Introduction to

AIJA

www.aija.org

Lost in Privacy? – How to tackle transatlantic data protection challenges

New York, 2-3 February 2017

The New Compliance Tools of the GDPR

Accountability, PIA, Privacy by design and by default, Record of processing activities, DPO, Code of Conduct

Silvia van Schaik
Mark Oliver Kühn
David Salgado Areias

3 February 2017

Welcome


You Snooze,
You Lose

Introduction of panel

Mark Oliver Kühn
RITTERSHAUS Rechtsanwälte
Germany

RITTERSHAUS
Rechtsanwälte

David Salgado Areias
Areias Advogados
Portugal

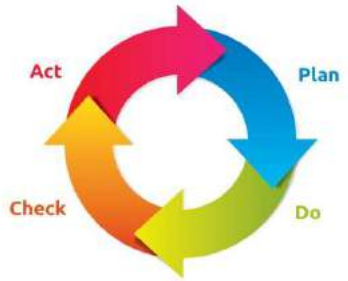
AREIAS ADVOGADOS

Silvia van Schaik
bureau Brandeis
The Netherlands

bureau Brandeis

Introduction of the topic

- New compliance tools
- More focus on accountability; i.e. “responsible and able to demonstrate”
  - Article 29 Data Protection Working Party Opinion 3/2010 on the principle of accountability (00062/10/EN - WP 173)
- Plan – do – check – act



Initial thoughts

Recital (78)

The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that ***appropriate technical and organisational measures*** *be taken to ensure that the requirements of this Regulation are met.*

In order to be able to demonstrate compliance with this Regulation, the controller should ***adopt internal policies*** *and* ***implement measures*** *which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task,* ***producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications*** *and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. (…)*

Data protection impact assessment

Article 35
Data protection impact assessment

1. *Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.*

Data protection impact assessment – When to carry out a DPIA?

Article 35
Data protection impact assessment

1. *Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is **likely to result in a high risk to the rights and freedoms** of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.*

3. *A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:*
   *(a) a **systematic and extensive evaluation of personal aspects** relating to natural persons which is based on automated processing, including **profiling**, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person*
   ***(b) processing on a large scale** of **special categories of data referred to in Article 9(1)**, or of personal data relating to **criminal convictions and offences** referred to in Article 10; or*
   *(c) a **systematic monitoring of a publicly accessible area on a large scale**.*

Data protection impact assessment – More guidance available?

Article 35
Data protection impact assessment

(…)

4. *The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.*

5. *The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.*

6. *Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.*

Data protection impact assessment – More guidance available?

Article 35
Data protection impact assessment

(…)

4. *The supervisory authority **shall** establish and make **public a list of the kind of processing operations** which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.*

5. *The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.*

6. *Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.*

Data protection impact assessment – More guidance available?

Article 35
Data protection impact assessment

(…)

4. *The supervisory authority **shall** establish and make **public a list of the kind of processing operations** which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.*

5. *The supervisory authority **may** also establish and make public a list of the kind of processing operations for which **no data protection impact assessment is required**. The supervisory authority shall communicate those lists to the Board.*

6. *Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.*

Data protection impact assessment – More guidance available?

Article 35
Data protection impact assessment

(…)

4. *The supervisory authority **shall** establish and make **public a list of the kind of processing operations** which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.*

5. *The supervisory authority **may** also establish and make public a list of the kind of processing operations for which **no data protection impact assessment is required**. The supervisory authority shall communicate those lists to the Board.*

6. *Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the **consistency mechanism referred to in Article 63** where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.*

Data protection impact assessment – Content?

Article 35
Data protection impact assessment

(…)

(7) The assessment shall contain at least:

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

(d) the measures envisaged to address the risks, including 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.

Data protection impact assessment – Content?

