# A black background with white text Description automatically generated

# The Concept of Data Controller and Data Processor

As a health researcher engaging on a new research project one of the first things you must do is determine the data protection role for each organisation involved. If each organisation’s role and the nature of the data protection relationship is not clarified at an early stage, this can cause difficulties later. You need to understand these concepts to complete your ethics application and the research DPIA.

The organisation’s role in relation to personal data will determine, amongst other things:

obligations under Data Protection laws;

the legal provisions required in the contract between the parties;

and any liability for fines and damages arising from a personal data breach.

In general, the organisation(s) that design(s) the project will be the Controller/Joint Controller. Organisation(s) that follow the instructions of the designing organisation will be a Data Processor.

Determining the appropriate data protection role is not always straightforward. You may need to consult with the University’s Data Protection Officer (DPO).

### Data Controller

|  |
| --- |
| [the **natural or legal person, public authority, agency or other body** which, **alone** or **jointly** with others, **determines** the **purposes and means** ofthe **processing of personal data**](https://gdpr-info.eu/art-4-gdpr/)**.** |

There are five key parts to this [definition](https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en):

1. The Controller is usually an organisation, and not an individual within the organisation (such as the Principal Investigator, or an employee).
2. The Controller must have genuine influence over the processing of personal data. In other words, the Controller must have decision-making power.
3. The Controller determines the purposes and means of the processing, i.e. the why and how of the processing:

* articulating the research question to be answered;
* the methods to answer the research question;
* the inclusion criteria, deciding the categories of research participants (data subjects);
* the types of data to be processed to achieve the purpose of the project;
* for how long the personal data will be stored;
* who will have access to the data.

1. The Controller can act alone or jointly with others (see Joint Controller section below).
2. The Controller’s decision-making power must relate to the processing of personal data. An organisation that provides funding but is not involved in determining the purpose and the means of the processing in any way would not be a Controller.

### Joint Controller

|  |
| --- |
| The overarching criterion for Joint Controllership to exist is the **joint participation** of two or more entities in the **determination of the purposes and means** of a processing operation. |

In health research, normally organisations that work collaboratively to design and conduct a project will be Joint Controllers. The five criteria outlined above also apply to Joint Controllers.

|  |
| --- |
| **Example:** Two consultants working in two different hospitals design a project together. It is likely that the Hospitals would be Joint Controllers. |

### Data Processor

|  |
| --- |
| [a natural or legal person, public authority, agency or other body which **processes personal data on behalf of the Controller**](https://gdpr-info.eu/art-4-gdpr/)**.** |

The Processor processes personal data only on behalf of the Controller. The Processor is normally a third party external to the Controller. Sometimes, a Controller may need to sub-contract some or all of the processing activities to a third party. That third party would generally be designated as a Processor.

Two basic conditions for qualifying as a Processor exist:

1. That it is a separate legal entity to the Controller and
2. That it processes personal data on the Controller’s behalf.

|  |
| --- |
| **Example**: A hospital designs a research project. It employs a private laboratory to carry out an analysis of blood samples. The laboratory uses its own expertise to decide on the appropriate method of analysis. The hospital is the Controller, and the laboratory is the Processor. |

To facilitate such an arrangement, the Processor is obliged to follow the instructions of the Controller which must be set out in a legally binding contract, a Data Processing Agreement (DPA), between the Controller and the Processor. However, practical or technical aspects of implementation of the instructions can be left to the Processor. If the Processor goes beyond the Controller’s instructions, it is at risk of breaching the DPA and becoming a Controller.

### Common Mistakes

1. It is commonly misunderstood that the organisation that possesses or handles the personal data must be the only Controller. This is not always the case. [Sometimes, an organisation that does not have access to the data can be the Controller](https://curia.europa.eu/juris/document/document.jsf;jsessionid=F9C9FA3B6155AB5A7E70C9A0EF2B9822?text=&docid=202543&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1951510). Possession of the data does not equate to Controllership.

|  |
| --- |
| **Example**: A sponsor and a hospital jointly design a project. The hospital recruits participants and collects personal data. Hospital staff pseudonymise the data before sharing the pseudonymised data with the sponsor. Even though the sponsor never has access to identifiable personal data, the sponsor is a Controller because it has determined the purpose and the means of the project. |

1. Researchers often identify an individual, such as the Principal Investigator (PI), as the Data Controller or Processor. It is rare that individuals will be Controllers or Processors in the context of health research. Normally an organisation that employs the PI is the Controller or the Processor. Employees generally act on behalf of the organisation that is the Controller or Processor. The PI will still be responsible for day-to-day compliance with data protection obligations arising from the research project.

### Dual Affiliation

It is common for a researcher to be an employee of a University and a hospital. It is important to separate these roles when determining the appropriate data protection role.

|  |
| --- |
| **Example**: A University professor, who is also a hospital consultant, designs a project as part of their role in the University. Having designed the project, the professor initiates the project in several different hospital sites including her own hospital. The study sites have no determinative influence over the design of the project. The University is the Controller, and the study site is a Processor. The professor will not be actively participating in the conduct of the project at their hospital site. The professor will be involved in the analysis of pseudonymised data obtained from the study sites. In this scenario, the professor/consultant is acting on behalf of the University as the Controller. |

### Clinical Trials

In the context of clinical trials, [the EDPB has provided clear guidance on the nature of the relationship between the Sponsor and the Study site](https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en). There are two examples provided:

1. **The Sponsor and the Healthcare Provider are Joint Controllers**

|  |
| --- |
| **Example**: A healthcare provider (the investigator) and a University (the sponsor) decide to launch together a clinical trial with the same purpose. They collaborate together on the drafting of the study protocol, i.e. purpose, methodology/design of the study, data to be collected, participant exclusion/inclusion criteria, database reuse (where relevant), etc. The healthcare provider and University will be considered Joint Controllers for this clinical trial as they jointly determine and agree on the purpose and the 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 healthcare provider remains the Controller. |

1. **The Sponsor is the Controller, and the Healthcare provider is a Processor**

|  |
| --- |
| **Example**: In the event that the investigator does not participate in the drafting of the protocol (they just accept the protocol already created 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. |

## Additional Resources

European Data Protection Board (EDPB) [*Guidelines 07/2020 on the concepts of controller and processor in the GDPR*](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en)

Regina Becker, et. al., [*Applying GDPR roles and responsibilities to scientific data sharing*](https://doi.org/10.1093/idpl/ipac011), International Data Privacy Law, Volume 12, Issue 3, August 2022, Pages 207–219

Data Protection Commission (DPC) [Guidance: A Practical Guide to Data Controller to Data Processor Contracts under GDPR](https://www.dataprotection.ie/en/organisations/know-your-obligations/controller-and-processor-relationships)

## Flowchart

