or a third party. ~~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.~~	• The situation of freely given consent, which is withdrawn later legitimates a period after withdrawal within which the controller or a third party can proceed with processing, since otherwise the controller could be run into illegitimate processing just because of the necessary response time to implement the withdrawal in the automated processing operations. For example, a withdrawal might be arriving by mail (or even letter) and has to be implemented into technical systems by the controller. Within this period the processing should still be regarded legitimate. • The general imbalance clause of paragraph 4 causes a high degree of legal uncertainty, in particular regarding the common relationship between a company / service and a customer. The envisaged provision has far-reaching consequences, since it renders data processing almost completely impossible for the controller, when such an imbalance is assumed. • As long as there are no clear and convincing practical examples, proving the need for such an approach the clause should be deleted. • Insofar as Art. 7 (4) was introduced to cover the relation between employer and employee this should rather be regulated by a specific clause.

Art. 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. 2. […]. 3. […]. 4. […].	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 an identified 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 the degree of intervention to the personal privacy of a child. ~~available technology~~. 2. […]. 3. **[new]** Paragraphs 1 and 2 shall not oblige a controller to identify a data subject or to verify the age of a data subject for the sole purpose of complying with this Article. 4. […]. 5. […].	• The general problem with Article 8 is the technical implementation of such an obligation given the fact that a controller normally cannot verify the age of a user and should not be obliged to do so, since this would lead to a general identification and age verification approach contradicting the underlying goal of data minimization. Hence the provision must be limited to situations of a direct identification of a child. • The requirement "verifiably" is redundant, since it is part of the general requirements of Art. 7. • Moreover a specific provision is necessary, which clarifies that a controller is not obliged to identify a data subject or to verify the age of a data subject to comply with the obligations of Art. 8.

Art. 9	1. […]. 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) […] (c) […] (d) […] (e) the processing relates to personal data which are manifestly made public by the data subject; or (f) […] (g) […] (h) […] (i) […] (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. […]	1. […]. 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) […] (c) […] (d) […] (e) the processing relates to personal data which are manifestly made public by the data subject; or	• Legal fragmentation should be avoided in this crucial field, thus the regulation should be exhaustive. • Art. 9 (e) is supported but should be extended to a general rule and thus also laid down in Art. 6.

Art. 10	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.	If the data processed by a controller do not permit the controller to identify a natural person, in particular when rendered anonymous or pseudonymous, the controller shall not be obliged to acquire additional information in order to identify or to individualize the data subject for the sole purpose of complying with any provision of this Regulation.	**General comment:** We support the underlying idea of Art. 10, since it deals with the fundamental and severe practical problems of the current draft regulation. The concept should be extended to the situation of individualizing a data subject, which means separating from a data pool without actual identification. However, the need for such a clause actually shows the fundamental shortcomings of the too broad definition of personal data and the lack of reference to methods like anonymization and pseudonymization throughout the material regulations draft. Rather than (only) focusing on Art. 10 those more fundamental aspects should be adjusted to render the regulation generally more practical.
Art. 11	1. […]. 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.	1. […]. 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.	• Minor amendment - the requirement to use language specifically adapted to the data subject seems to be impractical given the extreme broad definition of personal data, which covers various constellation, where the controller is not able to identify or even individualize the data subject.
Art. 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.	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 or would require the controller to undo anonymization or pseudonymization of data.	By using anonymization or pseudonymization technologies a controller can prevent itself from the possibility to identify a data subject on the basis of the data collected. Such privacy-by-design-mechanism should not be counteracted by legal obligations which would require the controller to undo those mechanisms merely in order to be compliant regarding material obligations.

