ROLES AND RESPONSIBILITIES OF DATA CONTROLLERS AND DATA PROCESSORS (GENERAL)

Matus Huba

ERA Young European Lawyers Academy

Trier, 11 June 2024

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.

McDermott Will & Emery BELGIUM LLP

WHAT WILL WE COVER TODAY?

- Identifying Controllers, Join Controllers & Processors
- Key Statutory Responsibilities
- Controller, Joint Controller & Processor Contractual Responsibilities
- Controller & Processor Liability

IDENTIFYING CONTROLLERS, JOIN CONTROLLERS & PROCESSORS

DEFINITION OF THE (JOINT) CONTROLLER

Art. 4(7) GDPR

- *"**the natural or legal person, public authority, agency or other body** which,*
  - *Individual v group of individuals (Judgment in Jehovah's witnesses, C-25/17)*

- ***alone** or **jointly** with others,*
  - *Independent v joint controllership*
  - *Joint controllership (Art. 26 GDPR) – common v converging decisions*
  - *Would processing be possible without one of the parties – is it inextricably linked?*
  - *Where one of the controllers decides alone the purposes/means of operations that take place before/after jointly determined operations → independent controller (Judgment in Fashion ID, C-40/17; Judgement in IAB Europe, C-604/22)*
  - *Use of a common system/network/infrastructure does <u>not</u> always = joint controllership. However, if an entity makes means available to other participants → may be considered joint controllers, under certain circumstances (Judgement in IAB Europe, C-604/22).*

- ***determines***
  - *Factual control*
  - *Explicit legal competence (legal task/duty to process certain personal data)*

DEFINITION OF THE (JOINT) CONTROLLER (CONT.)

- *the **purposes** and **means***
  - *Level of influence over why & how*
  - *Essential (e.g., categories of personal data/data subjects/recipients, duration, minimum TOMs) v non-essential (e.g., type of SW, details of TOMs implementation) means*

- ***of the processing of personal data**;*
  - *"any operation or set of operations which is performed on personal data or on sets of personal data […]" (Art. 4(2) GDPR)*
  - *"any information relating to an identified or identifiable natural person […]" (Art. 4(1) GDPR)*
  - ***No need to have access to personal data processed!** (Judgment in Wirtschaftsakademie Schleswig-Holstein GmbH, C-210/16; Judgment in Jehovah's witnesses, C-25/17) – keep in mind re data sharing arrangements*
  - *Single processing operation or a set of operations → entire processing, or only a part of it (Judgment in Fashion ID, C-40/17)*

- *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"*

DEFINITION OF THE (SUB) PROCESSOR

Art. 4(8) GDPR

- *"**natural or legal person, public authority, agency or other body***
  - *Must be a separate entity*
  - *Can two companies within the same group of companies be in a processor-controller relationship?*
  - *What about individuals within an organization acting under the organization's authority? (Art. 29 GDPR)*

- *which **processes personal data***
  - *Can never determine the purpose of processing.*
  - *Able to make (some) decisions on how to carry out the processing?*

- ***on behalf of the controller**"*
  - *Delegation with a limited level of discretion → processor becomes controller, if it goes beyond such discretion (essential v non-essential means)*
  - *Processor can offer a pre-defined service, but the controller must approve the way the processing is set up, at least regarding the essential means of the processing*
  - *Lawfulness of such processing*
  - *Processor can engage other (sub-)processors*

COMMON INTERPRETATION RULES

- **Factual analysis** v assigning the roles through a contract
  - Can contract play a role? When?

- **Broad interpretation** – favor protection of individuals (*Judgement in Google Spain, Case C-131/12*)

- Controller & Processor and **similar concepts under other laws** – equal or not?
  - Creator/rights holder in IP;
  - Provider/authorized representative in AI;
  - Customer/service provider in Commercial relationships; etc.

