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.

akd

# Roles and responsibilities of data controllers and data processors

**Olivier Belleflamme**

**ERA | June 25, 2025**

# Nearly EUR 6 Billion in Fines Since the GDPR

**DLA PIPER** / 18 FEBRUARY 2025 / HITS: 16543

## EU hands Meta record $1.3 billion fine over data transfers to US

The social media giant Meta was hit with a re billion fine (about $1.3 billion) on Monday for illegally transferring d ons to the United States.

## Dutch data privacy regulator fines Uber $324 million for failing to adhere to GDPR

The Dutch Data Protection Authority (DPA) announced Monday that it has fined Uber €290 million ($324 million) for gathering sensitive data from European drivers and then transferring it to the U.S. without appropriate safeguards.

## Amazon hit with $886m fine for alleged data law breach

## Instagram owner Meta fined €405m over handling of teens' data

Penalty follows investigation into Instagram setting that allowed teenagers to set up accounts that displayed contact details

## TikTok fined €530m by Irish regulator for failing to guarantee China would not access user data

Ireland's Data Protection Commission found video app breached GDPR and had submitted 'erroneous information' to inquiry

# Part 1 –

# The Actors & Their Evolving 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 (…)*"
> (Article 4(7) GDPR)


Defined **broadly** to ensure effective and complete protection

- **Determines** = Exercise influence on the processing with its decision-making power
- **Purposes and** *essential* **means** = The objective (why) and how to reach this goal
- **Processing** = Any operation performed on personal data


*Is direct control over or access to the data necessary?*

# Controllers and Joint controllers

akd

***Sole or separate controllers***

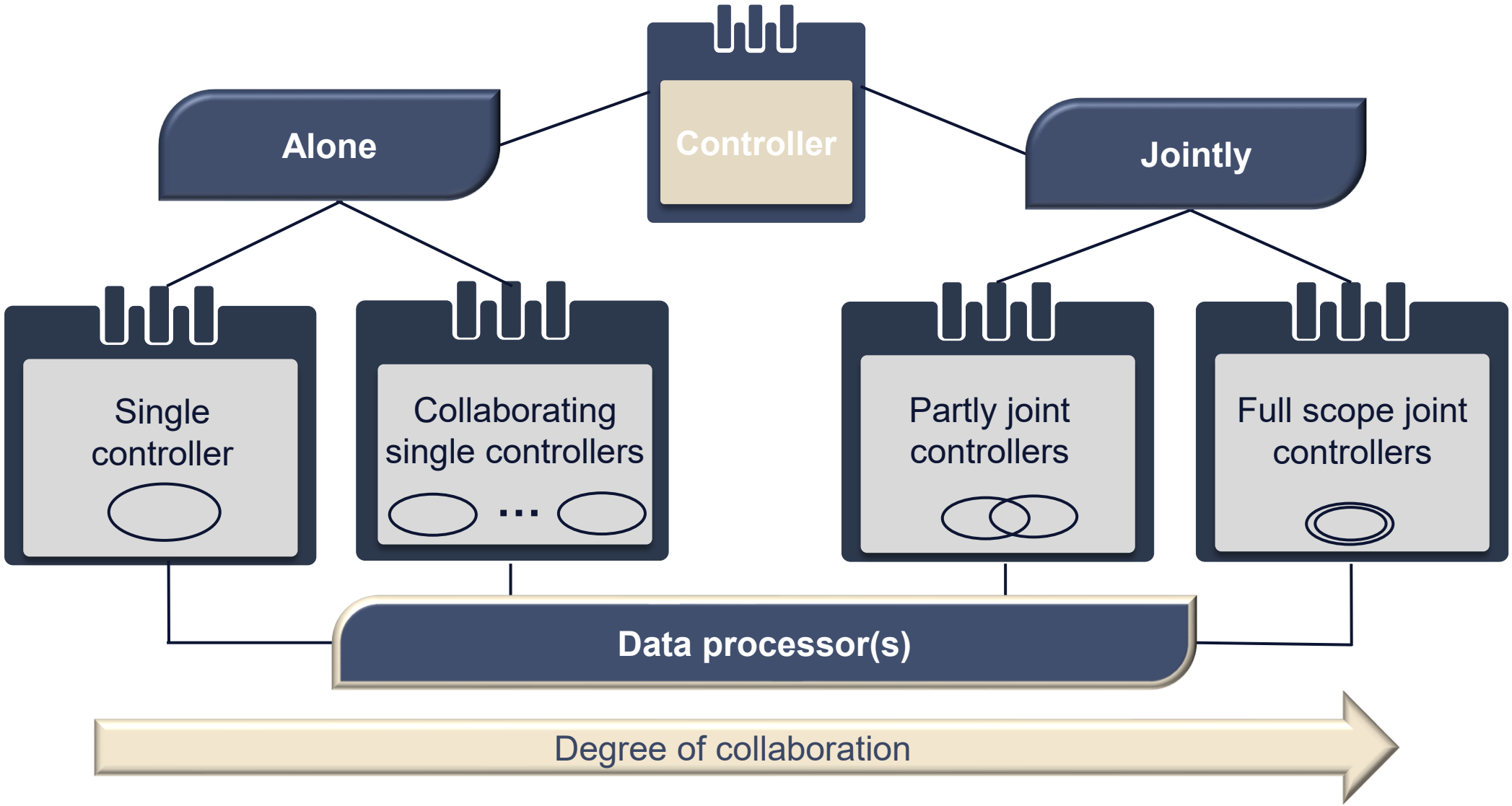
- **Sole controller**: One party determines the purposes and means of the processing
- **Separate controllers**: Exchange data, but each determine their own purposes and means