Article 35
Data protection impact assessment

(…)

*(7) The **assessment shall contain** at least:*

*(a) a **systematic description** of the envisaged **processing operations** and the **purposes** of the processing, including, where applicable, the legitimate interest pursued by the controller;*

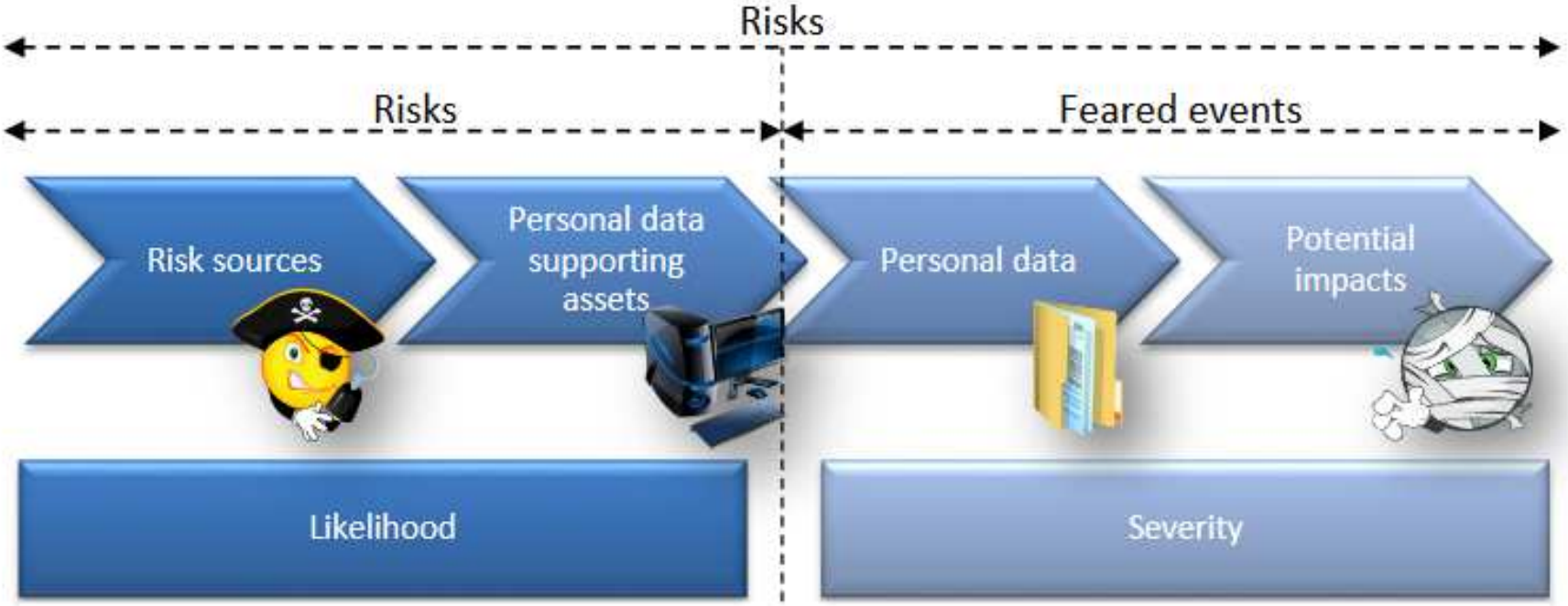
*(b) an assessment of the **necessity and proportionality** of the processing operations in relation to the purposes;*

*(c) an assessment of the **risks** to the rights and freedoms of data subjects referred to in paragraph 1; and*

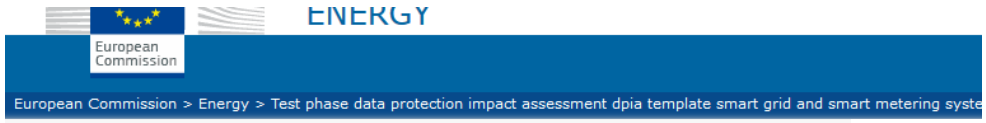
*(d) the **measures** envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.*

Data protection impact assessment – Content?

