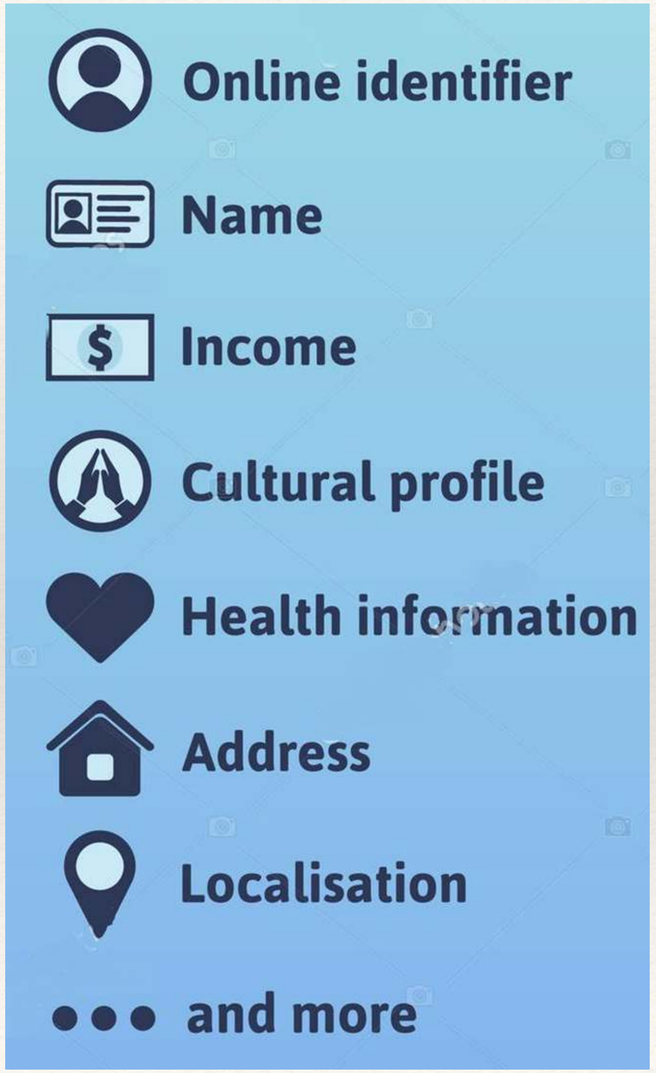
Identifying the Personal Data

Research & Development
Taighde & Forbairt

At an early point in the research project, you should identify how personal information is intended to be collected, stored, used and deleted as part of the project. This exercise should also identify:

- What kinds of information will be used as part of the project and
- Who will have access to the information
- Will any new personal information that will be generated by the research project and include it the mapping exercise

What is personal data?



By Laura Phelan, HSE R&D

Mapping the Personal Data Processing

Research & Development
Taighde & Forbairt

This mapping exercise should be documented using whatever means are most suitable for the project:

1. Where is Data Collected?
   Researchers need to identify where the personal data that they will process is coming from into their organisation. Researchers need to understand what information they are getting from which sources, and what their obligations with respect to that data collection are under the GDPR (General Data Protection Regulation (EU) 2016/679).

2. What Data is Collected?
   It is important for researchers to have a full understanding of all the personal data that they possess about individuals, e.g. given in Article 4 of GDPR include a name, identification number, location data, online identifier, or one or more physical, physiological, genetic, mental, economic, cultural or social identity factors specific to a natural person.

3. Where is the data stored? What is the format of the data?
   Researchers need to know where that data is located and what format it is held in (i.e electronically, paper records, etc). Even electronic records need in-depth examination since they may be stored in the cloud, local servers, local computers or even the equipment of third-party vendors.

4. Where does the data go?
   Researchers need to know where their data is going, both internally within the organisation, and/or externally to third-parties. It is also important to pay attention to whether data is crossing borders, when it is involved in a transfer to/from a processor or even when it is being moved for internal purposes, due to the special implications of personal data being transferred across the boundaries of the EU to other countries.

5. What is the data used for?
   Researchers need to know about their processing activities both to be able to provide accurate disclosures to research participants as well as to be able to fulfil Article 30 documentation requirements.