**Joint-controllership**: "*Where two or more controllers **jointly determine** the purposes and means of processing, they shall be joint controllers."* (Article 26(1) GDPR)

- Relevance: Allocation of obligations "*They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation*"
- Assessment criteria (similar to assessing "single" control)
  - Common decision: Jointly decide with shared intention
  - Converging decision: Complementary roles necessary for processing
- Joint responsibility ≠ equal responsibility

# Controllers and joint-controllership

akd




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

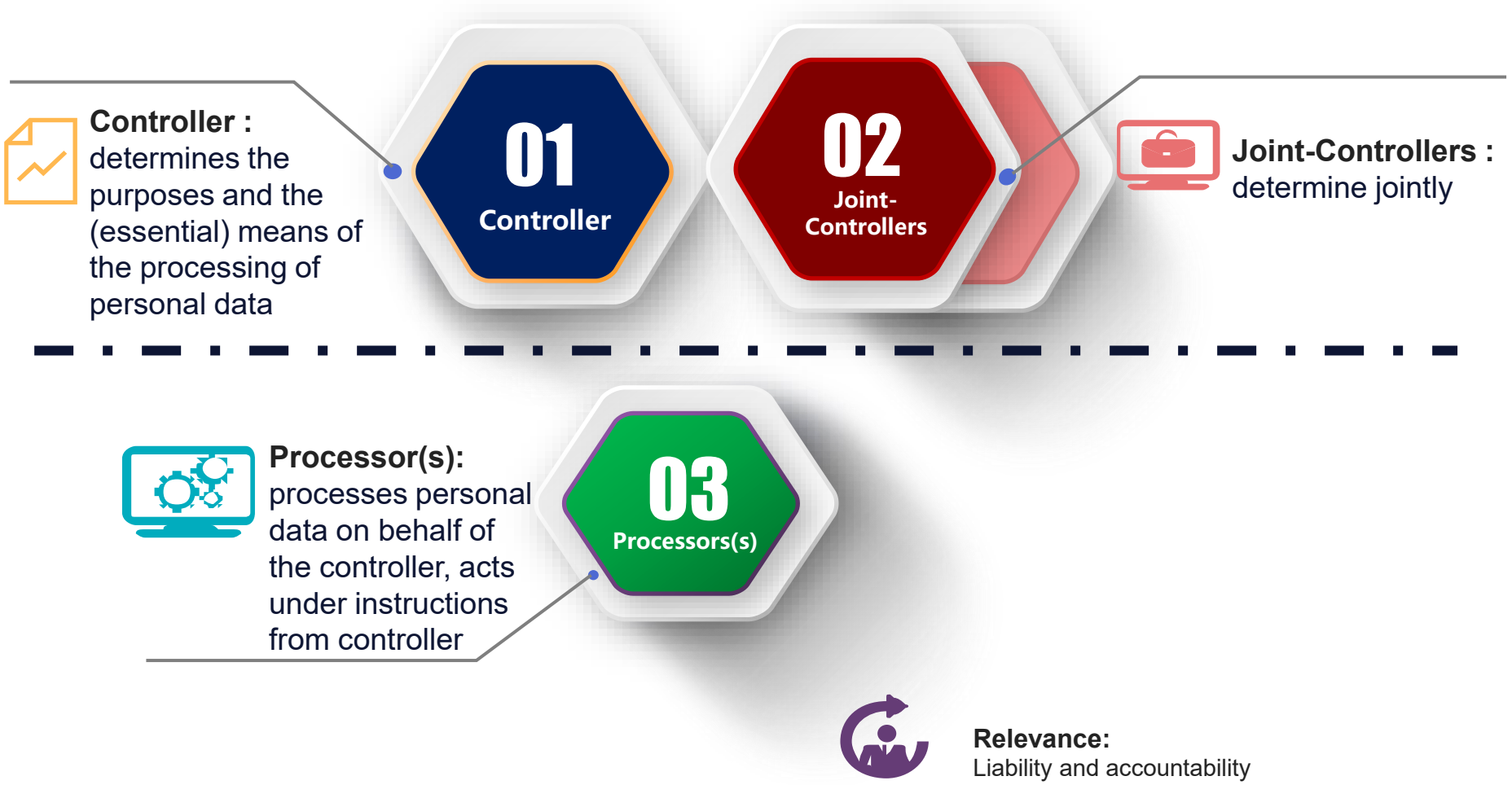
# Processor

Processor means "*a natural or legal person, public authority, agency or other* ***body*** *which* ***processes personal data on behalf of the controller***" (Article 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 & essential means
  - May not carry out processing for its own purpose: when acting outside of the controller's instructions, the processor becomes a 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*" (Article 28(3) GDPR)

# In summary




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

# Key Case Law

| Cases | Role Recognized | Why |
|---|---|---|
| ***Wirtschaftsakademie C-210/16*** | Fan page admin = **joint controller** with Facebook | Sets parameters, benefits from insights — controller = functional concept |
| ***Jehovah's Witnesses C-25/17*** | Religious community = **joint controller** with members | Community organized and directed note-taking — influence over purposes |
| ***Fashion ID C-40/17*** | Website = **joint controller** for data sent to Facebook | Embedded 'Like' button for economic gain – Triggered and benefited from the data transfer by embedding the 'Like' |

## 🎯 Takeaways

- **Joint controllership** arises when entities **influence the purposes or means** of data processing
- **Controllers can act at different stages** or with varying degrees of involvement
- **Contractual terms are not decisive** – what matters is the **functional role**
- **Joint responsibility ≠ equal liability**, and may apply even **without direct access** to the data

# Meta's Controller Addendum

akd

