Artykuły RODO, które będą przedmiotem dyskusji w dniu 16 kwietnia 2013 r.: ***Risk-based approach***		
Obecne brzmienie	**Proponowana zmiana**	**Komentarze**
Article 11 ***Transparent information and communication*** 1. (…) – Deleted 2. (…) - Moved to Article 12 (1).		
Article 12 ***Transparent information, communication and modalities for exercising the rights of the data subject*** 1. The controller shall take appropriate measures to provide any information referred to in Article 14, 14 a and 20(4) and any communication under Articles 15 to 19 and 32 relating to the processing of personal data to the data subject in an intelligible and easily accessible form, using clear and plain language, (…)in particular where addressed specifically to a child. The information shall be provided in writing, or where appropriate, electronically or by other means.		**We can accept it.**
1a. The controller shall facilitate **the processing of** data subject requests under Articles 15 to 19 (…). **(…)**.		**No real change**
2. The controller shall provide the information referred to in Article **15** and 20(4) and **information** on action taken **on a request**		**Positive adjustment innterms of taking into account COMPLEXITY.**

under Articles 16 to 19 **to** the data subject without undue delay and at the latest within one month of receipt of the request (…). This period may be extended for a further two months when necessary, **taking into account the complexity of the request and the number of requests**. Where the extended period applies, the data subject shall be informed within one month of receipt of the request of the reasons for the delay.		
3. If the controller does not take action on the request of the data subject, the controller shall inform the data subject **without delay and at the latest within one month of receipt of the request** of the reasons for not taking action and on the possibility of lodging a complaint to a supervisory authority (…).	If the controller does not take action on the request of the data subject, the controller shall inform the data subject **without delay and at the latest within one month of receipt of the request** of the reasons for not taking action and on the possibility of lodging a complaint to a supervisory authority (…). **This shall not apply to the situations when the controller is a wrong addressee of such request, or requuest is manifestly excessive or unfounded.**	**We can accept it, provided some additional limits will be imposed: there is no need to answer on every complaint. Cases, where:** • **Requests completely misses the point, is absurd, or a joke** • **The addresse is a wrong party for such a request** **shall be treated separately. There shall be a defense line against being forced to answer evewry stupid question. It is very easy to imagine a situation, when controller is elctronically flooded with such unsubstantial requests (e.g. social media rooted). Having answer all of them may paralyse its activitity completely.**
4. Information **provided under Articles 14, 14a and 20(4) and any communication under Articles 15 to 19 and 32 shall be provided** free of charge. Where requests from a data subject are (…)**unfounded or** manifestly excessive, in particular because of their repetitive character, the controller (…)	4. Information **provided under Articles 14, 14a and 20(4) and any communication under Articles 15 to 19 and 32 shall be provided** free of charge. Where requests from a data subject are (…)**unfounded or** manifestly excessive, in particular because of their repetitive character, the controller (…)	**The remarks stated above still apply here. Introduction of limits is good. But demontrating is a bad idea: to whom it shall be demonstrated:** – **Data subject? It may result in a lenghtly dispute** – **Supervisory authority?**

may decline the request. In that case, the controller shall bear the burden of **demonstrating the unfounded** or manifestly excessive character of the request.	may decline the request. In that case, the controller shall bear the burden of ~~**demonstrating the**~~ **unfounded** or manifestly excessive character of the request	
4a. Where the controller has reasonable doubts concerning the identity of the individual making the request referred to in Articles 15 to 19, the controller may request the provision of additional information necessary to confirm the identity of the data subject.	4a. Where the controller has reasonable doubts concerning the identity of the individual making the request referred to in Articles 15 to 19, the controller may request the provision of additional information necessary to confirm the identity of the data subject, **or ignore such a request**.	**There shall be a limit e.g. for enquiries when people use pseudonymes to hide their real identity – a very frequent phenomenoin in human Internet activities. The controller shall be allowed to ignore such a request.**
5. (…)		
6. (…)		
Article 13 ***Rights in relation to recipients*** *(…) - This Article was moved to Article 17b.*		

Article 14 ***Information to the data subject <u>where the data are collected from the data subject</u>*** 1. Where personal data relating to a data subject are collected <u>from the data subject</u>, the controller shall (…), <u>at the time when personal data are obtained</u>, provide the data subject with the following information: (a) the identity and the contact details of the controller and, if any, of the controller's representative; <u>the controller may also include the contact details</u> of the data protection officer<u>, if any</u>; (b) the purposes of the processing for which the personal data are intended (…);	1. Where personal data relating to a data subject are collected <u>from the data subject</u>, the controller shall (…), ~~at the time when personal data are obtained~~, provide the data subject with the following information:	**We can accept it reluctantly. But a beter solution is to include some degree of freedom for all cases where there is a time break between e.g.:** – **Filling in a for and posting it** – **Enerering the received data into a filing system** **In such cases it is not clear, what the term:** <u>at the time when personal data are obtained</u> **shall mean.**
1a. <u>In addition to the information referred to in paragraph 1, the controller shall provide the data subject with any further information necessary to ensure fair and transparent processing **in respect of the data subject**, having regard to the specific circumstances in which the personal data are processed, such as</u>: (a) the <u>envisaged</u> period for which the personal data will be stored; (b) <u>where the processing is based on point (f) of Article 6(1), the</u>		**The term envisaged may be problematic in interpretation and practical implementation.**