6. How long is the data retained?
   Although most data flow mapping is focused on its collection and sharing, a comprehensive look may include when data is being deleted by an organisation as well.

By Laura Phelan, HSE R&D

- Assess the role of each entity involved in the processing you must first identify the specific 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**"
- Controllership is a **functional concept:** 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

What Constitutes Personal Data Processing?

- Any operation or Set of operations Performed on Personal Data
- Includes automated and non-automated processing
- Incudes 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 combina
- Pseudonymisation
- Structuring
- Adaptation or Alteration
- Use
- Disclosure by transmission
- Transfer
- Storage
- Analysis
- Archive
- Erasure/destruction
- Transcription

PROCESSING MAPPING: CREATE A SYSTEMATIC DESCRIPTION OF THE PROCESSING

- Explain the processing step-by-step and distinguish between purpose (e.g. data collection/data analysis, now and for future uses)
- Start from the Personal data you already have if it applies
- Add the Personal Data you collect
  - *WHAT, from WHOM / WHERE, What do you do with it? Where do you keep it? To Whom do you give it*
  - *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'
- Ensure lawful processing

Other questions to consider that may help you:

- Think about what you need to do and limit yourselves to it.
- What exactly do we want to do and why?
- Why are we allowed to do it?
- What data do we need to do it and for how long?
- 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?
- Want to know more? Need guidance?
  - Talk to your Data Protection Officer
  - Document each step for accountability

By Laura Phelan, HSE R&D

Research & Development
Taighde & Forbairt

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

Option 1:

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

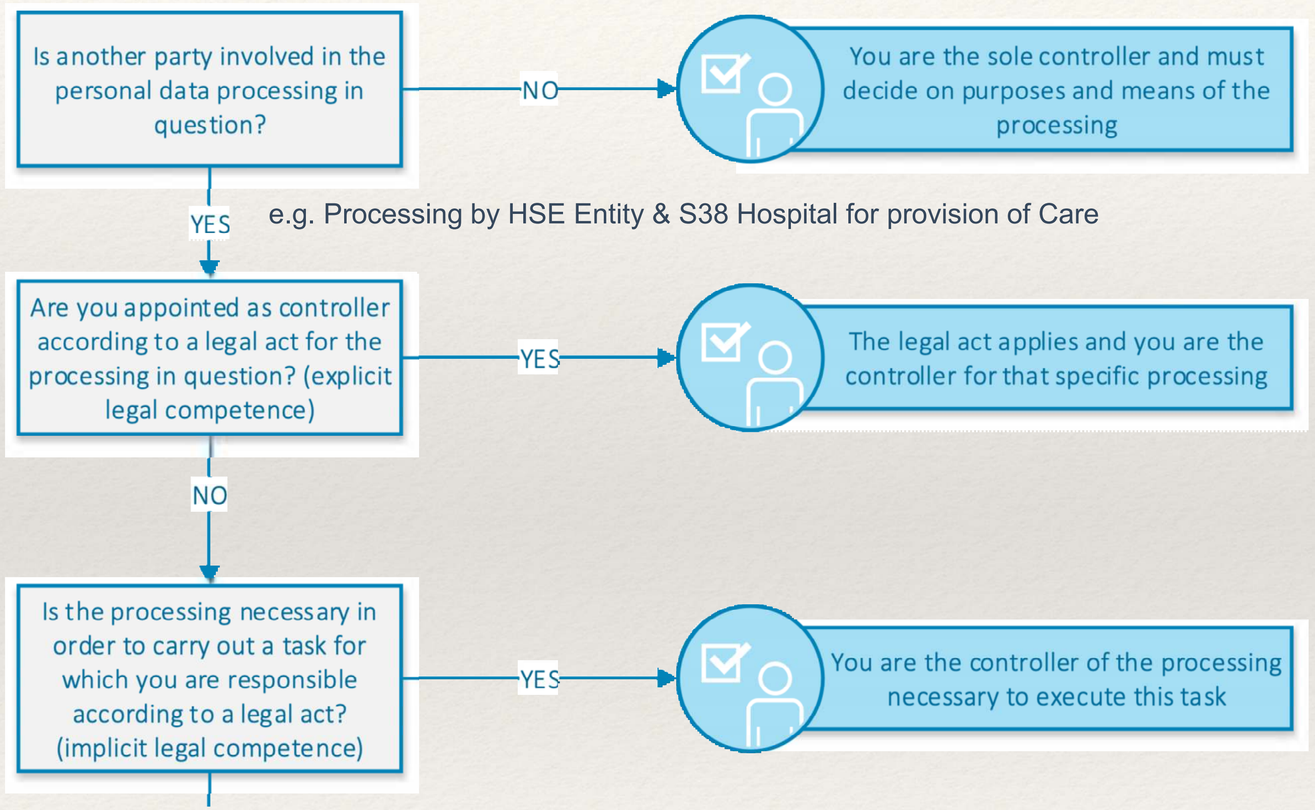
edpb
European Data Protection Board

https://edpb.europa.eu/edpb_en

By Laura Phelan, HSE R&D

Research & Development