Art. 14 / 1 *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) […]; (b) […]; (c) […]; (d) […]; (e) […]; (f) […]; (g) […], (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.	1. Where personal data relating to a data subject in an invidualizable or identifiable manner are collected, the controller shall provide the data subject with at least the following information: (a) […]; (b) […]; (c) […]; (d) […]; (e) […] (f) […]; (g) […] ~~(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.~~	• Many of the following obligation can logically only apply to situations where the data subject is at least individualizable to the controller, which is – given the too broad definition of personal data – not necessarily the case when collecting personal data pursuant to Art. 4. • Too vague wording, creating legal uncertainties.
Art. 14/2-3	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. 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 collected from the data subject in an invidualizable or identifiable manner, 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. 3. Where the personal data are not collected from the data subject, the controller shall, insofar as he is able to identify the data subject on the basis of the data received, inform the data subject, in addition to the information referred to in paragraph 1, from which source the personal data originate.	• Obligations of Art. 14 2 & 3 can logically only apply to situations where the data subject is at least individualizable to the controller, which is – given the too broad definition of personal data – not necessarily the case when collecting personal data pursuant to Art. 4

Art. 16	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.	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. **[new]** Paragraph 1 shall not apply, insofar as collecting and processing is limited to pseudonymous data and rectification would require the controller to undo the process of pseudonymization.	• The right to rectifictaion as laid down in Art. Art 16 of the draft could contradict the privacy by design approach, where the rectification would require a controller (or a third party) to collate data that had been separated for anonymization or pseudonymization purposes and thereby de facto identify a data subject. Paragraph 2 serves to clarify that rectifictaion does not require a controller to identify a data subject. This is in line with the approach of Art. 10 of the draft regulation.

Art. 17/1-3 *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 and 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~~.	The specific reference to data made public “as a child” has no legal consequences in the following paragraphs and should hence be deleted. The proposed wording of Art. 17 (19 d) implies that scenarios under Art. (1) a) – c) are noncompliant processing per se. This is misleading, since those Articles describe situations where an applicable legal basis for processing turns not applicable later.

Art. 17 / 2	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. 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.~~ Alternative: Where the controller ~~referred to in paragraph 1~~ has made the personal data public with no legal basis, 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.	The concept of Art. 17 (2) is highly impractical given the complex link economy of the internet. Moreover, Art. 17 (2) raises fundamental questions and problems, such as… • When is a controller considered to be responsible to have made data public? (for example in the context of a social network) • Why at all should a controller be obliged to delete "traces of data", when publication of such data was carried out in accordance with the regulation? • How should a controller gain knowledge on who is processing such data, given the fact that data which has made (legally) public eventually can be used by almost anyone who had access to it, in particular over the Internet? Art. 17 (2) hence should be fundamentally reconsidered. If at all, such a far reaching and almost impossible to comply with provision must be strictly limited to situation, where publication missed any legal basis from the outset.

Art. 18/1-3 *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. 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. 3. […].	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. 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. 3. **[new]** The above paragraphs do not apply on the processing of anonymized and pseudonymized data, insofar as the data subject is not sufficiently identifiable on the basis of such data or identification would require the controller to undo the process of pseudonymization. 4. **[new]** The above paragraphs do not apply where a controller can reasonably demonstrate, that it is not possible to separate the data subject's data from data of other data subjects. 5. […].	**General comment on liability risks for the controller:** *A general right to data portability is a far reaching concept that, which in particular causes problems in the context of data sets, where personal data of one data subject is mixed with data relating to other data subjects, for example regarding profile data of social networks which may include comments, links etc. relating to a third party. The proposed provisions do not deal with such constellation and thereby impose massive liability risks on side of the controller. The whole concept should thus be reconsidered carefully in order to prevent such liability risks.* *(see also proposed paragraph 4)* Moreover… • It is not clear whether the provision obliges the controller to actively support a portation in cases, where tools are freely available to the data subject to perform the portation. For example E-Mails can easily be exported to a database by use of common mail-clients like Thunderbird or Outlook. Where such tools are available it is not necessary to oblige an E-mail-provider to offer a separate portation mechanism or a copy of the data as stated in paragraph 1. • Where (only) anonymized or pseudonymized data are processed the controller will not be able to separate data of a specific data subject from other data. Thus, in such constellations the right to data portability must not apply.