legitimate interests pursued by the controller; (c) the recipients or categories of recipients of the personal data; (d) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation; (e) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject and to object to the processing of such personal data, including for direct marketing purposes; (f) the right to lodge a complaint to a supervisory authority (…); (…) (g) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as the possible consequences of failure to provide such data.	(e) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject and to object to the processing of such personal data, ~~including for direct marketing purposes;~~	**There is no raeson to treat direct marketing in such a way** **Wery disputable to impose such duty on the controller – it forces the controller to act as an educator – data subject shall invest in its privacy protection knowledge.**

		We strongly support this amendment. The change here – if adpoted - shall be made fully consistent with the articles delaing with consent, as in many cases consent may be discovered no to be free, actually, as it is necessary. This is especially true for senstive data.
2. (…)		
3. (…)		
4. (…)		
5. Paragraphs 1 and 1a shall not apply where and insofar as the data subject already has the information (…).		
6. (…)		
7. (…)		
8. (…)		

Article 14 a ***Information to be provided where the data have not been obtained from the data subject*** 1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information: (a) the identity and the contact details of the controller and, if any, of the controller's representative; the controller **may** also include the contact details of the data protection officer, if any; (b) the purposes of the processing for which the personal data are intended.		**OK, the DPO's non-mandatory amendment is a very good idea. If implemented, it shall be synchronised with Article listinng the DPO's duties. One of them is servicing the data subjects' enquiries. Publishing the DPO's contact information is the necessary, so, if non-obligatory may contradict with these provisions for duties.**
2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with any further information necessary to ensure fair and transparent processing in respect of the data subject, having regard to the specific circumstances in which the personal data are processed, such as: (a) the categories of personal data concerned; (b) the **envisaged** period for which the personal data will be stored; (c) where the processing is based on		**The term envisaged may be problematic in interpretation and practical implementation.** **Again, such a wording may result an**

point (f) of Article 6(1), the legitimate interests pursued by the controller; (d) the recipients or categories of recipients of the personal data; (e) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject and to object to the processing of such personal data**, including for direct marketing purposes**; (f) the right to lodge a complaint to a supervisory authority (…); (g) the origin of the personal data, unless the data originate from publicly accessible sources.		**administrative burden without any practical benefit to the data subject. Some limits shall be here inserted .** **We strongly support categories.** **There is no reason to specify direct marketing as a special case here.** **It effectively introduced personal data's full life cycle monitoring. Such an idea is ideologically absolutely correct, but its implementation will result in an significant administrative burden, including additional costs for IT processing.**
3. The controller shall provide the information referred to in paragraphs 1 and 2: (a) (…) within a **reasonable** period after obtaining the data, having regard to the specific circumstances in which the data are processed, or (b) if a disclosure to another recipient is		**We strongly support reasonable**

envisaged, at the latest when the data are first disclosed.		
4. Paragraphs 1 to 3 shall not apply where and insofar as: (a) the data subject already has the information; or (b) the provision of such information in particular when processing personal data for historical, statistical or scientific purposes proves impossible or would involve a disproportionate effort. In such cases the controller shall take appropriate measures to protect the data subject's legitimate interests, for example by using pseudonymous data; or (c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject, which provides appropriate measures to protect the data subject's legitimate interests; or (d) where the data originate from publicly available sources; or (e) where the data must remain confidential in accordance with a legal provision or on account of the overriding **legitimate** interests of a third party.	the provision of such information in particular when processing personal data for historical, statistical or scientific purposes proves impossible or would involve a disproportionate effort. In such cases the controller shall take appropriate measures to protect the data subject's legitimate interests, ~~for example by using pseudonymous data~~; or	**We stronly support introducing some economical limits for fulfilling this duty. Simulateneously, we do not understand the reason to apply here the psuedonymous data concept**

5. (…)		
6. (…)		
Article 15 ***Right of access for the data subject*** 1. The data subject shall have the right to obtain from the controller at reasonable intervals, on request, confirmation as to whether or not personal data concerning him or her are being processed. Where such personal data are being processed, the controller shall **communicate** the personal data undergoing processing and the following information to the data subject: (a) the purposes of the processing; (b) (…) (c) the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular to recipients in third countries; (d) the envisaged 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		**We strongly support categories.** **The term envisaged may be problematic in interpretation and practical implementation.**

	processing of such personal data; (f) the right to lodge a complaint to a supervisory authority (…); (g) where the personal data are not collected from the data subject, any available information as to their source; (h) in the case of **decisions** referred to in Article 20, knowledge of the logic involved in any automated data processing **as well as** the significance and envisaged consequences of such processing.		**The term:** knowledge of the logic involved **is very problematic.**
2.	(…)**Where personal data are processed by electronic means and in a structured and commonly used format, the controller shall provide a copy of the data in that format to the data subject.**		**Is here the intention to disclose all data being processed in a database concerining the data subject? How it refers to the pseudonymous data?**
3.	(…)		
4.	(…)		
5.	[The rights provided for in Article 15 do not apply when data are processed only for historical, statistical, or scientific purposes and the conditions in Article 83(1a) are met].		