* ***Resources****: EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, version 2.1, adopted on 7 July 2021, available at: https://www.edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf*

OTHER RELEVANT DEFINITIONS

- **Recipient** – *"a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not […]" (Art. 4(9) GDPR)*
  - Excludes public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law *(e.g., tax and customs authorities, financial investigation units, independent administrative authorities, or financial market authorities responsible for the regulation and supervision of securities markets – Rec. 31 GDPR)*

- **Third Party** – *"a natural or legal person, public authority, agency or body* ***other than*** *the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data"(Art. 4(9) GDPR)*

KEY STATUTORY RESPONSIBILITIES

CONTROLLER RESPONSIBILITIES

- **Ensure compliance with data protection principles** (Art. 5 (1) GDPR)
  - **Lawfulness, fairness and transparency;**
  - **Purpose limitation**
  - **Data minimization**
  - **Accuracy**
  - **Storage limitation**
  - **Integrity and confidentiality**

- **…and be able to demonstrate such compliance** (so-called '**Accountability**') (Art. 5(2) GDPR)
  - Records of processing activities ('**ROPAs**') (Art. 30 GDPR), may serve as an accountability tool (controller must provide ROPAs to the supervisory authority upon request)
  - **Exemption** – enterprise/organization <250 employees unless likely to result in a risk to the rights and freedoms of data subjects, it is not occasional, or contains special categories of personal data/relates to criminal convictions/offences

- General requirement to **cooperate with supervisory authorities** (on request) (Art. 31 GDPR)

CONTROLLER RESPONSIBILITIES (CONT.)

- **Provide data subjects with information about the processing** (Art. 13/14 GDPR)
  - Timing
  - Content ("*concise, transparent, intelligible and easily accessible form, using clear and plain language*")
    - the identity and the contact details of the controller
    - contact details of the DPO (if applicable)
    - purposes and legal basis for the processing
    - recipients or categories of recipients of the personal data, if any
    - where applicable, the intention to transfer personal data outside the and whether there is an adequacy decision; in other cases, reference to safeguards and how to obtain a copy of the same
    - source of the data (where different from data subject)
    - retention period
    - information on various data subject rights (including right to lodge a complaint with the supervisory authority) and existence of automated decision-making, including profiling
  - Exemptions (Art. 14 (5) GDPR)

- **Facilitate the exercise of data subject rights** (Arts. 15 – 22 GDPR)

CONTROLLER RESPONSIBILITIES (CONT.)

- **Implement data protection by design** (Art. 25(1) GDPR)
  - "*Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing*", controller is required to **implement technical and organizational measures designed to implement data protection principles from the outset** (when determining means of processing/at the time of processing)

- **Implement data protection by default** (Art. 25(2) GDPR)
  - Ensure that **by default, only personal data necessary for each specific purpose of the processing are processed.**

CONTROLLER RESPONSIBILITIES (CONT.)

- **Identify, Analyze, Notify and Document Data Breaches** (Arts. 33/34 GDPR)
  - **Identify:** Breach of **security** leading to the **accidental or unlawful** destruction, loss, alteration, unauthorized disclosure of, or **access to**, personal data transmitted, stored or otherwise processed.
    - The threshold is very low, as even accidental access is considered a breach.
  - **Analyze:** Determine whether suspected personal data breach indeed is one and whether it is notifiable. Remember, not every breach is a notifiable breach!
    - Controller has to notify relevant **EU supervisory authorities** without undue delay but **no later than within 72h after becoming aware of the breach** *(reasonable degree of certainty)*, **unless** the personal data breach is **unlikely to result in a risk** to the rights and freedoms employees.
    - Controller has to communicate personal data breach to **affected data subjects without undue delay**, **if** data breach is **likely to result in a high risk** to their rights & freedoms.
  - **Notify:** Determine whether suspected personal data breach indeed is one and whether it is notifiable. Remember, not every breach is a notifiable breach!
    - Categories & number of data subjects, categories and approximate number of personal data records concerned
    - Data protection officer or contact point
    - Likely consequences of the breach
    - Measures taken or proposed, including, how the breach will be mitigated
  - **Document:** **Any** **personal data breach**, comprising the facts relating to the personal data breach, its effects and the remedial actions taken.

- Breaches may be notifiable under other legal frameworks *(ePD, NIS 2, MDR, IVMDR, PSD2, DORA, etc.)*

CONTROLLER RESPONSIBILITIES (CONT.)

- Implement appropriate **technical and organizational measures** (‘**TOMs**’) (Art. 32 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, including inter alia as appropriate
    - The pseudonymisation and encryption of personal data
    - The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
    - The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
    - A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing

  - Any natural person acting under the authority of the controller who has access to personal data must not process it, except on instructions from the controller, unless required to do so by EU/Member State law (Art. 32(4) GDPR)

CONTROLLER RESPONSIBILITIES (CONT.)