Art. 19/1-3	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. […]. 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.	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) and (h) 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. […]. [3.] **[new]** Where pseudonymized data are processed pursuant to point (g) of Art. 6 (1) the data subject shall have the right to object free of charge to the processing. This right shall be explicitly offered to the data subject in an intelligible manner and shall be clearly distinguishable from other information. 3. Where an objection is upheld pursuant to paragraphs 1, ~~and~~ 2 and 3, the controller shall, after a reasonable period to implement the objection to automatic processing systems, no longer use or otherwise process the personal data concerned.	• Reference to the proposed new Art. 6 (1) h) – data already manifestly published by a data subject • Right to object regarding the proposed new point (g) of Art. 6 (1) • The situation here is similar to the withdrawal of consent by the data subject pursuant to Art. 7 (3). Since the objection might not be given by automated means but, for example, by E-Mail or a letter, the controller must be be given a reasonable short period to adopt the objection to the automated system used for processing.
Art. 20 / 1 *"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, reliability or behaviour.	1. Every data subject shall have the right not to be subject to ~~a measure~~ processing of personal data which produces legal effects concerning this data subject or comparably affects the legitimate interests of 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, reliability or behaviour.	• Art. 20 (1) refers to a "measure" without a specific link to the processing of personal data. Since the regulation generally can only impose obligations regarding personal data this has to be clarified. The same considerations apply to the term natural person, which should be replaced by data subject. • Whereas the criterion of "legal effects" is sufficiently precise to handle it in practice a criterion of a significant affect is too vague. Thus the clause should refer to legal or similar effects.

Art. 20 / 2	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, (c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards..	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; (c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards. (d) **[new]**: is limited to pseudonymized data. Art. 19 (3) [new] shall apply correspondingly.	• Whereas gaining users consent for measures based on profiling means that a controller de facto receives full control over the data collected – even for a fully identified data subject - the draft regulation does not contain any incentives to avoid such identification of the data subject in the context of profiling based measures. • Art. 20 (2) d) [new] shall implement such incentives by allowing for such measures under the condition data are properly pseudonymized and the recipient of a service is given a right to object. • This refers to the German law, where this principle is well established as an expression of privacy by design and has widely led to efforts for pseudonymization within the advertising sector. DPA in Germany are supportive of the approach and also offer official certification of proper pseudonymization.

Art. 21 / 1-4 *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. […].	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. […].	

Art. 22 / 1-4 *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. 2. The measures provided for in paragraph 1 shall in particular include: (a) keeping the documentation pursuant to Article 28; (b) […]; (c) […]; (d) […]; (e) […]. 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. 4. [….].	1. The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation. 2. The measures provided for in paragraph 1 shall in particular include: (a) keeping the documentation pursuant to Article 28; (b) […]; (c) […]; (d) […]; (e) […]. ~~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.~~ 4. […].	***General comment:*** It should be clarified whether or not Art. 22 imposes additional obligations to the controller in relation to the provisions mentioned here. Since Art. 22 (2) merely refers to other provisions this seems not to be the case and it is unclear which actual purpose Art. 22 could justifiably have. Art. 28 contains an extremely comprehensive obligation to document processing operations. We refer to our comments below. Again, it´s not clear what actual obligation follows from Art. 22 here. Since Art. 22 (1) and (2) actually just states that the controller is obliged to fulfill requirements of other provisions the reference point of this additional "prove of effectiveness" provision is eventually just "compliance with the regulation".

Art. 23 / 1 - 4 *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 organizational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject. 2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals. 3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services. 4. 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).	1. Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject. 2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals. ~~3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.~~ 4. ~~The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).~~	**General comment:** *The whole complex on privacy by design and privacy by default follows a very generalistic approach and creates massive legal uncertainties. In particular it remains completely unclear whether the provision imposes additional obligations on a controller, since Art. 23 (1) explicitly refers to the "meet the requirements of this regulation". Moreover the relationship to consent-based processing remains unclear.* *In sum the provision mainly seems to establish a legal frame for the commission to impose legal obligations on the basis of the "Comitology" – procedure based on Art. 23 (3). This is not acceptable, since the fundamental obligations following from EU-regulation must remain with the legislator.* ***Thus we recommend to completely reassessing the provision in particular as to establish incentives for controllers to follow a data minimization approach (e.g.] by anonymization & pseudonymization) rather than simply to establish vague general obligations.*** Since the material obligations of Art. 23 (1) & (2) are legally extremely vague the far reaching competence for the Commission regarding privacy by design and privacy by default is not acceptable, since this would put the Commission virtually in the position of the legislator.