Article 16 ***Right to rectification*** 1. (…) The data subject shall have the right to obtain from the controller the rectification of personal data concerning him or her which are inaccurate. Having regard to the purposes for which data were processed, the data subject shall have the right to obtain completion of incomplete personal data, including by means of providing a supplementary (…)statement.	***Right to rectification*** 1. (…) The data subject shall have the right to obtain from the controller the rectification of personal data concerning him or her which are inaccurate. Having regard to the purposes for which data were processed, ~~the data subject shall have the right to obtain completion of incomplete personal data~~, ~~including by means of providing a supplementary~~ (…)statement.	**Request to knowledge of the logic involved may result in an dramatic administrative burden. What is complete and enogh for the data controller, may be not satisfactory for the data subject. Any such amendments requests shall not be allowed.**
2. [The rights provided for in Article 16 do not apply when data are processed only for historical, statistical, or scientific purposes and the conditions in Article 83(1a) are met.]		
Article 19 ***Right to object*** 1. The data subject shall have the right to object, on **reasoned** grounds relating to his or her particular situation, at any time to the processing of personal data **concerning him or her** which is based on point[s] (…) [(e) and] (f) of Article 6(1). **In such cases the personal data shall no longer be processed** unless the	The data subject shall have the right to object, on **reasoned** grounds relating to his or her particular situation, at any time to the processing of personal data **concerning him or her** which is based on point[s] (…) [(e) and] (f) of Article 6(1). **In such cases the personal data shall be limited to the reamining legal**	**The wording no longer be processed is not acceptable as e.g. storage is also a processing !!! Intenetion is here to limit processing !**

	controller demonstrates (…) legitimate grounds for the processing which override the interests or (…) rights and freedoms of the data subject.	**grounds,** unless the controller demonstrates (…) legitimate grounds for the processing which override the interests or (…) rights and freedoms of the data subject.	
1a.	Where an objection is upheld pursuant to paragraph 1 (…), the controller shall no longer (…)process the personal data concerned except for the establishment, exercise or defence of legal claims.	Where an objection is upheld pursuant to paragraph 1 (…), the controller shall no longer (…)process the personal data concerned except for **the remaining legal grounds, including** the establishment, exercise or defence of legal claims	**Claims are not the only reamining legal grounds – there are many others, including archiving.**
2.	Where personal data are processed for direct marketing purposes, the data subject shall have the right to object free of charge at any time to the processing of personal data concerning him or her for such marketing. This right shall be explicitly brought to the attention of the data subject (…)**and** shall be presented clearly and separately from any other information.		**We do not see reason to treat direct marketing in such a harsh way.**
2a.	**Where the data subject objects to the processing for direct marketing purposes, the personal data shall no longer be processed.**		**Again, as the term processing is very broad, intention to block processing for current purpose in the most cases cannot result in blocking it altogether. If allowing for such a wording here, the very definion of processing shall be made narrower.** **The very idea is here probably to restrict the processing !!!**
3.	(...)		

4. [The rights provided for in Article 19 do not apply to personal data which are processed only for historical, statistical, or scientific purposes and the conditions in Article 83(1A) are met].		
Article 22 ***Responsibility of the controller*** 1. **Taking into account the nature, scope and purposes of the processing and the risks for the (..) rights and freedoms of data subjects**, the controller shall (…) implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.		**OK.**
2. (…) – *(The Presidency has deleted this paragraph as it deems that there is no need to repeat obligations which are spelt out later on in the Chapter)*		
2a. Where proportionate in relation to the processing activities, the measures referred to in paragraph 1 shall include the implementation of:		**This wording is inconsistent with asking to implement data protection management systems. Any policy is the a part of such system. Using wording policies instead of**

(a) appropriate data protection policies by the controller; (b) mechanisms to ensure that the time limits established for the erasure **and restriction** of personal data are observed.	mechanisms to ensure that the ~~time limits~~ **retenion periods** established for the erasure **and restriction** of personal data are observed.	**policy may be also very problematic for the implementation of such a system.** **This wording is very problematic, inconsistent with previously used descriptrs for such a situation. Time limit shall be replaced by retention period – the term also well established in many other sector laws.**
3. (…)		
4. (…)		