Taighde & Forbairt

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



e.g. Obligations on Public Bodies

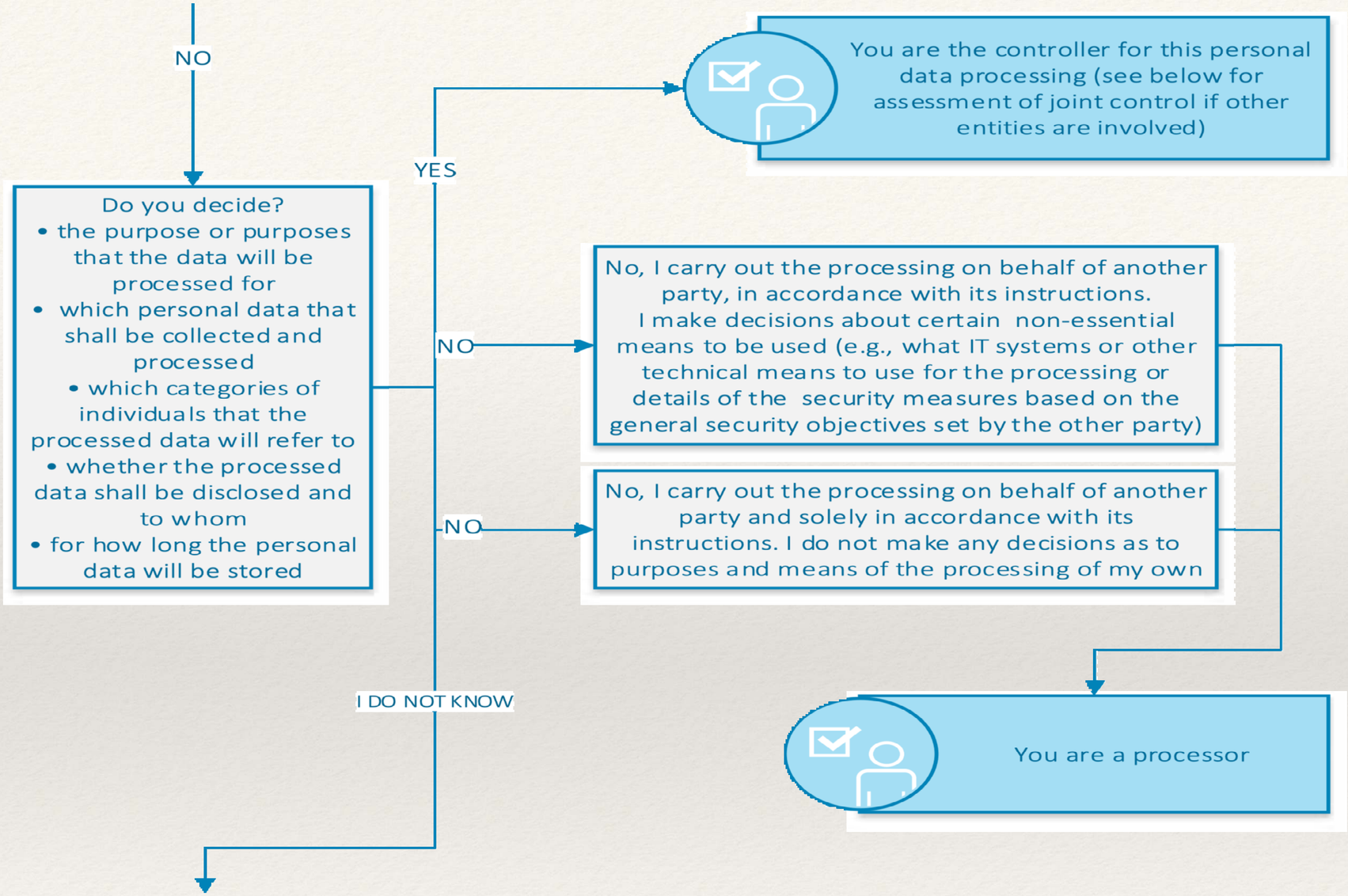
e.g. Processing by HSE Entity & S38 Hospital for provision of Care

