Data Processing Mapping and Data Controllers & Data Processors Determination Roles and Responsibilities

Step 1: Identifying Personal Data and Mapping Personal Data Processing

Step 2: Use findings from your Processing Mapping to determine Controllership

Laure Méchineau-Phelan,
National HSE Research and Development

Step 1:
Identifying Personal Data

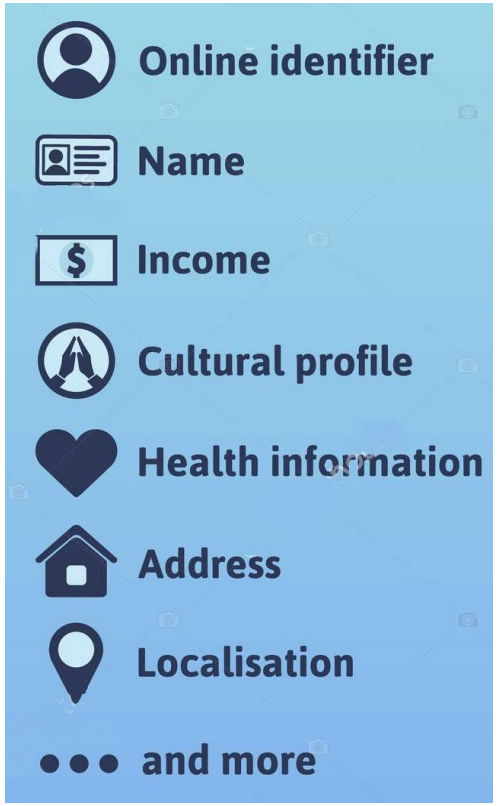
When designing your research project, or at the very latest before the start of your research project, you should identify what personal data will be processed as part of the project. The meaning of 'data processing' is addressed in Slide 4.

This exercise should also identify:

- Who will have access to the Personal Data and the security measures in place;
- What new Personal Data, or new processing, will be generated during the research project and factor these in the Personal Data Mapping exercise;
- The role of each entity involved in the processing

Information about the different types of Personal Data, and specific conditions attached to their processing is available at the Data Protection Commission Website

What is personal data?



Mapping Personal Data Processing

What should I focus on?

- To assess the role of each entity involved in the processing you must first identify all the activities that constitute personal data processing and its exact purpose.
- If multiple entities are involved, it is necessary to assess if the **purposes ('why') and essential means ("how')** are **determined** jointly, leading to joint controllership. **Determination** means 'decision-making power' AND "w**ho decides the processing should take place for a specific purpose**"
- Determination of Controllership is based on **(1) legal obligations** (*i.e. legal mandate to conduct certain processing)* and **(2) factual analysis. Data Processing Mapping** will help you in conducting your **factual analysis** and assessing the role and responsibilities of entities involved in the processing

Mapping Personal Data Processing

What Constitutes Personal Data Processing?

Any operation, or set of operations, performed on Personal Data

Including automated and non-automated processing

Including manual processing in structured filing systems

Data processing means anything you do with Personal Data including (but not limited to):

- Collection
- Consultation
- Copy
- Retrieval
- Organisation
- Recording
- Alignment or combination
- Pseudonymisation
- Structuring
- Adaptation or Alteration
- Use
- Disclosure by transmission
- Transfer
- Storage
- Analysis
- Archive
- Erasure/destruction
- Transcription

Mapping means to systematically describe the personal data processing activities

- Explain the processing step-by-step and distinguish between purposes
  (e.g. data collection/data analysis, now and for future uses)
- Start from the personal data you already have (if it applies)
- Continue with the personal data you will collect as part of the research
  What data, from Whom / Where, What do you do with it? Where do you keep it? Who will you share it with? etc…
  Any vulnerable group?
  What entity (data user) decides on means and purpose in the above processing - solely or jointly?
- Explain interactions with other processes
  (e.g. secondary use of data, re-use of data in other process)
- Detail IT, security infrastructure
- Review the entire Description assessing 'How this will affect data subjects'