Article 23 ***Data protection by design and by default*** 1. Having regard to the state of the art and the cost of implementation and taking account of the risks for rights and freedoms of individuals posed by the nature, scope or purpose of the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement (…) technical and organisational measures (…) appropriate to the activity being carried on and its objectives, including the use of pseudonymous data, in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of (…) data subjects.		**We do not support the pseudonymisation very idea. We are not shure whether it will result in real benefit for insurance sector and our customers.**
2. The controller shall implement appropriate measures for ensuring that, by default, only (…) personal data (…) which are necessary for each specific purpose of the processing are processed; (…) this applies to the amount of (…) data collected, (...) the period of their storage and their accessibility. In particular, those mechanisms shall ensure that by default personal data are	The controller shall implement appropriate measures for ensuring that, by default, only (…) personal data (…) which are necessary for each specific purpose of the processing are processed; (…) this applies to the amount of (…) data collected, (...) the **retention** period ~~of their storage and their accessibility~~. In particular, those mechanisms shall ensure that by default personal data are	**The wording shall be made precise, storage and accessibility are only some selected forms of processing.**

	not made accessible to an indefinite number of individuals <u>without human intervention</u>.	not made accessible to an indefinite number of individuals <u>without human intervention</u>.	
2a.	**<u>The controller may demonstrate compliance with the requirements set out in paragraphs 1 and 2 by means of a certification mechanism pursuant to Article 39.</u>**		**We strongly support this as this avoids duplicating an information security management system for personal data protection in case it is already implemented for data processing.**
3.	(…)		
4.	(…)		
	Article 24 ***Joint controllers***		**We support introdcing such limits.**
1.	(…)Joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the (…) exercising <u>of</u> the rights of the data subject <u>and their respective duties to provide the information referred to in Articles 14 and 14a</u>, by means of an arrangement between them <u>unless the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject</u>.		
2.	<u>The data subject may exercise his or her</u>		**This is ideologically OK, but may result in**

rights under this Regulation in respect of and against each of the joint controllers.		**forcing data protection supervisory authorities to be converted into foreign language translation offices and asking them to acquire pan-European legal knowledge, including contry-specific issues – absolitely necessary to assess whether the claims is legitimate – it may be a hoax!**
Article 25 ***Representatives of controllers not established in the Union*** 1. In the situation referred to in Article 3(2), the controller shall designate **in writing** 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 unless the processing it carries out involves high risks for the rights and freedoms of **data subjects, having regard to the nature, scope and purposes of the processing**; or (c) a public authority or body; or		

(d) (…).		
3. The representative shall be established in one of those Member States where the data subjects whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, reside.		
3a. The representative shall be mandated by the controller to be addressed in addition to or instead of the controller by in particular supervisory authorities and data subjects, on all issues related to the processing of personal data, for the purposes of ensuring compliance with this Regulation.		**It is aproblem with limiting the representation to be addressed. We are not sure it was the very idea.**
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 26 ***Processor*** 1. (…)The controller shall use only a processor providing sufficient guarantees to implement appropriate technical and organisational measures		**OK.**

(…) in such a way that the processing will meet the requirements of this Regulation (…).		
2. [Where the processor is not part of the same group of undertakings as the controller,] the carrying out of processing by a processor shall be governed by a contract setting out the subject-matter and duration of the contract, the nature and purpose of the processing, the type of data and categories of data subjects or other legal act binding the processor to the controller and stipulating in particular that the processor shall: (a) process the personal data only on instructions from the controller (…), unless required to do so by Union or Member State law law to which the processor is subject; (b) (…); (c) take all (…) measures required pursuant to Article 30; (d) determine the conditions for enlisting another processor (…); (e) as far as (…) possible, taking into account the nature of the processing, assist the controller in responding to requests for exercising the data subject's rights laid down in Chapter		**Undertaking, enterprise – wording to be sycnchronised.** **If the intention here is to allow sub-processing, this wording is very problematic. It may be interpreted, that egnaging into another relation with an processorcan be made dependent on concent of the existing one which is not acceptable for many reasons.**

III; (f) determine the extent to which the controller is to be assisted in ensuring compliance with the obligations pursuant to Articles 30 to 34; (g) (…) not process the personal data further after the completion of the processing specified in the contract or other legal act, unless there is a requirement to store the data under Union or Member State law to which the processor is subject; (h) make available to the controller (…) all information necessary to demonstrate compliance with the obligations laid down in this Article.		**This wording is problematic. STORAGE is not the only purpose. In many cases data shall be kept (e.g. stored) in order to e.g. be demonstrated to some appliacable supervisory authorities.**
3. The controller and the processor shall retain in writing or in an equivalent form the controller's instructions and the processor's obligations referred to in paragraph 2.		**The idea is very good, but the wording is highly problematic. The term EQUIVALENT may be interpretted in many different ways.**
4. (…).		
4a. **The processor shall inform the controller if the processor considers that an instruction by the controller would breach the Regulation.**		**OK**
5. (…)		

Article 27 ***Processing under the authority of the controller and processor*** (…)		