## Controller Addendum

This Controller Addendum applies when it is expressly incorporated by reference into terms for Meta Products, such as the **Meta Business Tools Terms** (any such terms, "**Applicable Product Terms**", any covered Meta Products, "**Applicable Products**"). Capitalised terms used but not defined in this Controller Addendum have the meanings given in the Applicable Product Terms. In the event of any conflict between the Applicable Product Terms and this Controller Addendum, this Controller Addendum will govern solely to the extent of the conflict.

Meta and you agree to the following:

- Meta Platforms Ireland Limited, Merrion Road, Dublin 4, D04 X2K5, Ireland ("**Meta Ireland**" or "**we**") and you (each a "**Party**", together the "**Parties**") are Joint Controllers in accordance with Article 26 GDPR for the Joint Processing specified by the Applicable Product Terms. The scope of the Joint Processing and this Controller Addendum covers the collection of the Personal Data specified by the Applicable Product Terms and its transmission to Meta Ireland; the subsequent processing of data by Meta Ireland does not form part of the Joint Processing. More information on the Joint Processing can be found in the Applicable Product Terms.
- This Controller Addendum determines Meta Ireland's and your responsibilities for compliance with the obligations under the GDPR with regard to the Joint Processing. The Joint Processing is subject to the provisions of this Controller Addendum. They apply to all activities in which the Parties, their employees or their Processors are involved in the Joint Processing.
- You agree to follow the available documentation regarding the correct technical implementation of the Applicable Products into your websites or apps and their configuration.
- Meta Ireland's and your responsibilities for compliance with the obligations under the GDPR with regard to the Joint Processing are determined as follows:

| No. | Obligation under GDPR | Meta Ireland | You |
|---|---|---|---|
| 1 | Article 6: Requirement of legal basis for Joint Processing | X<br>(regarding Meta Ireland's processing) | X<br>(regarding your own processing) |
| 2 | Articles 13,14: Providing information on Joint Processing of Personal Data | | X<br>This includes as a minimum the provision of the following information in addition to your standard data policy or similar document:<br><br>That Meta Ireland is a Joint Controller of the Joint Processing and that the information required by Article 13(1)(a) and (b) GDPR can be found in Meta Ireland's Privacy Policy at |

