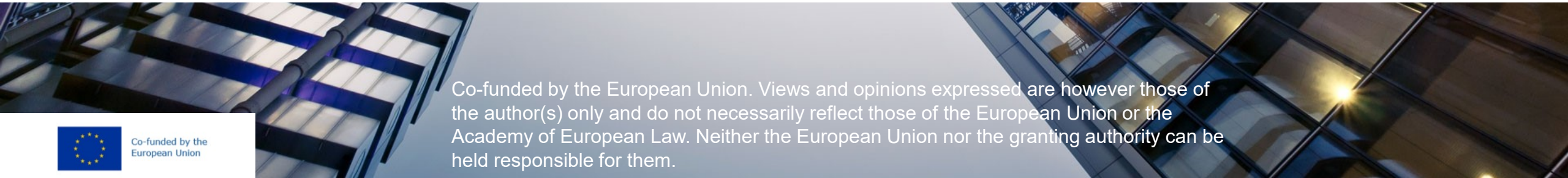
Roles and responsibilities of data controllers and data processors

Olivier Belleflamme| ERA | June 20, 2023



Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Academy of European Law. Neither the European Union nor the granting authority can be held responsible for them.

Co-funded by the European Union

Part 1: The actors and their roles

Controller

Controller means

> "*the natural or legal person, public authority, agency or other body which, alone or jointly with others, **determines the purposes and means of the processing** of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law*" (art. 4(7) GDPR)

- Defined broadly to ensure effective and complete protection
  - "Any body"
  - "Determines"
  - "Purposes and means"
  - "Alone or jointly"
  - Can be "provided for by Union or Member State law"

Qualification of controller

- The controller : "***determines*** *the* ***purposes and means*** *of the* ***processing of personal data***"
- **Determines**
  - Determined per processing operations
  - Exercises influence over the processing with its decision-making power

    explicit or implicit legal competence, or

    control stemming from factual influence

- **key elements about the processing**
  - The "why" and the "how" of the processing
  - Purpose of the processing: essential in the determination
  - Means used for the processing operations: essential means vs non-essential means

- **of personal data**
  - not necessary to actually have access to the data

Controllers

akd

Sole, joined or separate controllers

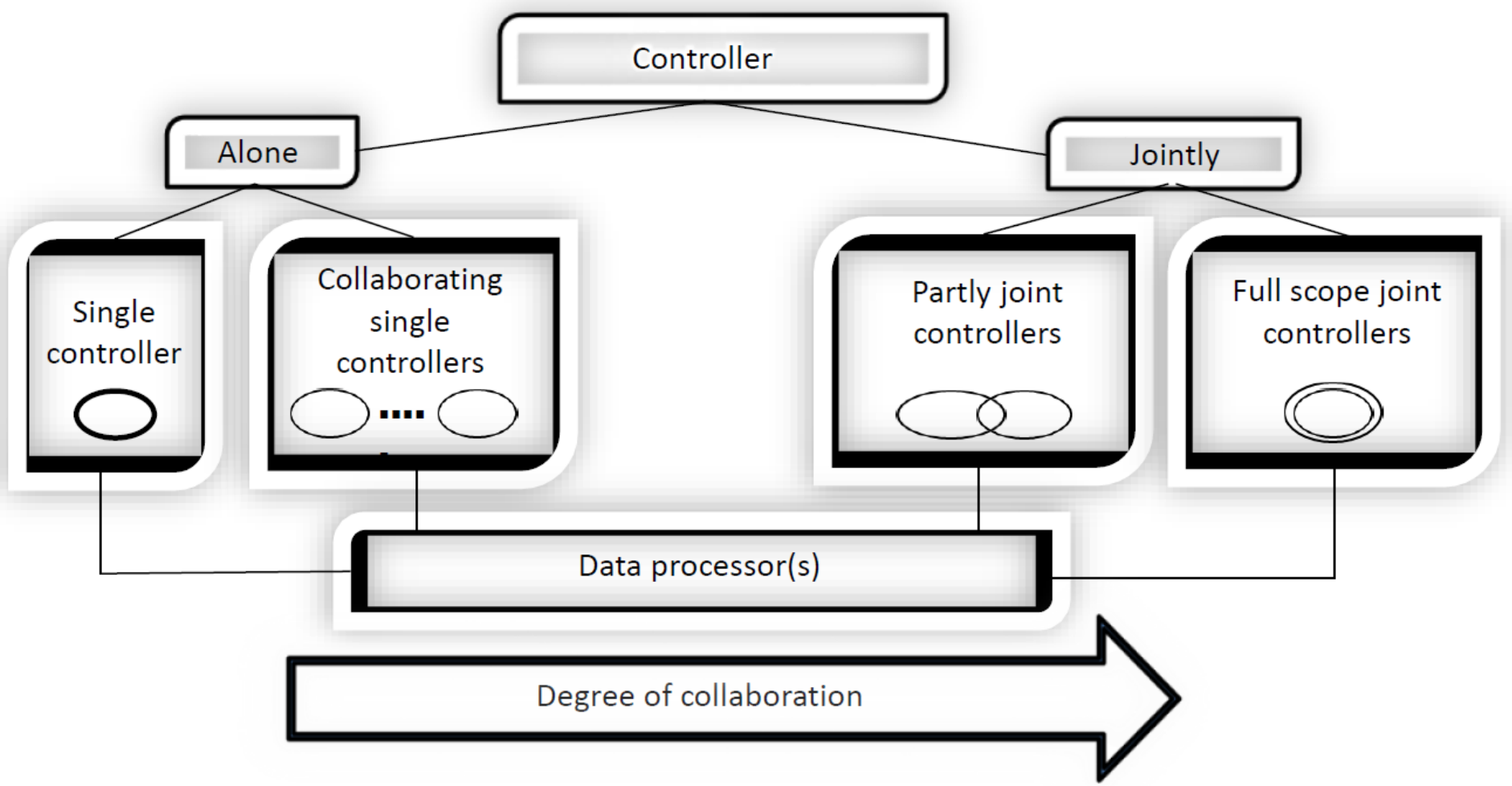
- "*Alone or jointly with others, determines the …*"