Article 28 ***Records of categories of processing activities*** 1. Each controller (…)and, if any, the controller's representative, shall maintain **a record regarding** all categories of processing activities under its responsibility. This **record** shall contain (…)the following information: (a) the name and contact details of the controller **and** any joint controller **(…),** controller's representative **and data protection officer**, if any; (b) (…); (c) the purposes of the processing (…); (d) a description of categories of data subjects and of the categories of personal data relating to them; (e) the (…) **regular** categories of recipients of the personal data (…); (f) where applicable, the categories of transfers of personal data to a third country or an international organisation, (…)[and, in case of transfers referred to in point (h) of Article 44(1), the **details** of appropriate safeguards]; (g) a general indication of the time limits	(f) where applicable, the categories of transfers of personal data to a third country or an international organisation, (…)[and, in case of transfers referred to in point (h) of Article 44(1), the ~~**details**~~ of appropriate safeguards];	**Please, consider replacing RECORDS by DOCUMENTATION** **Adding DPO here is OK** **We do not know what REGULAR actually means.** **We do not know what DETAILS MAY actually mean here.**

for erasure of the different categories of data; (h) (…).		
2a. Each processor shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing: **(a) the name and contact details of the processor and of each controller on behalf of which the processor is acting, and of the controller's representative, if any;** **(b) the name and contact details of the data protection officer, if any;** **(c) the categories of processing carried out on behalf of each controller;** **(d) where applicable, the categories of transfers of personal data to a third country or an international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards.**		**OK, provide replacing RECORDS by DOCUMENTATION**
3. On request, the controller and the processor and, if any, the controller's representative, shall make the **record**		**OK, provide replacing RECORDS by DOCUMENTATION** **Here RECORD, previously RECORDS**

available (…) to the supervisory authority.		
4. The obligations referred to in paragraphs 1, (…) **to** 3 shall not apply to: (a) (…) (b) an enterprise or a body employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities; or (c) categories of processing activities which by virtue of the nature, scope or purposes of the processing are unlikely to represent **high** risks for , the rights and freedoms of data subjects		**We support this, although we are not sure whether the 250 is a an optimal number.**
5. (…)		
6. (…)		
Article 29 ***Co-operation with the supervisory authority*** (…)		

Article 30 ***Security and confidentiality of processing*** 1. Having regard to the state of the art and the costs of their implementation and taking into account the nature, scope and purposes of the processing and the risks for the rights and freedoms of data subjects, the controller and the processor shall implement appropriate technical and organisational measures including the use of pseudonymous data to ensure a level of confidentiality and security appropriate to these risks.	***Security and confidentiality of processing*** 1. Having regard to the state of the art and the costs of their implementation and taking into account the nature, scope and purposes of the processing and the risks for the rights and freedoms of data subjects, the controller and the processor shall implement appropriate technical and organisational measures including the use of pseudonymous data to ensure a level of confidentiality, **integrity and availability of data, and accountability of its processing** ~~and security~~ appropriate to these risks.	**This wording shall be corrected, as it is inconsistent with the established information security terminology (e.g. ISO-27000 standards).** **Again, having pseudonymisation as the same level measure as basic descriptors from these stundrads, is logically wrong.** **CONFIDENTIALITY is on of 3 basic desriptors of SECURITY !!!**
2. (…).		
2a. The controller may demonstrate compliance with the requirements set out in paragraph 1 by means of a certification mechanism pursuant to Article 39.		**OK.**
2b. Any person acting under the authority of the controller or the processor shall be bound by an obligation of confidentiality, which shall continue to have effect after the termination of their activity for the controller or processor.		**OK**
3. (…).		
4. (…).		

Article 31 ***Notification of a personal data breach to the supervisory authority*** 1. In the case of a personal data breach which is likely to adversely affect the rights and freedoms of data subject**s**, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 51. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 72 hours.		**We support such limits.**
1a. The notification referred to in paragraph 1 shall not be required if a communication of the data subject is not required under Article 32(3)(b).		
2. **(…)** The processor shall alert and inform the controller **without undue delay after becoming aware** of a personal data breach.		**We support such limits.**
3. The notification referred to in paragraph 1 must at least:	(b) (c)	

(a) describe the nature of the personal data breach including**, where possible and appropriate,** the categories and number of data subjects concerned and the categories and **approximate** number of data records concerned; (b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained; (c) (…) ; (d) describe the **likely** consequences of the personal data breach **identified by the controller**; (e) decribe the measures taken or proposed to be taken by the controller to address the personal data breach; and (f) where appropriate, indicate measures to mitigate the possible adverse effects of the personal data breach .	(a)describe the nature of the personal data breach including**, where possible and appropriate,** the categories and number of data subjects concerned and the categories and **approximate** number of data ~~**records**~~ **persons** concerned; decribe the measures taken or proposed to be taken by the controller **and processor** to address the personal data breach; and	**The term RECORD is unprecise and already used as synonym to DOCUMENTEATION. It is much more better to refer to the numer of subjected persons (data subjects).** **We support this limitations, making the very task possible, managable and accontable.** **Measures shall also cover processor. In many cases the processor is the only one who understands the brach teachnicalities, and thus it is the only one capable to propose and undertake corresponding mitigation measures**
3a. Where it is not possible to provide the information referred to in paragraph 3 (f) within the time period laid down in paragraph 1, the controller shall provide this information without undue further		**We strongly support this amendment.**

	delay (…).		
4.	The controller shall document any personal data breaches referred to in paragraph 1, 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.		**OK**
[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.		**This is absolutely necesssary to lay out precise guidelines what to report and how.**
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	The Commission may lay down the standard ~~format~~ **form** 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).]	**We suggest replacing FORMAT (possibly interpretted very technically, which is not acceptable) by a more general FORM**