Determines the Roles of each Data User involved in the Processing
(Controllers, Joint-Controllers, Separate Controllers, Processors)

Determines the Obligations for Data Users as per GDPR

Mapping Personal Data Processing

Other questions that may help you to map the data processing for your research project:

- Think about what you need to do and limit yourself to that
- What exactly do we want to do and why?
- Why are we allowed to do it?
- What data do we need to do it?
- For how long do we need to the data?
- Who needs to have access to the data?
- How do we make sure it is not used otherwise?
- How do we tell people about it and give them access to their data?
- How do we document all this and steps taken for accountability?
- Need guidance? Talk to your DPO

Step 2:
Use findings from your Processing Mapping to determine Controllership

Option 1:

Use the HSE Annotated EDPB Flowchart* for applying the concepts of controller, processor and joint controllers in practice

(Go to slide7)

** Adopted after Public Consultation*

https://edpb.europa.eu/edpb_en

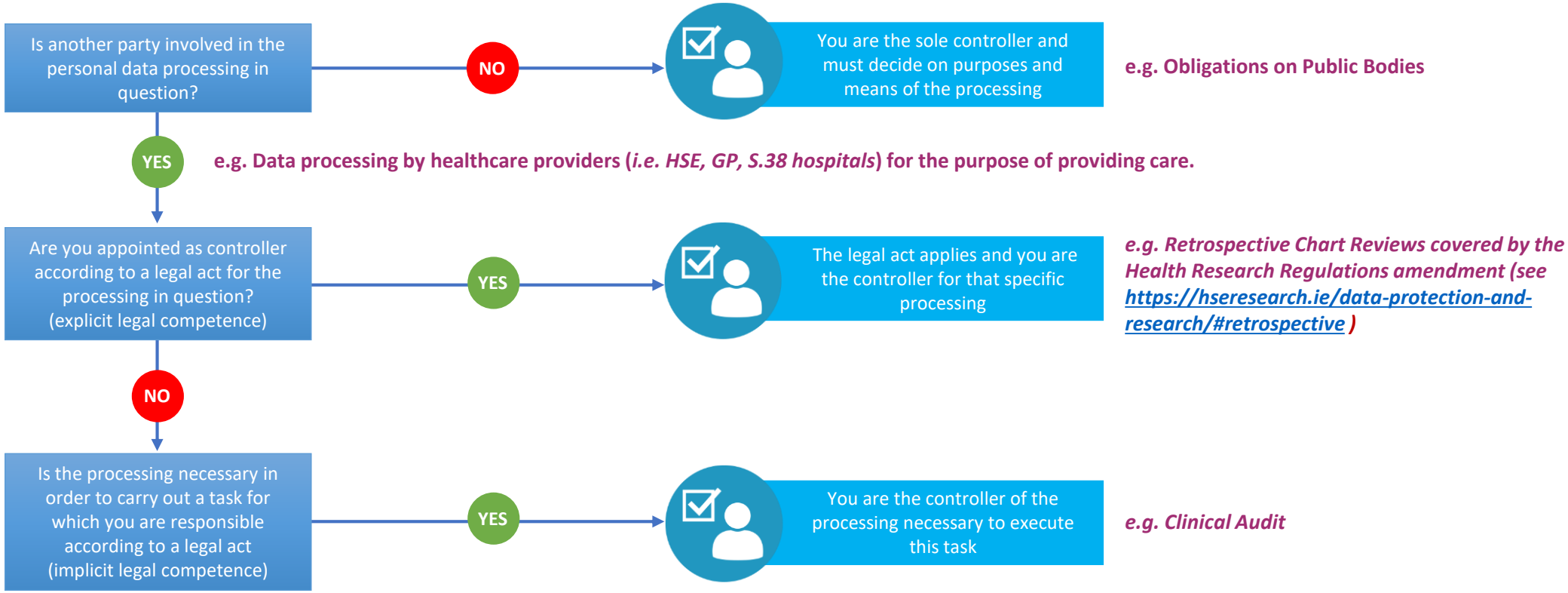
Option 2:

Use the HSE Annotated EDPS Flowchart for applying the concepts of controller, processor and joint controllers in practice

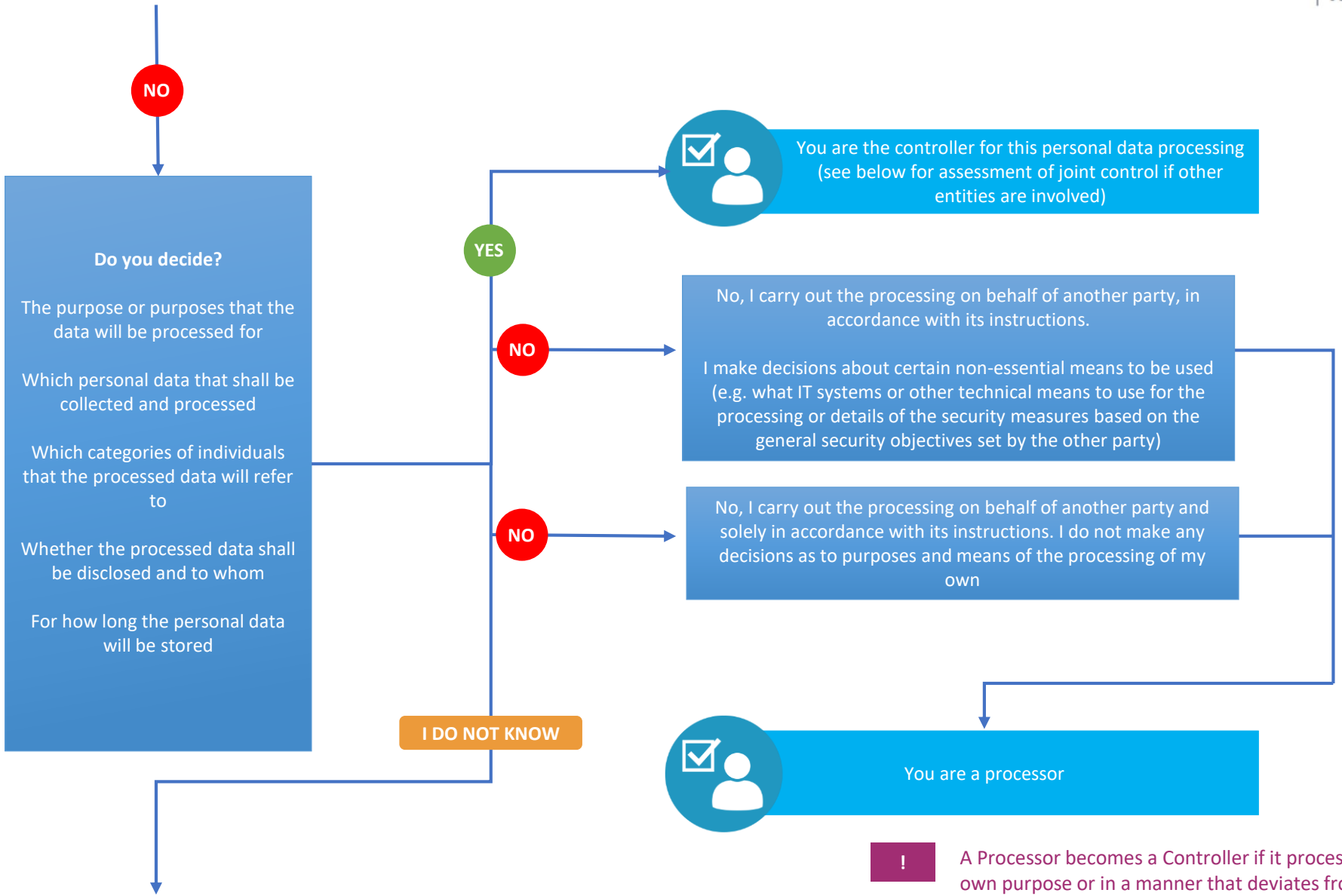
(Go to Slide 11)

https://edps.europa.eu/_en

Step 2 Option 1:
Use the HSE Annotated EDPB Flowchart for applying the concepts of controller, processor and joint controllers in practice