Article 35
Data protection impact assessment



Data protection impact assessment – A new idea?



substantially higher documentation requirements (also with respect to potential involvement of supervisory authority)

3.4.1.3 Threats that may jeopardize availability

The following table presents the generic threats that can lead to:

- Unavailability of legal processes,
- Disappearance of personal data,
- Unavailability of processing (if this feared event is considered).

Generic threats	Explanation of threats	Specific Energy industry examples of supporting asset vulnerabilities	Questions for guidance	
Hardware loss	Theft of a laptop from a hotel room; theft of a professional mobile phone by a pickpocket; retrieval of a discarded storage device or hardware; loss of an electronic storage device, etc.	Every device which contains sensitive data about the smart grid environment will cause unacceptable risk of alteration and abuse of those data. When information is retrieved about brand and type of firewalls, IP-ranges, OS and SCADA-system brand and type, a serious attack is made easy.	1. Are hardware devices containing data protected against abuse? (password, Pin code, biometrical recognition, pattern recognition) 2. Is the data in the hardware encrypted?	Reduc hardv vulne Reduc vulne relate circul paper
Loss of Power	Loss of power can harm hardware and software and lead to unavailability of computing systems, network equipment and disruption of smart grid devices	Examples: Due to power loss crash of hard drives or other hardware components; Due to power loss crash of OS or loss of unsaved data; Long time power loss has impact on availability of systems. Not all systems will be covered by emergency power	1. Are measures taken to avoid disruption of power, such as UPS and no-break? 2. For vital information systems are uninterruptible power supplies in place? 3. Are there provisions made in order to refuel in time?	Reduc vulne Reduc hardv vulne Reduc

Source: EU, https://ec.europa.eu/energy/en/test-phase-data-protection-impact-assessment-dpia-template-smart-grid-and-smart-metering-systems

Data protection impact assessment – Plan-Do-Check-Act …

Recital (84)

*In order to enhance compliance with this Regulation where **processing** operations are likely to result in a **high risk** to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk. The outcome of the assessment should be taken into account when **determining the appropriate measures** to be taken in order to demonstrate that the processing of personal data complies with this Regulation.*

Source: CNIL, PIA Methodology

Recital (76)

*The **likelihood and severity** of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.*

*Where a data-protection impact assessment indicates that processing operations involve a **high risk which the controller cannot mitigate** by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing.*

Data protection impact assessment – A compliance tool…

Article 35
Data protection impact assessment

(…)

(8) Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.

Source: CNIL, PIA Methodology

Data protection impact assessment – A compliance tool…

Article 35
Data protection impact assessment

(…)

(8) Compliance with approved ***codes of conduct*** *referred to in Article 40 by the relevant controllers or processors* ***shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors****, in particular for the purposes of a data protection impact assessment.*

Source: CNIL, PIA Methodology

Additional Aspects

- involve data subjects, where appropriate [Art. 35 (9)]
- continuous process, especially if changes (factually or legally) occur [Art. 35 (11)]
- involve supervisory authority in accordance with Art. 36

Data protection impact assessment – Documentation …

Article 36
Prior consultation

1. *The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.*

3. *When consulting the supervisory authority pursuant to paragraph 1, the controller shall provide the supervisory authority with:*

   (a) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;
   (b) the purposes and means of the intended processing;
   (c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;
   (d) where applicable, the contact details of the data protection officer;
   (e) the data protection impact assessment provided for in Article 35; and
   (f) any other information requested by the supervisory authority.

Data protection impact assessment – Documentation …

Article 36
Prior consultation

1. *The controller shall consult the supervisory authority prior to processing **where** a data protection impact assessment under Article 35 indicates that the processing would result in **a high risk in the absence of measures** taken by the controller to mitigate the risk.*

3. *When consulting the supervisory authority pursuant to paragraph 1, the controller shall **provide the supervisory authority with:***

   *(a) where applicable, the respective **responsibilities** of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;*
   *(b) the **purposes and means** of the intended processing;*
   *(c) the **measures and safeguards** provided to protect the rights and freedoms of data subjects pursuant to this Regulation;*
   (d) where applicable, the contact details of the data protection officer;
   *(e) the **data protection impact assessment** provided for in Article 35; and*
   ***(f) any other information requested by the supervisory authority**.*

Data protection impact assessment – Supervisory authority

Article 36
Prior consultation

(…)

2. *Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 58.*

   That period may be extended by six weeks, taking into account the complexity of the intended processing. The supervisory authority shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation.