- **Sole controller**: single party determines the purposes and means of the processing

- **Joint controllers**: two or more parties determine the purposes and means of the processing together

- **Separate or independent controllers**: two or more parties exchange data but have full autonomy over determination of means and purpose

Controllers and joint-controllership



Source : J. Dhont, I. Vereecken and M. Scuvée from T. Olson and T. Mahler (on the basis of WP29)

Joint-controllership

akd

- "*Where two or more controllers **jointly determine** the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation …*" (art. 26.1 GDPR)

- Relevancy: allocation of obligations for compliance with data protection rules & with respect to the rights of individuals
- Assessment of joint controllership should mirror the assessment of "single" control
  - Can result from a **common decision**: deciding together and involves a common intention
  - Can result from a **converging decisions**: when they complement each other and are necessary for the processing to take place

    ➔ Important criterion for converging decisions: whether the processing would not be possible without both parties' participation; **processing by each party is inextricably linked**
- Joint responsibility does not imply equal responsibility

Relevant Case law (1)

Wirtschaftsakademie (C-210/16, Grand Chamber CJEU, 5 June 2018)

- Facts: academy advertises course, use Facebook fanpage, insights
- Question: does Directive 95/46 allow a party that is not in “control” to be held accountable?
- Decision :
  - By its **definition of parameters**, the administrator of a fan page takes part in the **determination of the purposes and means of processing** the fan page visitors’ personal data
  - The administrator uses Facebook’s platform in order to **benefit from the associated services**
  - Contractual terms are not relevant → **Functional concepts**
  - Joint controllership does **not require** each of the controller to have **access to the personal data** concerned
  - Joint responsibility does **not necessarily** imply **equal responsibility**
- Conclusion: **the administrator of a fan page on Facebook is jointly responsible** with Facebook for the processing of the fan page visitor’s personal data

Relevant Case law (2)

Jehovah's Witnesses (Grand Chamber CJEU - Case C-25/17, 10 July 2018)

- Facts: Notetaking during door-to-door preaching, achieve an objective, coordination of activities,
- Question: can the Jehovah's Witness community be regarded as a controller ?
- Decision:
  - Actors may be involved : (1) at different stages of the processing and (2) to different degrees
  - Joint responsibility **does not require for each controller to have access** to the personal data concerned
  - For the determination of the purpose and means of processing, the **use of written guidelines or instructions from the controller is not necessary**
  - **Influence** over the processing of personal data, **for its own purposes,** may be regarded as a controllership of the processing of personal data
- Conclusion: A religious community, such as the Jehovah's Witnesses, is a controller, **jointly** with its members who engage in preaching, for the processing of personal data carried out in the context of door-to-door preaching organised, coordinated and encouraged by that community

Relevant Case law (3)