e.g. HRR Amendments on 'Consent Exemption for retrospective chart reviews and how they apply

e.g. Clinical Audit

Ctnd next slide

By Laura Phelan, HSE R&D


NO
Do you decide?
• the purpose or purposes that the data will be processed for
• which personal data that shall be collected and processed
• which categories of individuals that the processed data will refer to
• whether the processed data shall be disclosed and to whom
• for how long the personal data will be stored
YES
You are the controller for this personal data processing (see below for assessment of joint control if other entities are involved)
NO
No, I carry out the processing on behalf of another party, in accordance with its instructions. I make decisions about certain non-essential means to be used (e.g., what IT systems or other technical means to use for the processing or details of the security measures based on the general security objectives set by the other party)
NO
No, I carry out the processing on behalf of another party and solely in accordance with its instructions. I do not make any decisions as to purposes and means of the processing of my own
I DO NOT KNOW
You are a processor

Research & Development
Taighde & Forbairt

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

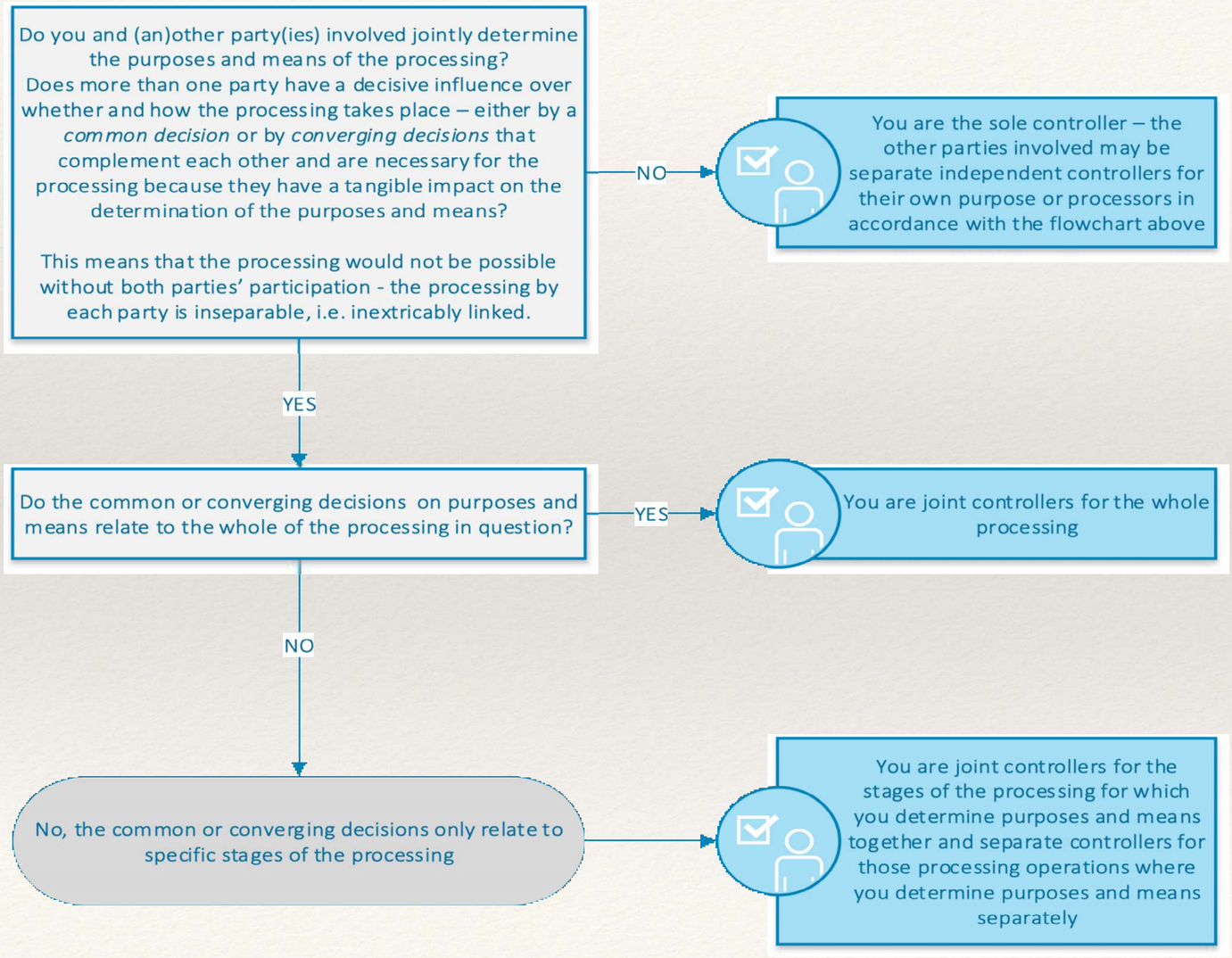
- You obtain a benefit from, or have an interest in, the processing (other than the mere payment for services received from another controller)
- You make decisions about the individuals concerned as part of or as a result of the processing (e.g. the data subjects are your employees)
- The processing activities can be considered as naturally attached to the role or activities of your entity (e.g. due to traditional roles or 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)

Updated by Dr L Phelan, HSE R&D

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.

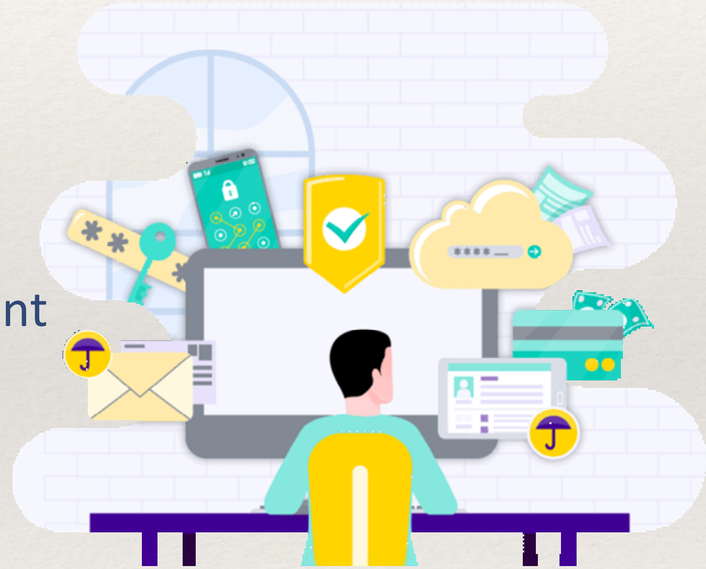
Several research institutes decide to participate in a specific joint research project and to use to that end the existing platform of one of the institutes involved in the project. Each institute feeds personal data it holds into the platform for the purpose of the joint research and uses the data provided 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.