- Assess and address **high-risk processing** (Art. 35/36 GDPR)

  - A so-called **Data Protection Impact Assessment ('DPIA') required** when processing of personal data is likely to result in high risk to rights and freedoms of employees (particularly new technologies) – prior to processing:
    - Nature, scope, context and purposes of the processing
    - Assessment of the necessity and proportionality of the processing
    - Assessment of the risks to the rights and freedoms of data subjects
    - Measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with data protection rules

  - **DPIA required in particular when processing includes:**
    - systematic and extensive evaluation - based on automated processing - decisions produce legal effects / similarly significantly affect data subjects
    - processing on a large scale of special categories of data (e.g., processing of trade union membership data for all Amcor in one database)
    - systematic monitoring of a publicly accessible area on a large scale (e.g., CCTV coverage)

  - **Consider national lists**

CONTROLLER RESPONSIBILITIES (CONT.)

- Designate a **representative in the EU** (Art. 27 GDPR)
  - Where extraterritorial application of the GDPR under Art. 3(2) applies

- **Appoint a data protection officer** (‘**DPO**’)
  - Designate a DPO, publish DPO details and communicate them to the supervisory authority (Art. 37 GDPR)
    - Processing is carried out by a public authority or body, except for courts acting in their judicial capacity
    - Core activities 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
    - Core activities consist of processing on a large scale of special categories/personal data relating to criminal convictions and offences
  - Ensure that the DPO is involved, properly and in a timely manner, in all issues which relate to the protection of personal data;
  - Support the DPO in performing their tasks by providing necessary resources;
  - Ensure the DPO does not receive any instructions regarding the exercise of their tasks, or is dismissed or penalized for performing them;
  - Ensure DPO reports to highest management levels;
  - Where DPO performs other tasks and duties, ensure these do not result in a conflict of interests (Art. 38 GDPR)

CONTROLLER RESPONSIBILITIES (CONT.)

– Ensure **transfers (including onward transfers)** of personal data to third countries or international organizations take place only subject to appropriate safeguards (Chapter V GDPR)

GDPR applies

- Controller/Processor is in the EEA
- Controller/Processor outside the EEA:

  a) but processing inextricably linked to activities of an establishment in the EEA

  b) offers good/services to EEA residents

  c) monitors their behavior

Personal data is disclosed

- Disclosed by transmission
- Otherwise made available by the exporter to another

Importer in a 3rd country

- Outside of the EEA
- 'Adequate' countries – still a transfer, but same regime as EEA (e.g., the UK)

✓ A data subject disclosing his/her own personal data directly cannot be considered an "exporter";

✓ Transfers also include 'onward transfers' – need to ensure compliance all the way down the transfer chain.

CONTROLLER RESPONSIBILITIES (CONT.)

Rule: 'Transfers' outside of the EEA must be either to an adequate country, or protected by an appropriate safeguard.

Adequacy Decision

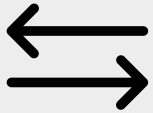
- Third countries recognized by EU as providing adequate protection to UK personal data;
- Countries are the same (for now): Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the UK under the GDPR and the LED, Uruguay, the United States commercial organizations participating in the EU-US Data Privacy Framework only;
- EU negotiating with other countries.

EU Standard Contractual Clauses (SCCs)

- Contractual protections;
- Parties cannot modify, except for specific clauses (e.g., governing laws, type of authorization for processors, etc.);
- All can be used as standalone solutions;
- Need to choose the correct module, depending on the role of the parties
  - *Controller to controller*
  - *Controller to processor (**Note**: includes Art. 28 GDPR DPA)*
  - *Processor to processor*
  - *Processor to controller*

EU / UK BCRs

- Set of binding internal data processing/transfer rules and policies;
- Approved by EU regulators;
- Controller BCRs – for intra-group transfers;
- Processor BCRs – for transfers to non-EEA processors.



Other Safeguards / Derogations

- Codes of conduct;
- Certifications;
- In the absence of adequacy/other safeguards (SCCs, BCRs) - derogations:
  - Explicit consent;
  - Performance of contract;
  - Establishment, exercise or defence of legal claims;
  - If not repetitive & for limited number of data subjects – for compelling legitimate interests
  - Etc.