- **Fashion ID (Case C-40/17, 29 July 2019)**
- Facts: Website integrate a Facebook like button, collection of data & transmission to Facebook
- Question : The website operators that integrates a facebook like button is a controller ?
- Decision:
  - Fashion ID is **not a controller** for the processing **operations of Facebook subsequent** to the data transmission
  - Facebook and Fashion ID **determine jointly** the purposes and means at the **origin of the operations of collection and transmission to Facebook of the personal data**
  - Fashion ID embedded the Facebook 'like' button for its own **economic interests**
  - **Liability** is limited to **the operation(s)** involving processing of personal data for which the controller actually determines the purposes and means
- Conclusion: **the operator of a website that features a Facebook 'Like' button** can be a controller **jointly** with Facebook in respect of the **collection and transmission** to Facebook of the personal data of visitors to its website

Key takeaways

akd

	Wirtschaftsakademie	Jehovah's Witnesses	Fashion ID
Decisive/factual influence	- No processing without cookies (*means*) - Setting of processing parameters (*purposes*)	- Community members determined data collection modalities (*means*) - Community encourages data collection (*purposes*)	- No processing without embedment of plugin (*means*)
Interest	- Processing serves WA's own interests	- Processing serves Community's own interests	- Processing serves Fashion ID's own commercial interests
Comments - Relevance of "decisive influence" / "dependence" of parties - "Interest" in the processing => potentially points to joint decision on purposes - Interests of parties do not need to converge			

Source : J. Dhont, I. Vereecken and M. Scuvée

Processor

- Processor means

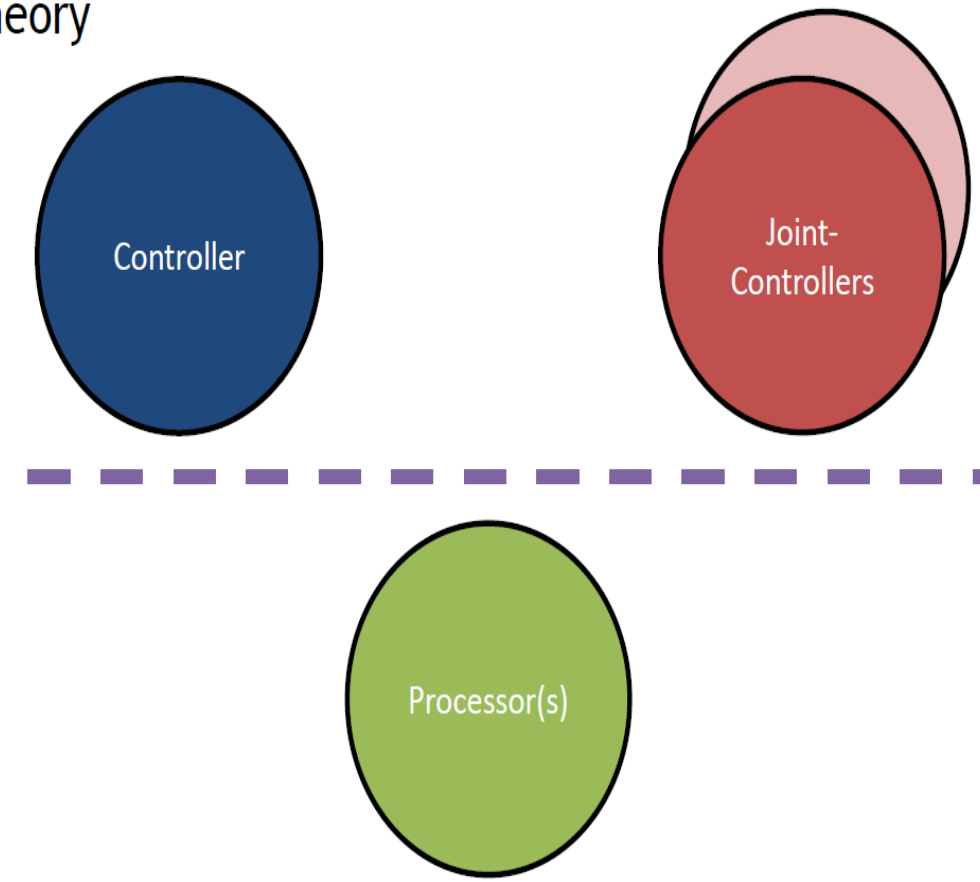
  > "*a natural or legal person, public authority, agency or other **body** which **processes personal data on behalf of the controller***" (art. 4(8) GDPR)