Article 87(2).]		
Article 32 ***Communication of a personal data breach to the data subject*** 1. When the personal data breach is likely to adversely affect the rights and freedoms of the data subject, the controller shall (…)communicate the personal data breach to the data subject without undue delay.		**OK**
2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b), (e) and (f) of Article 31(3).		**It shall not go to technical and specific. The subject is actually interested in the CONSEQUENCES FOR HIM/HER.**
3. The communication (…) to the data subject **referred to in paragraph 1** shall not be required if**:** a. the controller (…)has implemented appropriate technological protection measures and (…) those measures were applied to the data affected by the personal data breach, **in particular** those that render the data unintelligible to any person who is not authorised to access it**,** such as encryption or the use of		**OK**

pseudonymous data; or b. **the controller has taken subsequent measures which ensure that the data subjects' rights and freedoms are no longer at risk; or** **c. it would involve disproportionate effort, in particular owing to the number of cases involved. In such case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner; or** **d. it would adversely affect a substantial public interest.**		**We strongly support this economical criterion.**
[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.]		**OK**
[5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements as to the circumstances in which a personal data breach is likely to		

	adversely affect the personal data referred to in paragraph 1.		
6.	The Commission 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).]	The Commission may lay down the ~~format~~ **form** 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).]	**Again, we suggest to replace FORMAT by FORM, for reasons already stated**
	Article 33 ***Data protection impact assessment*** 1. Where the processing, **taking into account the nature, scope or purposes of the processing**, is likely to present specific risks **for** the rights and freedoms of data subjects, the controller or processor shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. **(…)**.		**We strongly support adding this additional condition to be obliged to conduct this in many cases complex and costly impact analysis.**
2.	The following processing operations (…) present specific risks referred to in paragraph 1: (a) a systematic and extensive		**We strongly support limiting to the ADVERSE effects, even risking some intepretation problems.**

evaluation (…) of personal aspects relating to (…) natural persons (…), which is based on automated processing and on which decisions are based that produce legal effects concerning (…) data subjects or **adversly** affect data subjects; (b) information on sex life, health, race and ethnic origin **(…),** where the data are processed for taking **(…)** decisions regarding specific individuals on a large scale; (c) monitoring publicly accessible areas, especially when using optic-electronic devices (…)on a large scale; (d) personal data in large scale **processing** systems **containing** genetic data or biometric data; (e) other **operations where** (…) the **competent** supervisory authority **considers that the processing is likely to present specific risks for the fundamental rights and freedoms of data subjects**.		**Principally OK, but lacks safeguards against dictating some extra rules paralysing business. Such a safeguard could be e.g. reference to recommendations and good practices, pointed out or developed by the supervisory authority. Such a process always involves some dose of consulation thus making the process more accountable from the business's perspective.**
2a. The supervisory authority shall establish and make public a list of the		**We strongly recommend this direction. What it lacks is requirement to consult**

kind of processing which are subject to the requirement for a data protection impact assessment pursuant to point (e) of paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board.		**before being issued. Also the word LIST shall be replaced by RECOMMENDATION thus making it more stable and accountable, and also referring to Articles concerning recommendations.** **Additionally, the is a need to open another path: DPC blesses recommendations issued by other supervisory authorities.**
2b. Prior to the adoption of the list the supervisory authority shall apply the consistency mechanism referred to in Article 57 where the list provided for in paragraph 2a 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.		**We support this economical limitation.**
3. The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks for rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data		**OK**

	subjects and other persons concerned.		
4.	(…)		
5.	Where a controllers is a public authority or body and where the processing pursuant to point (c) **or (e)** of Article 6(1) has a legal basis in Union law or the law of the Member State to which the controller is subject, paragraphs 1 to 3 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.		**OK**
[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.		**We strongly support proposing an unified approach to PIA**
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		**OK**

accordance with the examination procedure referred to in Article 87(2).]		
Article 34 ***Prior (…) consultation*** 1. (…) - *this paragraph was moved to Article 42(6).*		
2. The controller or processor shall consult the supervisory authority prior to the processing of personal data where a data protection impact assessment as provided for in Article 33 indicates that the processing is likely to present a high degree of specific risks. (…)		**OK**
3. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 2 would not comply with this Regulation, in particular where risks are insufficiently identified or mitigated, it shall within a maximum period of 6 weeks following the request for consultation (…) make appropriate recommendations to the data controller or processor. This period may be extended for a further month, taking into account the complexity of the intended processing. Where the extended period applies, the controller or		**This is a very good set of measures.**

	processor shall be informed within one month of receipt of the request of the reasons for the delay.		
3a.	During the period referred to in paragraph 3, the controller [or processor] shall not commence processing activities.		**OK**
4.	(…)		
5.	(…)		
6.	**When consulting the supervisory authority pursuant to paragraph 2,** the controller or processor shall provide the supervisory authority, on request, with the data protection impact assessment provided for in Article 33 and any (…) information **requested by** the supervisory authority **(…)**.		**OK**
7.	Member States shall consult the supervisory authority during the preparation of (…) legislative or regulatory measures which provide for the processing of personal data and which may significantly affect categories of data subjects by virtue of the nature, scope or purposes of such processing (…).		**We support REGULATORY measures, which may results in a business friendly soft-law.**
[8.	The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further		**Delegated "how to do it" acts are very useful here.**