Research & Development
Taighde & Forbairt

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

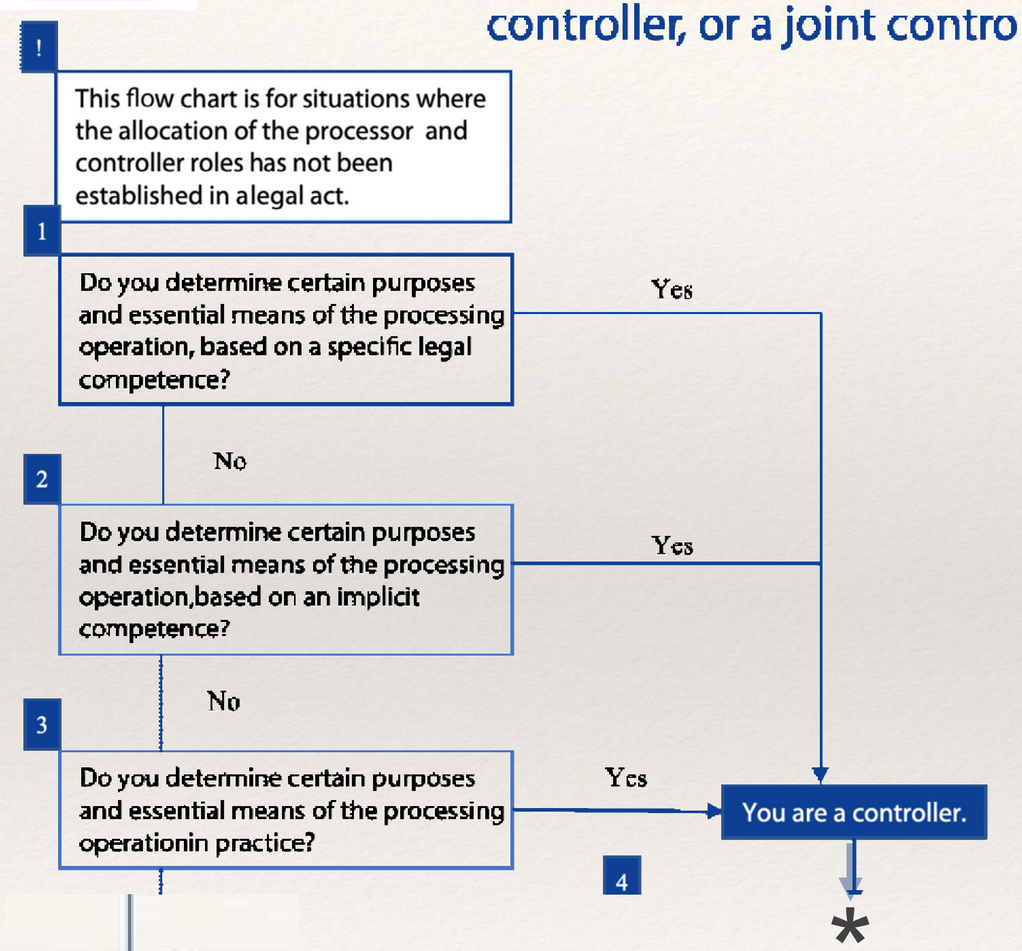
Option 2:

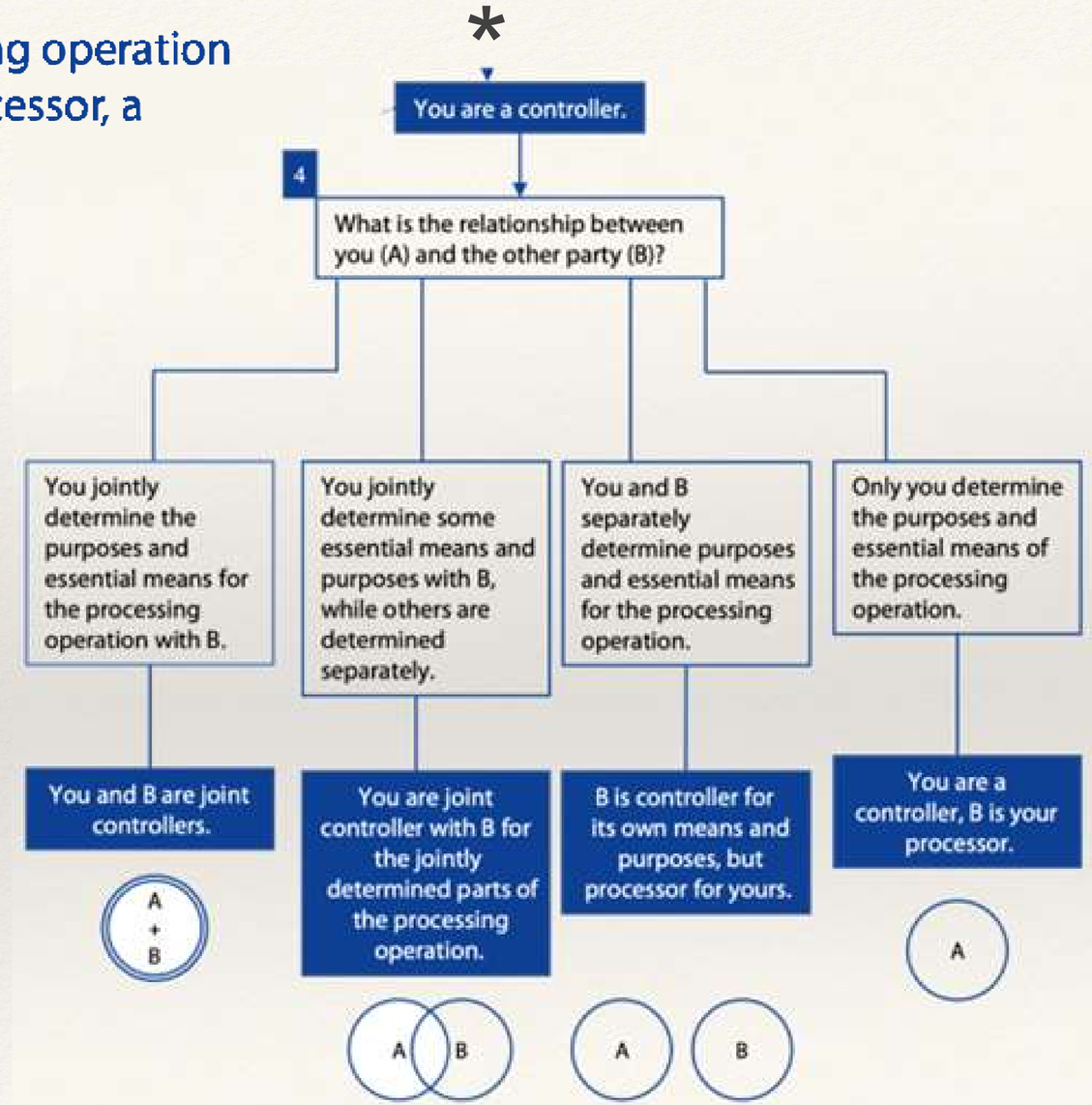
Use the EDS Flowchart for applying the concepts of controller, processor and joint controllers in practice



By Laura Phelan, HSE R&D

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 controller?



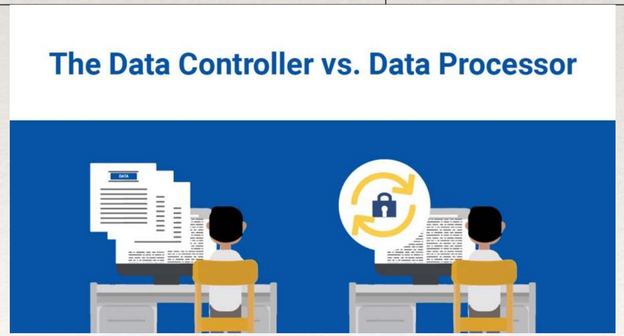


By Laura Phelan, HSE R&D

Additional Support to determine Controllership: ICO Guidelines

Research & Development
Taighde & Forbairt

Controller	Processor
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) and • How long to retain the data or whether to make non – routine amendments to the data. **This are all the decisions that can only be taken by the data controller as part of its overall control of the data processing operation**	Within the terms of the agreement with the Data Controller, a Data Processor maybe 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



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

Updated by Dr L Phelan, HSE R&D

For Information, please see HSE Research and Development

https://hseresearch.ie/