- **"Any body"**:
  - broad range of actors
  - entity separate from the controller
- **Acts "on behalf of"**:
  - implement the controller's instructions regarding the purpose & the essential elements of the means
  - may not carry out processing for its own purpose (art. 28(10) GDPR): when acting outside of the controller's instructions, processors becomes controller for these processing operations
- The **processing operations** "*by a processor **shall be governed by a contract** or other legal act under Union or Member State law, that is binding on the processor with regard to the controller*" (art. 28.3 GDPR)

In summary

akd

Simple in theory



- **Controller:** determines the purposes and the(essential) means of the processing of personal data
- **Joint controllers:** determines jointly
- **Processor:** processes personal data on behalf of the controller, acts under instructions from controller

- Relevance: Liability and accountability

Source : J. Dhont, I. Vereecken and M. Scuvée

Part 2: The controllers and processors responsibilities

Relationship between controllers

akd

- **Joint controllership**

  - **Arrangement necessary**: "*They shall in a transparent manner 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 13 and 14*" (art. 26.1 GDPR)

  - Leads to **joint responsibility**, the arrangement "*shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects*" & its essence shall be made available to them (art. 26.2 of the GDPR)

  - **Each controller can be held fully liable** for the entire damage "*the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers*" (art. 26.3 of the GDPR)

Relationship between controller and processor

akd

- Controller must choose and "*use only processors providing sufficient guarantees*" (art. 28.1 GDPR)
- Processor acts upon the controller's instructions ; Controller is responsible for the provided instructions
- Mandatory to conclude a Data Processing Agreement ("DPA") :

  "*Processing by a processor shall be **governed by a contract or other legal act** under Union or Member State law, that is binding on the processor with regard to the controller and that **sets out the subject-matter and duration** of the processing, **the nature and purpose** of the processing, the **type of personal data** and **categories of data subjects** and the obligations and rights of the controller*." (art. 28.3 GDPR)

- Which must at a minimum stipulate that the processor:

i. processes data only on the controller's documented instructions;
ii. ensures confidentiality of its personnel;
iii. takes all appropriate measures to ensure security of processing;
iv. respects the conditions for engaging a sub-processer;
v. assists the controller, in the fulfilment of its obligations regarding data subject;
vi. assists the controller in ensuring compliance with its obligations of : security, data breach notification, data protection impact assessment
vii. at the end of the provision of services, must deletes or returns all personal data to the controller;
viii. makes available to the controller the information necessary to demonstrate compliance with the obligations of art. 28 & allow and contribute to audits by the controller.

Accountability

akd

Article 5.2 GDPR

"*The **controller shall** be responsible for, and be **able to demonstrate** compliance*" with the principles relating to processing of personal data

- Actively implement measures to safeguard data protection in processing activities
- Responsible to implement measures to comply with the GDPR
- Must be able to demonstrate compliance

  in practice: by using documentation, records, internal policies and procedures

Duty to inform the data subjects

akd

Transparency obligations of controllers (art. 12, 13 and 14 GDPR)

- *Ratio legis* data subjects should in principle:
  - be notified of the processing of their personal data
  - have means to obtain further information
  - have means of recourse against the data controller
- Controllers are **required to provide information** "*to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language*": usually through a privacy policy
- The data subject must be informed of:
  i. the identity and contact details of the controller;
  ii. the purposes and legal basis of the processing;
  iii. the (categories of) recipients;
  iv. the period for which the personal data will be stored;
  v. the data subject's rights;
  vi. etc.
- Controllers also have a **duty to respond to data subject request**

Data protection by design

akd

- **Privacy by design**

  - "*the **controller shall**, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are **designed to implement data-protection principles**, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects*." (art. 25.1 GDPR)

- Data protection must be integrated at the earliest stages when designing IT systems and processes
- Regulates processing of personal data through the technology itself
  - Use of pseudonymisation
  - Use of encryption of personal data

Data protection by default

akd

- **Privacy by default**

  - "*The **controller shall** implement appropriate technical and organisational measures for **ensuring that, by default**, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.*" (art. 25.2 GDPR)

- By default, controller should ensure that personal data is processed with the highest privacy protection
  - e.g. only the data necessary should be processed, short storage period, limited accessibility
- Ensure that by default personal data isn't made accessible to an indefinite number of persons
- Use of settings that protect privacy by default without manual input from the end user

Records of processing activities

akd

Controllers and processors should keep records of their data processing activities

- In order to:
  - be able to demonstrate compliance,
  - respond to data subject request, and
  - ensure that supervisory authorities can receive the necessary documentation
- Content of the records is described in article 30 GDPR

Exception

- Not mandatory to have a records "*for enterprise or organisation employing fewer than 250 persons*"
- **Unless** the processing carried out by the controller or processor:

i. "*is likely to result in a risk to the rights and freedoms of data subjects*",
ii. "*the processing is not occasional*", or
iii. "*the processing includes special categories of data*".