specifying the criteria and requirements for determining the high degree of specific risk referred to in point (a) of paragraph 2.] 9. **(…)**		
Article 35 ***Designation of the data protection officer*** 1. The controller **or** the processor **may, or, where required by Union or Member State law, shall,** designate a data protection officer (…)**.**		**This is a very good compromise, leaving as actually with a situation as for the current Directive**
2. (…) **A** group of undertakings may appoint a single data protection officer.		**Very good.**
3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several (…) such authorities or bodies, taking account of their organisational structure and size.		**Also very pragmatic and also beneficial for data subjects as leading to more professional DPOs**
4. (…). – (*Deleted in view of the optional nature of the appointment of the DPO)*		**OK**
5. The (…) data protection officer **shall be designated** on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37**.** (…)		**OK**

6.	(…). (*Moved to Article 36, new paragraph 4, for systematic reasons.)*		**OK**
7.	(…). During their term of office, the data protection officer may, apart from serious grounds under the law of the Member State concerned which justify the dismissal of an employee or civil servant, be dismissed only if the data protection officer no longer fulfils the conditions required for the performance of his or her duties **under paragraph 5**.		**OK**
8.	The data protection officer may be a staff member of the controller or processor, or fulfil his or her tasks on the basis of a service contract.		**A very pragmatic solution.**
9.	The controller or the processor shall **publish the** (…) contact details of the data protection officer **and communicate these** to the supervisory authority (…).		**This shall be reworked: to be sychronised with the part dealing with DPO duties. If he/she shall service customer contacts, including noifying them on data breaches, his/her contact data shal be made public. If not, there is no reason to publish it.**
10.	Data subjects may **at any time** contact the data protection officer on all issues related to the processing of the data subject's data and the exercise of their rights under this Regulation.		**Remark the same as above.**
11.	(…).		

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.		**OK**
2. The controller or the processor shall support the data protection officer in performing the tasks **referred to in Article 37 by** provid**ing (…)**resources necessary to carry out the duties **as well as access to personal data and processing operations**. (…).		**OK**
3. The controller or processor shall ensure that the data protection officer acts in an independant manner with respect to the performance of his or her duties and tasks and does not receive any instructions regarding the exercise of these **duties and tasks**. The data protection officer shall directly report to the highest management level of the controller or the processor**.**		**Ideologically OK, in practical terms it means revolution in HR terms. Now a typical DPO is a lower rank personnel. The proposed solution posiotions him/her somewhere at the equivalent of managing board's proxy. In the most case it will another person. An this in course may result in recruitment problems: there may be not many highly qualifiwed and so trusted professional available on the labour market.**

4. <u>The data protection officer may fulfill other tasks and duties. The controller or processor</u> <u>shall ensure that any such tasks and duties do not result in a conflict of interests</u>		**This is also very pragmatic solution, especially for smaller controllers.**
Article 37 ***Tasks of the data protection officer*** 1. The controller or the processor shall entrust the data protection officer **(…)** with the following tasks: (a) to inform and advise the controller or the processor **<u>and the employees who are processing personal data</u>** of their obligations pursuant to this Regulation **(…);** (b) to monitor **<u>compliance with</u>** <u>this Regulation and</u> **<u>with</u>** <u>the</u> policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, <u>awareness-raising and</u> training of staff involved in the processing operations, and the related audits; (c) (…); (d) (…); (e) (…);		**OK**

(f) (…); (g) to monitor responses to requests from the supervisory authority and, within the sphere of the data protection officer's competence, to co-operate with the supervisory authority at the latter's request or on the data protection officer's own initiative; (h) to act as the contact point for the supervisory authority on issues related to the processing, including the prior consulation referred to in Article 34, and consult with the supervisory authority, on his/her own initiative;		
2. (….).		

Article 38 ***Codes of conduct*** 1. The Member States, the supervisory authorities, **the European Data Protection Board** 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 and the specific needs of micro, small and medium-sized enterprises.		**A very good idea.**
1a. Associations and other bodies representing categories of controllers or processors may draw up codes of conduct, or amend or extent such codes, for the purpose of specifying the application of provisions of this Regulation, such as: (a) fair and transparent data processing; (b) the collection of data; **(ba) the use of pseudonymous data;** (c) the information of the public and of data subjects; (d) the exercise of **the** rights **of data**		**A very good solution** **Again, we are sceptical about such an elevation of the pseudonymisation.**