# GDPR Roles in Complex Data Ecosystems

akd

*In a data-driven economy, organisations rarely process personal data alone*

- Cloud providers, ad tech partners, app developers, data analytics firms...
- These actors often **shape or enable** data processing
- GDPR roles like *controller* and *processor* are no longer static
  - Roles are **dynamic and context-dependent**
  - Entities can **switch roles** depending on the activity
  - The line between *controller* and *processor* has become blurred

*How do we determine **who is a controller** and **who is a processor** in **multi-party data environments**?*

- It's about **real influence** over **why** and **how** data is used
- *Increasingly complex: multiple layers of subcontracted services, technical opacity, shared decision-making*

# App development for Covid-19 Tracking

**Nacionalinis visuomenės sveikatos centras (C-683/21, Grand Chamber CJEU, 5 December 2023)**

- Facts: National Public Health Centre of the Lithuanian Ministry of Health instructs a company to build a mobile app (provided: design information and questions) for the monitoring of COVID-19 cases: Jointly fined for GDPR violations
- Key Questions: (1) Can a public body that only instructed the processing of data be qualified as a "controller"? ; (2) Do **joint controllers** need an arrangement to be held responsible?
- CJEU Decision:
  - NVSC didn't operate the app or host the data BUT the app was created to meet the Centre's **objectives** and according to its **instructions**
  - The Centre for Public Health thereby **participated** in the determination of the **purposes and means** of the processing – unless they had expressly objected to the making public of the app (up to the national court)
  - **No formal arrangement required** for the qualification – it is **appreciated** ***in concreto***
- Conclusion: An entity outsourcing IT application development can be seen as a data Controller if it **influences** data processing decisions. **Joint controllership** does not require a formal arrangement but involves converging decisions impacting data processing. A Controller may be fined for processing operations performed by a Processor on its behalf, unless the Processor carried them out for its own purposes / in a manner incompatible with their arrangements.

# When coordinating actor shape the system

**IAB Europe (C-604/22, Grand Chamber CJEU, 7 March 2024 & Belgian Court of Appeal 14 May 2025)**

- Facts: IAB Europe designed a Transparency and Consent Framework (TCF) to record user preferences and communicate it to its members using a TC String – IAB did **not process data directly** but it **structured how** others did
- Decision:
  - IAB Europe is a **joint controller** with its members as it determines the **purposes** (the sale of advertising space on the Internet) and the **means** (a framework, compulsory for all its members) of the processing of data
  - Joint controllership **does not extend automatically to all subsequent processing** of the data by members or third parties – it must be determined for each operation
  - Fine upheld – Held liable for lack of legal basis, transparency, DPIA, sufficient security measures
- Takeaways:
  - IAB acted as a **coordinator**, not a typical data user – yet still a controller
  - GDPR roles are **based on influence**, not access or execution
  - Ecosystems involve **layered responsibilities** – joint, partial, evolving
  - Courts apply a **functional, context-based test** in ecosystems with many players

# Key takeaways

akd

| | Wirtschaftsakademie | Jehovah's Witnesses | Fashion ID | NVSC | IAB Europe |
|---|---|---|---|---|---|
| **Decisive/ factual influence** | - No processing without cookies (*means*)<br>- Setting of processing parameters (*purposes*) | - Community members determined data collection modalities (*means*)<br>- Community encourages data collection (*purposes*) | - No processing without embedment of plugin (*means*) | - No processing without instructions and objective of monitoring pandemic (*purposes*) | - No processing without compulsory framework and instructions (*means*)<br>- No processing without purpose of promotion and sale of advertising space on the Internet (*purposes*) |
| **Interest** | - Processing serves WA's own interests | - Processing serves Community's own interests | - Processing serves Fashion ID's own interests | - Processing serves NVSC's own interests | - Processing serves IAB Europe's own interests |
| **Comments** | - Relevance of "decisive influence" / "dependence" of parties<br>- "Interest" in the processing → potentially points to joint decision on purposes<br>- Interests of parties do not need to converge | | | | |

# Part 2 –
# The Controllers and Processors Responsibilities and Challenges

# Controller's Responsibilities

akd

- Comply with the data protection principles under (Art. 5 GDPR)
- Uphold individuals' data protection rights
- Keep clear records of processing activities
- Ensure security of processing
- Choose trustworthy data processors
- Sign a binding contract with processors (detailing the relationship – DPA)
- When acting as Joint Controllers, define each party's responsibilities in a clear arrangement
- Notify personal data breaches to the relevant Supervisory Authority and to individuals, where applicable
- Demonstrate accountability for the processing operations, practise data protection by design & default, conduct data protection impact assessments when necessary
- Appoint a data protection officer when necessary
- Comply with the data protection obligations on international transfers of personal data
- Cooperate with Supervisory Authorities