Cooperate with supervisory authority

akd

Obligation of the controller and processor

Article 31

Cooperation with the supervisory authority

The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks.

- Obligated to cooperate with the supervisory authority solely upon its request
- Tasks and powers of supervisory authority described in Articles 57 and 58 GDPR
- Cooperation obligation *e.g.* provide documentation necessary to demonstrate compliance, provision of records of processing activities upon request, obligation to report a data breach

Implement security measures (1)

akd

Controllers and processors must implement appropriate technical and organisational measures

- Article 32.1 GDPR
  - "***Taking into account*** *the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons,* ***the controller and the processor shall implement*** *appropriate technical and organisational* ***measures to ensure a level of security appropriate to the risk***"

Appropriate technical and organisational measures

- **Organisational**: policies within the organisations & physical security
  - Company protocol to solely collect the necessary data, internal policies in case of data breach / security incident
  - Awareness training, risk assessments, audits, records of informed consent received from data subjects
- **Technical**: security of the systems
  - Access control to organisation's premises, use of firewall and antivirus, access control, robust passwords & use of two factor authentification, encryption or pseudonimysation of personal data

Implement security measures (2)

akd

The **controller and processor** shall implement measures "*to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services*"

- **Confidentiality**: protect the systems/data against unauthorised access (hacking); keeping the content of information secret
- **Integrity**: protect the authenticity of the data; ensuring that the data has not been altered by unauthorised or unknown means
- **Availability**: protect the data against accidental destruction or loss; ensure the accessibility of the systems and the ability to restore availability

Breach notification

akd

Controllers have an obligation to

1) **Notify** personal data breaches to the **supervisory authorities** (art. 33.1 GDPR)
   - Unless, "*the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons*"
   - Within *"72 hours after having become aware of it"*
2) **Communicate** personal data breach **to the data subject,** without undue delay, when "*the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons*" (art. 34.1 GDPR)
3) **Document** any personal data breaches (facts, effects, actions taken)
   - Enables supervisory authority to verify compliance (accountability principle)

Processors have a duty to *"notify the controller without undue delay after becoming aware of a personal data breach*" (art. 33.2 GDPR)

Data protection impact assessment (1)

akd

Obligation for the controller to carry out a data protection impact assessment or DPIA

- When a type of 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***" (art. 35.1 GDPR)

- **A DPIA is required** in the case of (art. 35.3 RGPD):
  - automated processing on which **decisions** are based that produce legal effects on or similarly affect the data subject;
  - processing on a large scale of special categories of data or data relating to criminal convictions and offences;
  - "*systematic monitoring of a publicly accessible area on a large scale*".

Data protection impact assessment (2)

Obligation for the controller to carry out a data protection impact assessment or DPIA

- The assessment must be **documented in writing & at least contain**:
  i. a description of the envisaged processing operations and the purposes;
  ii. an assessment of the necessity and proportionality of the processing operations in light of the purposes;
  iii. an assessment of the risks to the rights and freedoms of the concerned data subjects; and
  iv. the measures envisaged to address the risks (goal of the DPIA)

- If the DPIA indicates that the processing would result in a high risk in the absence of mitigating measures, the **controller must consult the supervisory authority** prior to processing (art. 36.1 GDPR)

Appointment of a DPO

akd

- **Controller and processor** shall designate a data protection officer when:
  - the processing is carried out by a public authority or body
  - the core activities of the entity consist of processing operations that require regular and systematic monitoring of data subjects on a large scale
  - the core activities of the entity consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences
- Other entity can designate a DPO, it is not mandatory but a good practice
- **The DPO's tasks**
  - informs and advise on compliance with the GDPR
  - cooperate with & act as contact point for supervisory authorities
  - monitor compliance and assist the controller with performing a DPIA
- **The DPO** (i) must be involved in all issues regarding personal data; (ii) receive sufficient resources; (iii) report to the highest management level; (iv) is the contact point for data subject

Thank you !
Questions or Comments?

- www.akd.eu

- obelleflamme@akd.eu
- T: +32 629 42 74
- M: +32 472 03 48 93