subjects; (e) information and protection of children; (ea) **measures and procedures referred to in Articles 22 and 23 and measures to ensure security and confidentiality of processing referred to in Article 30**; (f) transfer of data to third countries or international organisations. (g) (…) (h) (…)		
1b. Such a code of conduct shall contain mechanisms for monitoring and ensuring compliance with it by the controllers or processors which undertake to apply it, without prejudice to the duties and powers of the supervisory authority which is competent pursuant to Article 51.		**OK**
1c. In drawing up a code of conduct, associations and other bodies referred to in paragraph 1a shall consult, as appropriate, relevant stakeholders and in particular data subjects, and consider any submission received in response to their consultations.		**OK**
2. Associations and other bodies **referred to in paragraph 1a** which intend to		

	draw up a code of conduct or to amend or extend an existing code of conduct may submit them to the supervisory authority **which is competent pursuant to Article 51. Where the code of conduct relates to processing activities in several Member States,** the supervisory authority **shall submit it in the procedure referred to in Article 57 to the European Data Protection Board which** may give an opinion whether the draft code of conduct or the amendment is in compliance with this Regulation.(…).		
2a.	**The European Data Protection Board shall register the codes of conduct and publish details of them.**		**OK**
3.	**Where a code of conduct is drawn up by** associations and other bodies representing categories of controllers in several Member States, **the European Data Protection Board shall** submit **its opinion on the** code of conduct and on amendments or extensions to an existing code of conduct to the Commission(…).		**Ok, but it may be problematic in implementation. It assumes an in-depth knowledge of this board concerning sector specific national laws.**
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.		**A very good idea.**

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.		
Article 39 ***Certification*** 1. (…) **The** Member States**, the European Data Protection Board and** the Commissionshall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks **for procedures and products**, allowing data subjects to quickly assess the level of data protection provided by controllers and processors. (…)		**A danegerous idea as it may result in costly overregulation and ambiguities. Most of these procedures will have to take into account sector specific national laws. It is very difficult to imagine even a need for their pa-European certification.**
2. A certificate may enable the controller to demonstrate compliance with the controller obligations under this Regulation, in particular the requirements set out in Articles 23 and 30 and the provision of		**This may lead to overregulation. It shall refer to mechanisms to be certified according to the established information security standards, e.g. ISO-27000 series, if any.**

mechanisms to facilitate data subject requests under Articles 15 to 19.		
3. A certificate does not reduce the responsibility of the controller for compliance with this Regulation.		**OK**
4. The controller which submits its processing to the certification mechanism shall provide the body referred to in Article 39a (1) with all information and access to its processing activities which are necessary to conduct the certification procedure. Where the processing concerns processing operations referred to in Article 33(2), the controller shall provide the data protection impact assessment to the body. The supervisory authority may request the controller in accordance with Article 33(2)(e) to carry out an impact assessment in order to support the assessment by the body.		**OK, provided that this will be interpretetd as directions of how use established information security riks based security standards like ISO-27000 series.**
5. The certification issued to a controller shall be subject to a periodic review by the body referred to in Article 39A(1). It shall be withdrawn where the requirements for the certification are not or no longer met.		**OK, provided that this will be interpretetd as directions of how use established information security riks based security standards like ISO-27000 series.**

Article 39a **Certification body and procedure** **1. The certification and its periodic review shall be carried out by an independent certification body which has an appropriate level of expertise in relation to data protection and is accredited by the supervisory authority which is competent according to Article 51.**		**OK, provided that this will be interpretetd as directions of how use established information security riks based security standards like ISO-27000 series.**
2. The supervisory authorities shall submit the draft criteria for the accredition of the body referred to in paragraph 1 to the European Data Protection Board under the procedure referred to in Article 57.		**OK, provided that this will be interpretetd as directions of how use established information security riks based security standards like ISO-27000 series.**
3. The body referred to in paragraph 1 shall act in an independent manner with respect to certification, without prejudice to the duties and powers of the supervisory authority. The body shall ensure that its tasks and duties do not result in a conflict of interest. The data protection certification mechanism shall set out the procedure for the issue, periodic review and		**OK, provided that this will be interpretetd as directions of how use established information security riks based security standards like ISO-27000 series.**

withdrawal of data protection seals and marks.		
4. The body referred to in paragraph 1 shall be liable for the proper assessment leading to the certification, without prejudice to the responsibility of the controller for compliance with this Regulation.		**OK, provided that this will be interpretetd as directions of how use established information security riks based security standards like ISO-27000 series.**
5. The body referred to in paragraph 1 shall inform the supervisory authority on certifications issued and withdrawn and on the reasons for withdrawing the certification.		**OK, provided that this will be interpretetd as directions of how use established information security riks based security standards like ISO-27000 series.**
6. The criteria for the certification and the certification details shall be made public by the supervisory authority in an easily accessible form.		**OK, provided that this will be interpretetd as directions of how use established information security riks based security standards like ISO-27000 series.**
7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of (…) specifying the criteria and requirements to be taken into account for the data protection certification mechanisms referred to in paragraph 1, including		**OK**

	conditions for granting and **revocation**, and requirements for recognition **of the certification and the requirements for a standardised 'European Data Protection Seal'** within the Union and in third countries.		
8.	The Commission may lay down technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).		**OK, provided that this will be interpretetd as directions of how use established information security riks based security standards like ISO-27000 series.**