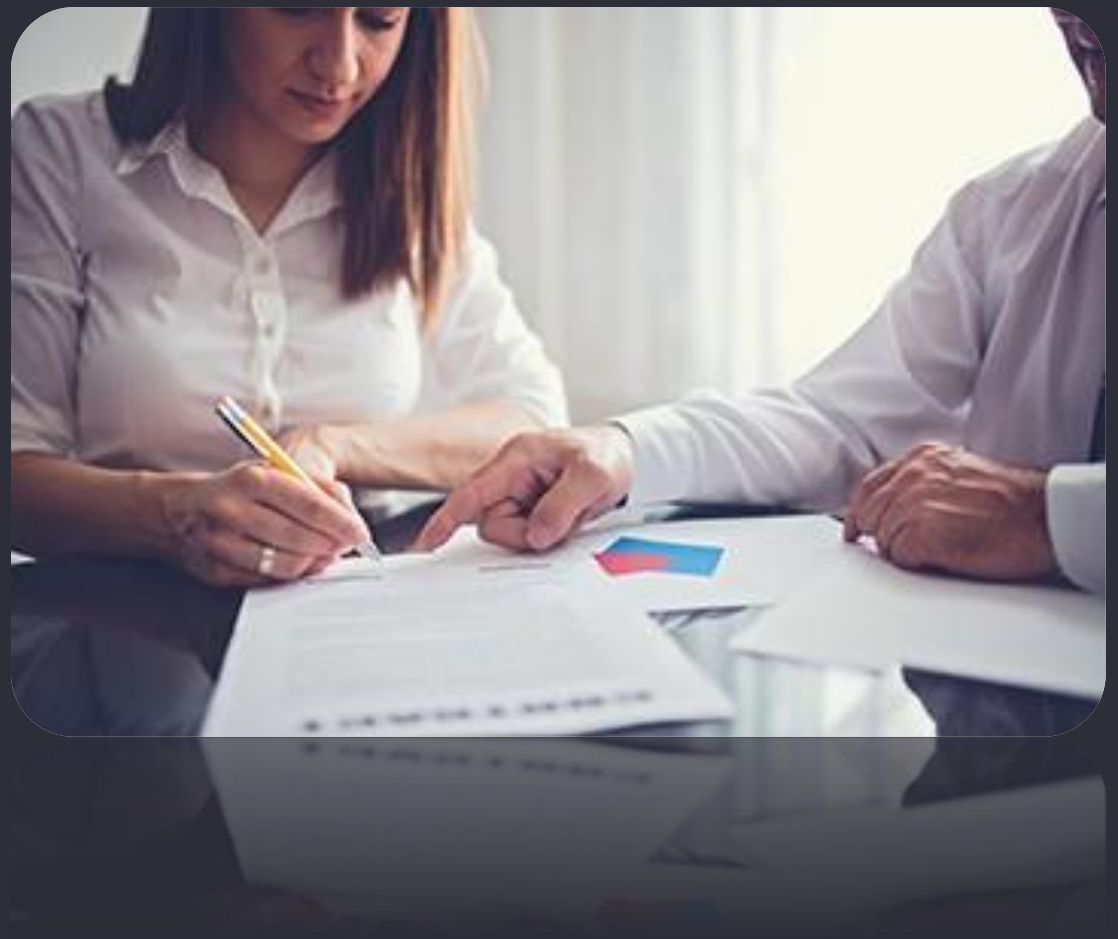
Module 2

The new developments in the roles and responsibilities of the data controllers and data processors



Written by

Irina Yaneva
Manager, EY

The concept of a “controller”

1. A data controller is the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.

2. The key role of a controller is to determine the purposes for which personal data is being collected, stored, used, altered and disclosed

3. A data controller may be a legal or a natural person. Despite the broad nature of the definition of who may be a data controller, preference should be given to consider the controller to be the company or body as such rather than an individual appointed by the company or body.

4. The joint controllers must determine their respective responsibilities for compliance with the GDPR in a transparent manner. To further protect individuals, the joint controllers are required to make “the essence of the arrangement” available to the data subjects. The data subjects may exercise their rights under the GDPR in respect of and against each of the controllers.