PROCESSOR RESPONSIBILITIES

- **Statutory responsibilities are more limited compared to controller – broad contractual requirements**
  - Maintain and make available to a supervisory authority on request the records of processing activities ('**ROPA**') in writing, subject to exceptions provided by law (Art. 30(2) GDPR)
  - **Cooperate with supervisory authorities** (on request) (Art. 31 GDPR)
  - Implement appropriate technical and organizational measures ('**TOMs**') to ensure a level of security appropriate to the risk (Art. 32 GDPR)
  - Notify the controller without undue delay after becoming aware of a **personal data breach** (Art. 33(2) GDPR)
  - Designate a data protection officer ('**DPO**') to the extent required by law and publish DPO details and communicate them to the supervisory authority (Art. 37 GDPR); ensure appropriate involvement and protections of the DPO position (Art. 38 GDPR);
  - Designate a **representative in the EU** to the extent required by law (Art. 27 GDPR)
  - Ensure **transfers (including onward transfers)** of personal data to third countries or international organizations take place only subject to appropriate safeguards (Chapter V GDPR)

CONTROLLER, JOINT CONTROLLER & PROCESSOR CONTRACTUAL ARRANGEMENTS

CONTROLLER-TO-PROCESSOR
(PROCESSOR-TO-SUB-PROCESSOR)

- **Processor assessment** → Controllers to use only processors providing **sufficient guarantees** to implement appropriate technical and organizational measures that meet GDPR requirements and ensure protection of data subject's rights *(Article 28(1) GDPR)*.
  - How can processor demonstrate such guarantees?

- Processor shall immediately inform the controller if, in its opinion, an **instruction infringes the GDPR/other EU/Member State data protection provisions**.

- **Data processing agreement** → The processing shall be governed by a written contract binding on the processor. Needs to determine (*Article 28(3) GDPR*):
  - Subject-matter, duration, nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.
  - Processor obligations and responsibilities.

CONTROLLER-TO-PROCESSOR (CONT.)
(PROCESSOR-TO-SUB-PROCESSOR)

Processor's obligations and responsibilities that should be specified in the data processing agreement:
Process personal data only on **documented** **instructions from the controller** (including regarding transfers of personal data to a third country/an international organisation, unless required to do so by law)
Ensure that persons authorised to process the personal data are bound by a **confidentiality obligation** (subject to commitment/statutory obligation)
Implement appropriate **technical and organisational measures** to ensure a level of security appropriate to the risk
Assist the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the **data subject's rights**
Assist the controller with the **data breach notification** requirements
Assist the controller with **data protection impact assessment** *['DPIA']* requirements
At the choice of the controller, **delete or return all the personal data** to the controller after the end of the provision of the services, and to delete existing copies, unless otherwise required by EU/Member State laws
Make available to the controller all **information necessary to demonstrate compliance** with the data processing agreement
Allow for and contribute to **audits, including inspections**, conducted by the controller or an auditor mandated by the controller
Engage a **sub-processor** only with the prior specific or general written **authorisation** of the data controller (in the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of sub-processors, giving the controller the opportunity to object to such changes)
Impose by way of contract the **same obligations** as above in case the processor engages a **sub-processor**

JOINT CONTROLLERS

- *"shall in a transparent manner **determine their respective responsibilities** for compliance with the obligations under [the GDPR], in particular as regards"*:
  - Exercising of the rights of the data subject;
  - Transparency obligations;
- **Other obligations/measures** recommended by the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR:
  - Implementation of general data protection principles
  - Legal basis of the processing
  - Security measures
  - Personal data breach notifications
  - DPIAs
  - Use of processors
  - International data transfers
  - Organisation of contact with data subjects and supervisory authorities
- **Form of the arrangement** – not specified
  - Make the essence of the arrangement available to data subjects – not specified how
- Joint controllers may decide to designate a **contact point** for data subjects.
- **Data subjects may exercise their rights in respect of and against each of the joint controllers**

CONTROLLER-TO-CONTROLLER

- No strict contractual requirement

- Consider essential contractual guarantees
  - Establish roles
  - Establish separate responsibilities
  - Consider cooperation obligations
  - Establish clear separate liability obligations

! International data transfers requirements apply nevertheless

THANK YOU!

QUESTIONS?

MATUS HUBA
Data Privacy Advisor
Tel +32 492252754 | **Email** mhuba@mwe.com
McDermott Will & Emery Belgium LLP
Avenue des Nerviens 9-31
1040 Brussels, Belgium