Artykuły RODO, które będą przedmiotem dyskusji w dniu 16 kwietnia 2013 r.:
Risk-based approach

Obecne brzmienie	Proponowana zmiana	Komentarze
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.**
2a. Where proportionate in relation to the processing activities, the measures referred to in paragraph 1 shall include the implementation 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.	**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 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's very idea. We are not sure 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	The controller shall implement appropriate measures for ensuring that, by default, only (…) personal data (…) which are necessary for each specific purpose of	**The wording shall be made precise, storage and accessibility are only some selected forms of**

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 not made accessible to an indefinite number of individuals without human intervention.	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 not made accessible to an indefinite number of individuals without human intervention.	**processing.**
2a. **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.**		**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 – PROVIDED IT WILL RESULT FOR USING ESTABLISHED STANDARDS AND NOT REINVENTING THE WHEEL !!! WE ARE AGAINST SEPARATE FULL CERTIFICATION STANDARDS FOR DATA PROTECTION ONLY!**
3. (…)		
4. (…)		

Article 24 ***Joint controllers*** 1. (…)Joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the (…) exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 14 and 14a, by means of an arrangement between them unless the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject.		**We support introdcing such limits.**
2. The data subject may exercise his or her rights under this Regulation in respect of and against each of the joint controllers.		**This is ideologically OK, but may result in 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 processin**g; 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		**It is aproblem with limiting the representation to be addressed. We are not sure it was the very idea.**

by in particular supervisory authorities and data subjects, on all issues related to the processing of personal data, for the purposes of ensuring compliance with this Regulation.		
4. The designation of a representative by the controller shall be without prejudice to legal actions which could be initiated against the controller itself.		
Article 26 ***Processor*** 1. (…)The controller shall use only a processor providing sufficient guarantees to implement appropriate technical and organisational measures (…) in such a way that the processing will meet the requirements of this Regulation (…).		**OK.**
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		**Undertaking, enterprise – wording to be synchronised.**

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 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		**If the intention here is to allow sub-processing, this wording is very problematic. It may be interpreted in a wrong way: so as egnaging into another relation with another processor can be made dependent on concent of the existing one which is not acceptable for many reasons.**

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 and possibly result in damaging financial and org-tecg burden.**
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:		**Please, consider replacing RECORDS by DOCUMENTATION**
(a) the name and contact details of the controller **and** any joint controller **(…),** controller's representative **and data protection officer**, if any;		**Adding DPO here is OK**
(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 (…);		**We do not know what REGULAR actually means.**
(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];	(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];	**We do not know what DETAILS MAY actually mean here.**
(g) a general indication of the time limits		

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 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 limitating 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 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		**We strongly support limiting to the ADVERSE effects, even risking some intepretation problems.**

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 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.		**We strongly recommend this direction. What it lacks is requirement to consult 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		**We support this economical limitation.**

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.		
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 subjects and other persons concerned.		**OK**
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		**OK**

activities.		
[6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.		**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 accordance with the examination procedure referred to in Article 87(2).]		**OK**
Article 34 ***Prior (…) consultation*** 1. (…) - *this paragraph was moved to Article 42(6).*		
2. The controller or processor shall consult		**OK, but better to replace the word SHALL**

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. (…)		**by by MAY**
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 processor shall be informed within one month of receipt of the request of the reasons for the delay.		**This is a very good set of measures.**
3a. During the period referred to in paragraph 3, the controller [or processor] shall not commence processing activities.		**OK, pod warunkiem że ostateczna redakcja całości nie będzie skutkować zablokowaniem pzretwarzaniua wskutek**

		dowolnie długich konsultacji
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 specifying the criteria and requirements for determining the high degree of specific risk referred to in point (a) of paragraph 2.] 9. **(…)**		**Delegated "how to do it" acts are very useful here.**