5. A controller may delegate decisions about the technical and organizational aspects of the processing to the processor provided it reserves the most important determinations of purposes or means to itself.

Opinion 1/2010 & Guidelines 07/2020

Control stemming from explicit legal competence

Control stemming from implicit competence

Control stemming from factual influence

The concept of a “controller”/”joint controller”

Guidelines 07/2020

- Certain processing activities are naturally attached to the roles or activities of an entity (e.g. due to traditional roles of professional expertise) which entails responsibilities
- The processing refers to your relation with the data subjects as employees, customers, members etc

- Not necessary that the controller has access to the data processed
  Two parties one of whom does not have such access can be joint controllers
  CJEU, C-25/17, Jehovah’ Witnesses
- Two parties not having the same purpose for the processing can be joint controllers if the pursued purposes are closely linked/complementary
  CJEU, C-40/17, Fashion ID
  CJEU, C-210/16, Wirtschaftsakademie
- The mere existence of a mutual benefit
- Mere use of a common data processing system/infrastructure
- Mere successive processing of the same personal data in a chain of operations

- Terms of the contract may help BUT are not always decisive

The concept of a “processor”

01

The GDPR defines a processor as “a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller”.

02

The existence of a data processor depends upon a decision by the controller to delegate all or part of processing activity to an external organization or individual. The role of a processor stems from the organization’s concrete activities in a specific context.

03

A processor who goes beyond its mandate and decides on the purposes or the essential means of the processing shall be considered to be a controller in respect of that processing.

Guidelines 07/2020: can decide on “non-essential means”

04

The GDPR requires that a processor processes personal data only on the controller’s instructions and that a contract or a binding legal act regulating the relations between the controller and the processor be put in writing.

Best practices in negotiating the terms and conditions of controller-to-controller relations

- Contract or other legal act under EU or Member State law which shall be in writing, including in electronic form, and be binding;
- Determine the respective responsibilities with regard to:

- the exercise of data subjects' rights and duties to provide information;
- general data protection principles;
- legal basis;
- security measures;
- data protection impact assessments;
- use of processors;
- third country transfers;
- contacts with data subjects and supervisory authorities, incl. data breach notification obligation.

Best practices in negotiating the terms and conditions of controller-to-processor relations (1)

- **Contract or other legal act which shall be in writing, including in electronic form, and be binding.**

- **Do not merely restate GDPR provisions! You should agree upon and provide <u>detailed</u> information on:**

- the subject-matter, duration and nature of the processing;
- the type of personal data to be processed and the categories of data subjects;
- the rights and obligations of the controller (incl. to perform inspections and audits);

  Limitations to controller's audit rights within the agreement under Art.28 of the GDPR should not be imposed!

- the rights and obligations of the processor (incl. obligation to only process data on documented instructions by the controller, to ensure that only persons who have committed themselves to confidentiality will be authorized to process the personal data, to take appropriate technical and organizational measures);
- level of security required;

Best practices in negotiating the terms and conditions of controller-to-processor relations

- **Remember to specify:**

- how the processor shall assist the controller in fulfilling its GDPR obligations;
- specific timeframe to notify the controller about a data breach;
- for sub-processors - the choice between general and specific prior written authorizations;
- whether data transfers out of the EU/EEA are allowed or prohibited;
- ability to change choice on whether data managed by processors shall be deleted or returned.

- **Code of conduct.**

How to choose our data processor (1)

- **Only use processors who provide sufficient guarantees to implement appropriate technical and organizational measures.**

- **Elements to be taken into account in your risk assessment:**

- the processor's expert knowledge (e.g. technical expertise with regard to security measures and data breaches);
- the processor's reliability;
- the processor's resources;
- the processor's reputation on the market; and
- the processor's adherence to an approved code of conduct or certification mechanism.

20 May 2021: EDPB approved Codes of Conduct on cloud infrastructure service providers in Europe – already has subscribers

Not to be used in the context of international transfers of personal data

How to choose our data processor (2)

- **Require relevant documentation:**

- privacy policy
- terms of service,
- record of processing activities,
- management policy,
- information security policy,
- reports of external audits,
- recognized international certifications, like ISO 27000 series).

N.B.! The imbalance of power of a small data controller with respect to big service providers is not a justification for accepting GDPR terms!