Data protection impact assessment – Supervisory authority

Article 36
Prior consultation

(…)

2. *Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall, within **period of up to eight weeks** of receipt of the request for consultation, provide **written advice** to the controller and, where applicable to the processor, and **may use any of its powers referred to in Article 58**.*

   *That period **may be extended by six weeks**, taking into account the complexity of the intended processing. The supervisory authority shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation.*

Privacy by design and by default

"At the conceptual level, data protection by design means that privacy should be **a feature of the development** of a product rather than something that is tacked on later." (IAPP, *The Top 10 Impacts of the EU's General Data Protection Regulation*, 2016)

- Any means of processing shall be **designed to implement data protection principles** and should **by default ensure that only personal data which is necessary are processed.**
- **Proportionality** Principle: state of the art / cost of implementation / nature, scope, context and purposes of processing / risks of processing.
- Appropriate technical and organisational measures: encryption, pseudonymisation, data minimisation.

Privacy by design and by default

7 Foundational Principles of Privacy by Design (Ann Cavoukian, 2009)

1 - Proactive not Reactive; Preventive not Remedial

2 - Privacy as the Default Setting

3 - Privacy Embedded into Design

4 - Full Functionality – Positive-Sum, not Zero-Sum

5 - End-to-End Security – Full Lifecycle Protection

6 - Visibility and Transparency – Keep it Open

7 - Respect for User Privacy – Keep it User-Centric

Records of processing activities – Controller's duties …

Article 30
Records of processing activities

1. *Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:*

   (a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
   (b) the purposes of the processing;
   (c) a description of the categories of data subjects and of the categories of personal data;
   (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
   (e) where applicable, transfers of personal data to a third country or an international organisation, (…);
   (f) where possible, the envisaged time limits for erasure of the different categories of data;
   (g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

Records of processing activities – Controller's duties …

Article 30
Records of processing activities

1. *Each **controller** and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:*

   *(a) the **name and contact details** of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;*
   *(b) the **purposes** of the processing;*
   *(c) a description of the **categories of data subjects and** of the categories **of personal data**;*
   *(d) the **categories of recipients** to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;*
   *(e) where applicable, **transfers of personal data to a third country** or an international organisation, (…);*
   *(f) where possible, the envisaged **time limits for erasure** of the different categories of data;*
   *(g) where possible, a general description of the **technical and organisational security measures** referred to in Article 32(1).*

Records of processing activities – Processor's duties …

Article 30
Records of processing activities

(…)

2. *Each processor and, where applicable, the processor's representative 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 or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
   (b) the categories of processing carried out on behalf of each controller;
   (c) where applicable, transfers of personal data to a third country or an international organisation, (…);
   (d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

Records of processing activities – Processor's duties …

Article 30
Records of processing activities

(…)

2. *Each **processor** and, where applicable, the processor's representative 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 or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
   (b) the categories of processing carried out on behalf of each controller;
   (c) where applicable, transfers of personal data to a third country or an international organisation, (…);
   (d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

Records of processing activities – Additional aspects …

Article 30
Records of processing activities

(…)

3. The records referred to in p ***electronic form****.*

4. The controller or the proces *rocessor's representative, shall make the record* ***available to the sup***

5. The obligations referred to *rise or an organisation employing* ***fewer than 250 persons*** *risk to the rights and freedoms of data* ***subjects****, the* ***processing is not*** *gories of data as referred to in Article 9(1) or personal data relating t* *rticle 10.*

Recital (13)