Ctnd next slide



! A Processor becomes a Controller if it processes Personal Data for its own purpose or in a manner that deviates from the Controller's instruction

Ctnd next slide

I DO NOT KNOW

I don't know who decides on the purposes or means of the processing:

The following factors may help to determine the appropriate qualification of the roles:

Factors that indicate that you are the controller

You obtain a benefit from, or have an interest in, the processing *(other than the mere payment for services received from another controller)*

You make decisions about the individuals concerned as part of or as a result of the processing *(e.g. the data subjects are your employees)*

The processing activities can be considered as naturally attached to the role or activities of your entity *(e.g. due to traditional rules of professional expertise)* which entails responsibilities from a data protection point of view

The processing refers to your relation with the data subjects as employees, customers, members *etc…*

You have complete autonomy in deciding how the personal data is processed

You have entrusted the processing of personal data to an external organisation to process the personal data on your behalf

Factors that indicate that you are the processor

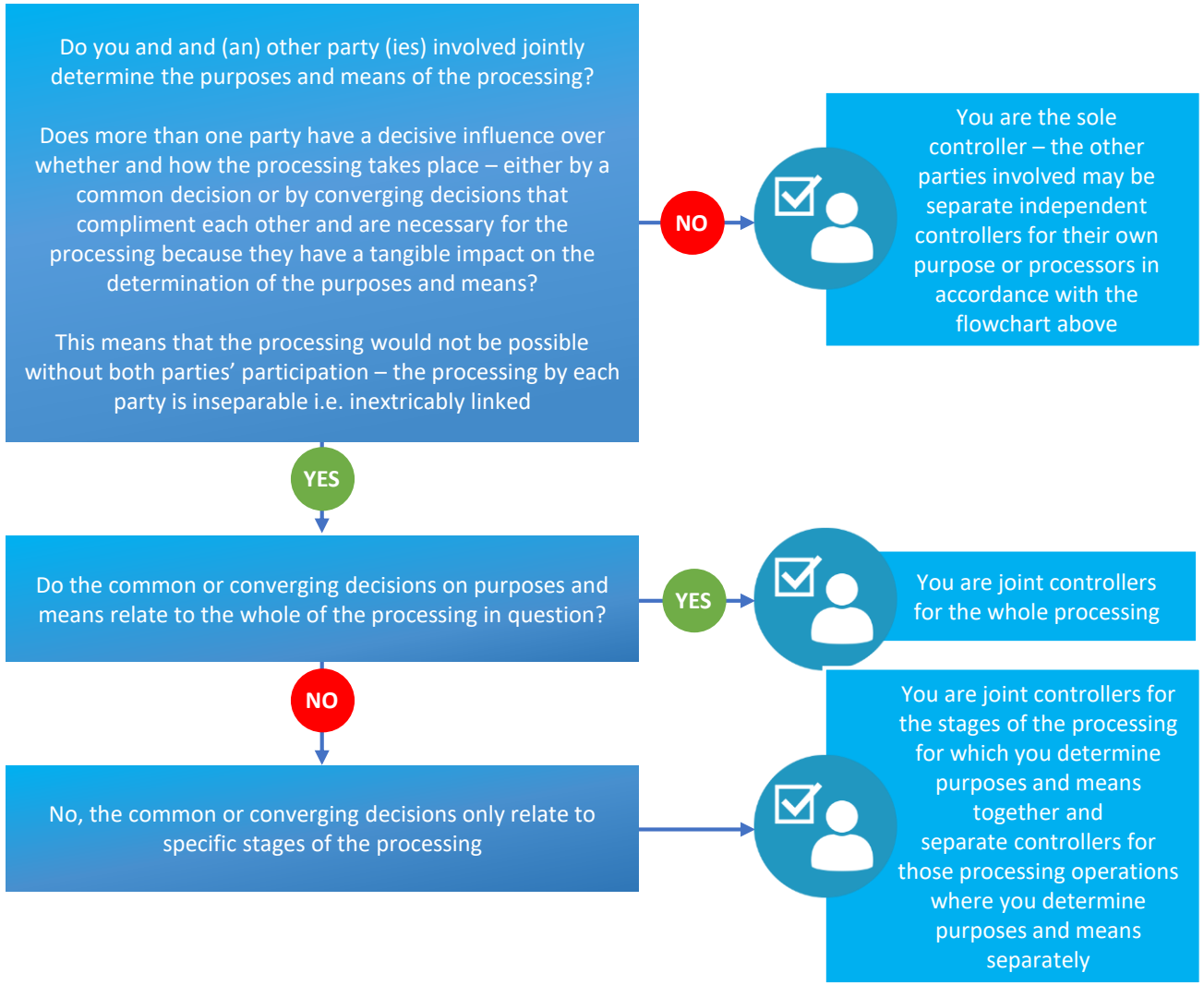
You *process* the personal data for another party's purposes and in accordance with its documented instructions – you do not have a purpose of your own for the processing