# Processor's Responsibilities

- Follow the Controller's instructions
- Keep records of processing activities
- Ensure the processing is secure using appropriate measures
- Respect and uphold the terms of the Data Processing Agreement
- Get prior authorisation of the Controller before engaging a new sub-processor (and give the controller a possibility to object). *If applicable*, a processor - sub-processor contract must be put in place and refer to the initial DPA
- Notify personal data breaches to the Controller
- Notify GDPR breaches to the Controller
- Assist the Controller in ensuring compliance with its obligations
- Appoint a data protection officer when necessary
- Ensure that international transfers are authorised by the controller and comply with the GDPR
- Cooperate with Supervisory Authorities

# 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*" (Article 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 (Article 26(2) 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*" (Article 26(3) GDPR)

# Relationship between Controller and Processor

akd

- Controller must choose and "*use only processors providing sufficient guarantees*" (Article 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*." (Article 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: 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 Article 28 & allow and contribute to audits by the controller.

# Duty to inform the data subjects

akd

**Transparency obligations of controllers (Articles 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 notice
- 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 requests**

# 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*".

# 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

# Non-compliance can be expensive

akd

**VODAFONE Fined 45 Million EUR by the BfDI for GDPR Violations**

- **€15M Fine** – Poor monitoring of partner agencies /processors (Art. 28.1 GDPR)
  - *Use of partner agencies that broker contracts with customer on behalf of Vodafone*
  - Partner agencies misused customer data
  - BfDI considered the agencies' behavior to be the result of inadequate monitoring
  - Vodafone lacked effective processes for selecting, auditing and continuously monitoring the partners
- **€30M Fine** – Security flaws in authentication process (Art. 32 GDPR)
  - *Authentication process when using "MeinVodafone" in connection with telephone customer support*
  - A technical combination attack on both systems made it possible to gain access to user account
- **Warning issued** – Vulnerabilities in sales system

💡 **The Lesson**

- GDPR compliance requires more than formal contracts – it demands active, risk-based oversight of processors and technical systems
- Controllers are required to implement technical and organizational measures that reflect the real-world risks to personal data

# Breach notification

akd

**Controllers have an obligation to**

1) **Notify** personal data breaches to the **supervisory authorities** (Article 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*" (Article 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*" (Article 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***" (Article 35(1) GDPR)

- **A DPIA is required** in the case of (Article 35(3) GDPR):
  - 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)

akd

**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 (Article 36(1) GDPR)

# New Challenges for Controllers in AI Ecosystems

akd

Scope of due diligence when engaging processors expands

- "*Today's AI landscape demands a sophisticated, multi-layered assessment architecture that meticulously evaluates technical robustness, regulatory compliance postures, and ethical governance across every stratum of the service delivery ecosystem, from primary vendors to the most distant subprocessors.*"

AI Vendors, from Processor to (joint) Controller

- Use vast datasets to train algorithms – transforms input into output through complex/opaque neural network layers
- Output is significantly shaped by the AI's training process (managed by AI vendor)
- Pivots on the decision-making authority – JC frequently arise, when data is also leveraged for training, refinement

The GDPR and EU AI Act

- AI Act introduces a range of stakeholder: providers, deployers, importers, distributors, and manufacturers
- Complex task of navigating the regulatory frameworks & Challenge to define and classify roles and responsibilities

# Technical Challenges with AI

akd

**Tensions between traditional data protection principles and full deployment of AI and Big Data**

- **Data minimisation vs Need for large datasets**
  - AI systems increasingly depend on large volumes of data (gathered via web scraping or data brokers)
  - When personal data is used to train the system, collection and use must comply with the GDPR
  - Challenging to uphold Data subjects' rights (access, erasure, portability, …)
- **Transparency vs Opacity**
  - Users frequently remain unaware of how their information is collected and processed, many platforms engage in opaque data sharing arrangements
  - AI can replicate or worsen **biases** present in training data, resulting in **unfair or discriminatory outcomes** Real-world examples: biased hiring algorithms that favor specific demographics & predictive policing tools faced scrutiny for disproportionately targeting minority communities, perpetuating cycles of inequity

⚠ Data protection cannot be an afterthought in AI development – it must be embedded from the start

- Modern compliance goes beyond meeting standards – it's about managing real risks

# Thank you !
# Questions or Comments?


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