(…) To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a derogation for organisations with fewer than 250 employees with regard to record-keeping. In addition, the Union institutions and bodies, and Member States and their supervisory authorities, are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation. The ***notion of micro, small and medium-sized enterprises*** *should draw from Article 2 of the Annex to Commission Recommendation 2003/361/EC.*

Data Protection Officer – Designation

Article 37
Designation of the data protection officer

1. *The controller and the processor shall designate a data protection officer in any case where:*

   (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
   (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
   (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

4. *In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.*

Data Protection Officer – „public authority or body“

Article 37
Designation of the data protection officer

1. *The **controller and the processor** shall designate a data protection o*

   *(a) the processing is carried out by a **public authority or body**,*
   (b) the core activities of the controller or the processor consist of pr… their nature, their scope and/or their purposes, require regular and sy… a large scale; or
   (c) the core activities of the controller or the processor consist of pr… gories of data pursuant to Article 9 and personal data relating to crimina… Article 10.

4. *In cases other than those referred to in paragraph 1, the controller o… odies representing categories of controllers or processors may or, where re… hall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.*

- *to be determined under national law*
- *usually include national, regional and local authorities, and other bodies governed by (national) public law*
- *even though no obligation exists in such cases, WP29 recommends, as a good practice that private organisations carrying out public tasks or exercising public authority designate a DPO*

Data Protection Officer – „core activities“

Article 37
Designation of the data protection officer

1. *The **controller and the proc***

   (a) the processing is carrie *y;*
   *(b) the **core activities** of t* *eir nature, their scope and* *large scale; or*
   (c) the core activities of the *ries of data pursuant to Article* *Article 10.*

4. *In cases other than those re* *ies representing categories of* *ll, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.*

Recital (97)

*In the private sector, the **core activities** of a controller relate to its primary activities and do not relate to the processing of personal data as ancillary activities.*

⇒ ***WP29**:* ‘Core activities’ can be considered as the key operations necessary to achieve the controller’s or processor’s goals. However, ‘core activities’ should not be interpreted as excluding activities where the processing of data forms an inextricable part of the controller’s or processor ’s activity (e.g. hospital; other evaluation re IT support and employee payment).

Data Protection Officer – „monitoring on a large scale“

Recital (91)

*“**large-scale processing** operations which aim to process a **considerable amount of personal data** at regional, national or **supranational** level and which could affect a **large number of data subjects and** which are **likely to result in a high risk**, for example, on account of their sensitivity, where in accordance with the achieved state of technological knowledge a new technology is used on a large scale as well as to other processing operations which result in a high risk to the rights and freedoms of data subjects, in particular where those **operations render it more difficult for data subjects to exercise their rights**.”*

Article 37
the data protection officer

1. *The **contro** data protection officer in any case where:*
   - *(a) the pro **rity or body**, except for courts acting in their judicial capacity;*
   - *(b) the **co** essor consist of processing operations which, by virtue of their nature regular and systematic **monitoring of data subjects on a large scale**;*
   - *(c) the co essor consist of processing on a large scale of special categories of data p elating to criminal convictions and offences referred to in Article*
4. *In cases ot 1, the controller or processor or associations and other bodies representi s may or, where required by Union or Member State law shall, designate ction officer may act for such associations and other bodies representi*

Data Protection Officer – „monitoring on a large scale“

Recital (91)

*“**large-scale processing** operations which aim to process a **considerable amount of personal data** at regional, national or **supranational** level and which could affect a **large number of data subjects and** which are **likely to result in a high risk**, for example, on account of their sensitivity, where in accordance with the achieved state of technological knowledge a new technology is used on a large scale as well as to other processing operations which result in a high risk to the rights and freedoms of data subjects, in particular where those **operations render it more difficult for data subjects to exercise their rights**.”*