Another party monitors your processing activities in order to ensure that you comply with instructions and terms of contract

You do not pursue your own purpose in the processing other than your own business interest to provide services

You have been engaged for carrying out specific processing activities by someone who in turn has been engaged to process data on another party's behalf and on this party's documented instructions (you are a sub processor)

Joint controllership – If you are the controller and other parties are involved in the personal data processing:



Example: Clinical trials

A health care provider (the investigator) and a university (the sponsor) decide to launch together a clinical trial with the same purpose. They collaborate together to the drafting of the study protocol *(i.e. purpose, methodology/design of the study, data to be collected, subject exclusion/inclusion criteria, database reuse (where relevant) etc.).* They may be considered as joint controllers for this clinical trial as they jointly determine and agree on the same purpose and the essential means of the processing.

The collection of personal data from the medical record of the patient for the purpose of research is to be distinguished from the storage and use of the same data for the purpose of patient care, for which the health care provider remains the controller.

In the event that the investigator does not participate to the drafting of the *protocol (he just accepts the protocol already elaborated by the sponsor),* and the protocol is only designed by the sponsor, the investigator should be considered as a processor and the sponsor as the controller for this clinical trial.

Example: Research project by institutes

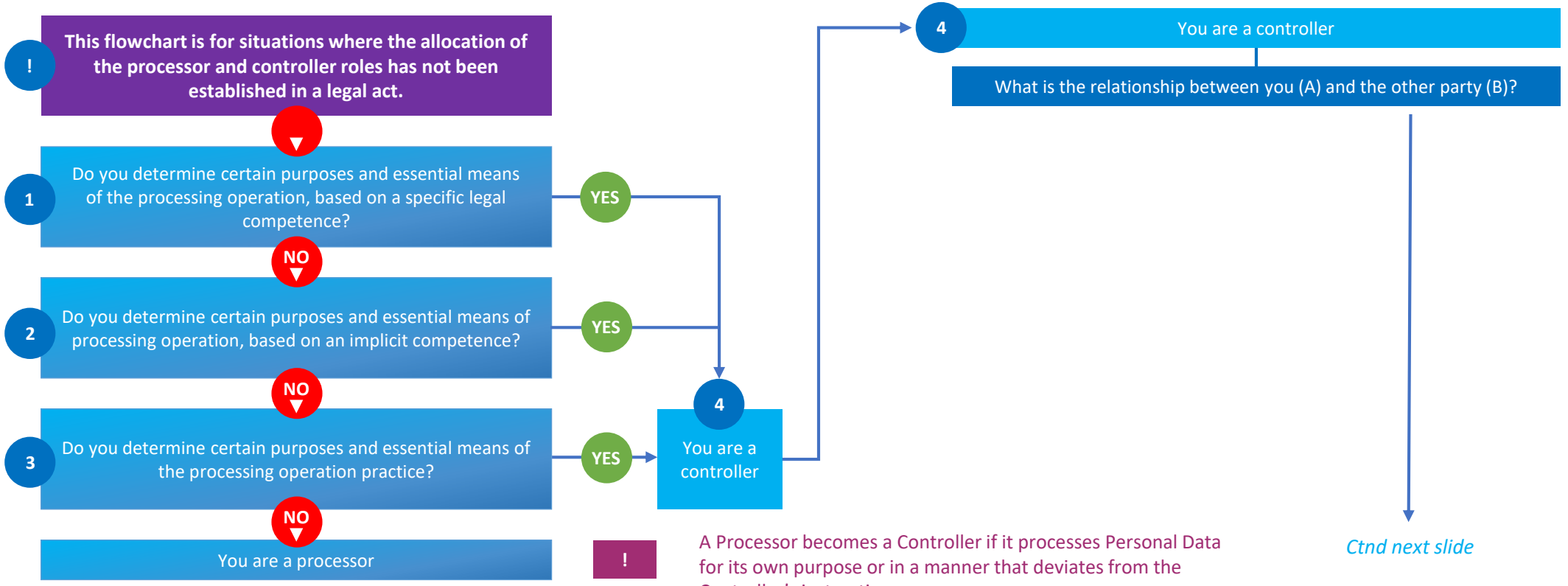
Several research institutes decide to participate in a specific joint research project and to use to that end the existing platform of one of the institutes involved in the project. Each institute feeds personal data it holds into the platform for the purpose of the joint research and uses the data provided by others through the platform for carrying out the research. In this case, all institutes qualify as joint controllers for the personal data processing that is done by storing and disclosing information from this platform since they have decided together the purpose of the processing and the means to be used (the existing platform). Each of the institutes however is a separate controller for any other processing that may be carried out outside the platform for their respective purposes.

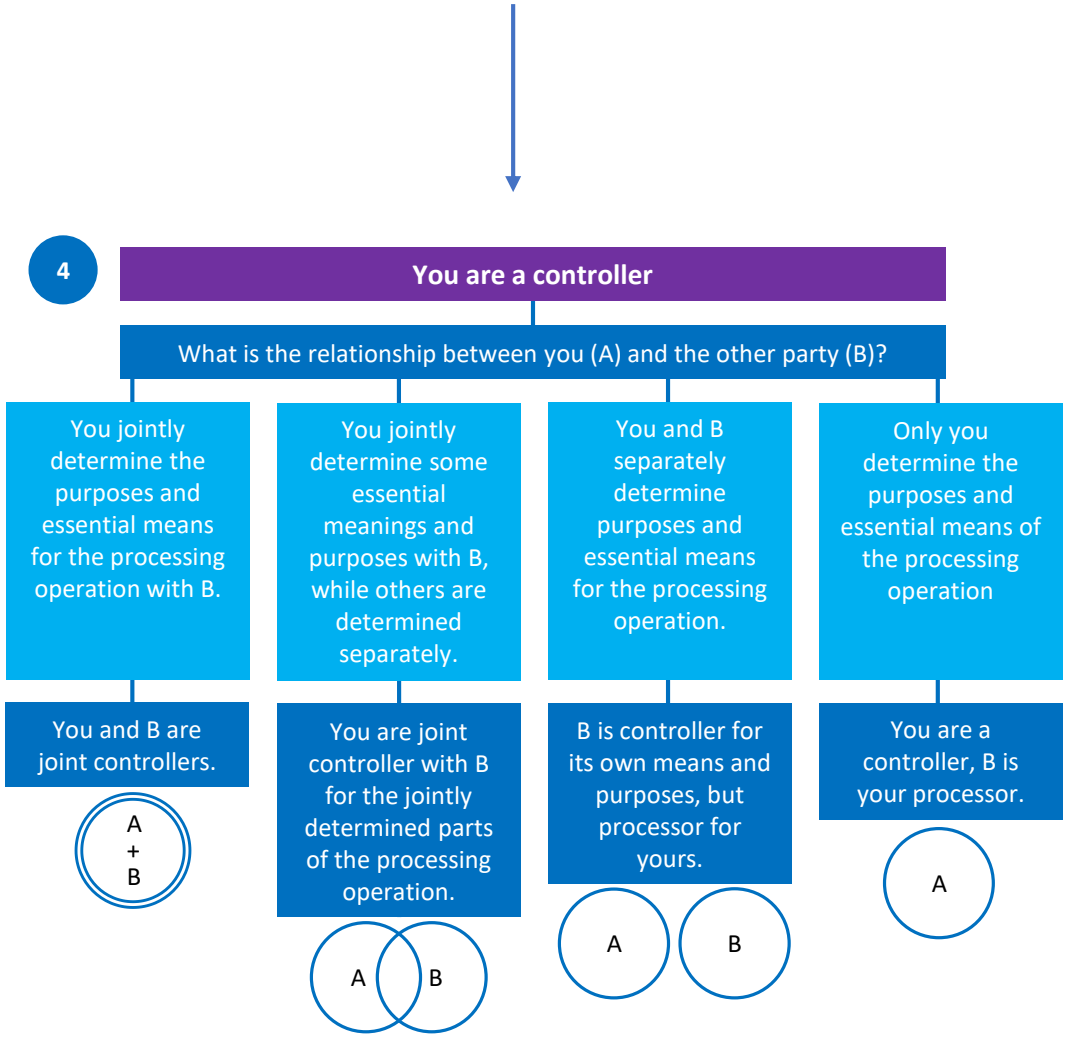
Step 2 Option 2:

Use the EDPS Flowchart for applying the concepts of controller, processor and joint controllers in practice

https://edps.europa.eu/_en

Flowchart for EUIs. You are involved in a processing operation with one or more third parties: are you a processor, a controller, or a joint a controller?





Example: Multiple separate controllers

Multiple controllership applies to situations where various actors successively process the same personal data in a chain of operations and each of these actors have an independent purpose and independent means in their part of the chain.

In the absence of joint participation in the determination of the purposes and means of the same processing operation or set of operations, joint controllership has to be excluded and the various actors must be regarded as successive independent separate controllers.

Example: Statistical analysis for a task of public interest

A public authority (Authority A) has the legal task of making relevant analysis and statistics on how the country's employment rate develops. To do that, many other public entities are legally bound to disclose specific data to Authority A. Authority A decides to use a specific system to process the data, including collection. This also means that the other units are obligated to use the system for their disclosure of data. In this case, without prejudice to any attribution of roles by law, Authority A will be the only controller of the processing for the purpose of analysis and statistics of the employment rate processed in the system, because Authority A determines the purpose for the processing, and has decided how the processing will be organised. Of course, the other public entities, as controllers for their own processing activities, are responsible for ensuring the accuracy of the data they previously processed, which they then disclose to Authority A

Additional Support to Determine Controllership

Research & Development
Taighde & Forbairt

EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR
https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf

Useful guidance is provided by the ICO, including on the distinction between a controller and a processor.

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/

Table of Conceptual Distinctions between a Controller and a Processor based on ICO Guidance:

Controllership	Roles a Processor might play in practice
To determine whether you are the data controller, you need to ascertain which organisation decides: • To collect the personal data in the first place and the legal basis to do so • Which items of personal data to collect (i.e. the content of the data) • The purpose or purposes the data is to be used for • Which individuals to collect data about • Whether to disclose the data, and if so, who to • Whether subject's access and other individual rights apply (i.e. the application of exemptions) • How long to retain the data or whether to make non-routine amendments to the data **These decisions can only be taken by the data controller as part of its overall control of the data processing**	Within the terms of the agreement with the Data Controller, a Data Processor may be in the position to decide: • What IT systems or other methods to use to collect personal data • How to store personal data • The detail of the security surrounding the personal data • The means used to transfer the personal data about certain individuals • The method for ensuring a retention schedule is adhered to • The means used to delete or dispose of the data