Article 37
the data protection officer

1. *The **contro** data protection officer in any case where:*
   - *(a) the pro **rity or body**, except for courts acting in their judicial capacity;*
   - *(b) the **co** essor consist of processing operations which, by virtue of their nature regular and systematic **monitoring of data subjects on a large scale**;*
   - *(c) the co essor consist of processing on a large scale of special categories of data p elating to criminal convictions and offences referred to in Article*
4. *In cases ot 1, the controller or processor or associations and other bodies representi s may or, where required by Union or Member State law shall, designate ction officer may act for such associations and other bodies representi*

Data Protection Officer – special categories of data

Article 37
Designation of the data protection officer

1. *The **controller and the processor** shall designate a data protection officer in any case where:*

   *(a) the processing is carried out by a **public authority or body**, except for courts acting in their judicial capacity;*
   *(b) the **core activities** of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic **monitoring of data subjects on a large scale**; or*
   *(c) the core activities of the controller or the processor consist of **processing on a large scale of special categories of data** pursuant to Article 9 and personal data relating to **criminal convictions and offences** referred to in Article 10.*

4. *In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.*

Data Protection Officer – national laws

Article 37
Designation of the data protection officer

1. *The **controller and the processor** shall designate a data protection officer in any case where:*

   *(a) the processing is carried out by a **public authority or body**, except for courts acting in their judicial capacity;*
   *(b) the **core activities** of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic **monitoring of data subjects on a large scale**; or*
   *(c) the core activities of the controller or the processor consist of **processing on a large scale of special categories of data** pursuant to Article 9 and personal data relating to **criminal convictions and offences** referred to in Article 10.*

4. *In **cases other than those referred to in paragraph 1**, the controller or processor or associations and other bodies representing categories of controllers or processors may or, **where required by Union or Member State law** shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.*

Data Protection Officer – Group DPO?

Article 37
Designation of the data protection officer

(…)

2. *A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.*

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.*

Data Protection Officer – Group DPO?

Article 37
Designation of the data protection officer

(…)

2. *A **group of undertakings** may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.*

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.*

Data Protection Officer – additional aspects

Article 37
Designation of the data protection officer

(…)

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 the **ability to fulfil the tasks** referred to in Article 39.*

6. *The data protection officer **may be a staff member** of the controller or processor, or fulfil the tasks on the basis of a service contract.*

7. *The controller or the processor shall **publish the contact details of the data protection officer** and communicate them to the supervisory authority.*

Article 38
Position of the data protection officer

(…)

5. *The data protection officer shall be **bound by secrecy or confidentiality** concerning the performance of his or her tasks, in accordance with Union or Member State law.*

6. *The data protection officer may fulfil **other tasks and duties**. The controller or processor shall ensure that any such tasks and duties **do not result in a conflict of interests**.*

4. ***Data subjects may contact the data protection officer** with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.*

Data Protection Officer – controller/processor duties

Article 38
Position of the data protection officer

Controllers and processors shall *…*

1. *(…)* ***ensure that the data protection officer is involved****, properly and in a timely manner, in all issues which relate to the*

2. *(…)* *orming the tasks referred to in Article 39 by* ***providing resources*** ***nec*** *to personal data and processing operations, and to maintain his or her exp*

3. *(…)* ***does not receive any instructions regarding the exercise of those tasks****. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.*

Recital (97)

"Such data protection officers, whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner."

Data Protection Officer – WP29 recommendations

Article 38
Position of the data protection officer

*The **WP29 recommends** that the controller should seek the advice of the DPO, on the following issues, amongst others:*

- *whether or not to carry out a DPIA;*
- *what methodology to follow when carrying out a DPIA;*
- *whether to carry out the DPIA in-house or whether to outsource it;*
- *what safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects;*
- *whether or not the data protection impact assessment has been correctly carried out; and*
- *whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with the GDPR.*

(http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf)

Data Protection Officer – DPO‘s tasks

Article 39
Tasks of the data protection officer

1. *The data protection officer shall have **at least** the following tasks:*

   *(a) to **inform and advise** the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;*
   *(b) to **monitor compliance** with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;*
   *(c) to provide advice where requested as regards the **data protection impact assessment** and monitor its performance pursuant to Article 35;*
   *(d) to cooperate with the **supervisory authority**;*
   *(e) to act as the **contact point** for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.*

Data Protection Officer – DPO‘s tasks

Article 39
Tasks of the data protection officer

2. *The data protection officer shall in the performance of his or her tasks **have due regard to the risk associated with processing operations**, taking into account the nature, scope, context and purposes of processing.*

Additional Aspects

- *no personal liability => concept of accountability of controller and processor*
- *More information:*
  Article 29 Working Group - WP243 “Guidelines on Data Protection Officers (‘DPOs’), 13 December 2016
  (http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf)

Data Protection Codes of Conduct

- **What is a Data Protection Code of Conduct?**

  A Data Protection Code of Conduct is a set of rules specifying the application of the GDPR and contributing to its proper application in the context of specific features of the data processing activity and of specific features of a given sector and of small and medium-sizes enterprises.

- **What is the content of a Data Protection Code of Conduct?**

  The rules set by a Data Protection Code of Conduct may cover any necessary topic to establish and demonstrate compliance with the GDPR, from personal data collection to notification of personal data breaches. It must contain mechanisms to enable mandatory compliance monitoring. It also opens the door to rules on out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects.

- **Who can prepare a Data Protection Code of Conduct?**

  A Data Protection Code of Conduct may be prepared by associations and other bodies representing categories of controllers or processors.

Data Protection Codes of Conduct

- **Who can approve a Data Protection Code of Conduct?**

  It the Data Protection Code of Conduct does not relate to processing activities in several EU Member States, it will be approved, registered and published by the national supervisory authority.

  It the Data Protection Code of Conduct relates to processing activities in several EU Member States, it will be approved, registered and published by the national supervisory authority, after obtaining the opinion of the European Data Protection Board. Also, the European Commission may decide that the code of conduct may have general validity within the European Union.

- **Who is subject to a Data Protection Code of Conduct?**

  Only the processors and controllers subject to the GDPR who adhere to a Data Protection Code of Conduct are subject to its rules. The processors and controller not subject to the GDPR may adhere to a Data Protection Code of Conduct making a binding and enforceable commitment.

Data Protection Codes of Conduct

- **Who monitors compliance with a Data Protection Code of Conduct?**
  The compliance with a Data Protection Code of Conduct is monitored by a body accredited by the national supervisory authority according to criteria subject to the European Data Protection Board (independence and expertise).

- **What are the powers of the monitoring body of a Data Protection Code of Conduct?**
  To take appropriate action in cases of infringement, including the suspension or exclusion from the Data Protection Code of Conduct of the concerned processor or controller. It must inform the national supervisory authority of such actions and the reasons for taking them.

Certification, Seals and Marks

- **What is a Data Protection Certification, Seals or Marks?**
  Data Protection Certification, Seal or Mark are mechanisms for the purpose of demonstrating compliance with the GDPR.

- **Who is subject to Data Protection Certification, Seals or Marks?**
  The certification process is voluntary. The processors and controllers not subject to the GDPR may also adhere making a binding and enforceable commitment in order to demonstrate the existence of appropriate safeguards.

- **Who issues the Data Protection Certification, Seals or Marks?**
  A certification body accredited by the national supervisory authority according to criteria subject to the European Data Protection Board (independence and expertise).

- **What are the responsibilities of the certification body?**
  The certification body is responsible for the proper assessment leading to the certification or the withdrawal of such certification.

Final remarks

Q & A

Thank you!

Mark Oliver Kühn
RITTERSHAUS Rechtsanwälte
Germany
Mark-Oliver.Kuehn@rittershaus.net

RITTERSHAUS
Rechtsanwälte

David Salgado Areias
Areias Advogados
Portugal
david.areias@areiasadvogados.com

AREIAS ADVOGADOS

Silvia van Schaik
bureau Brandeis
The Netherlands
silvia.vanschaik@bureaubrandeis.com

bureau Brandeis