Health Research Data Protection Network (HRDPN)

PRACTICAL GUIDE ON DATA PROTECTION FOR HEALTH RESEARCHERS

Background and purpose of this guide:

The Health Research Data Protection Network (HRDPN) is a Network of members involved in data protection compliance from Universities, the HSE, Hospitals, NCTO, and not-for-profit Research Organisation/Networks. The HRDPN was established in 2018 to promote consistency in Data Protection approaches across the Irish Health Research sector through the sharing of experiences, information and resources including systems, procedures, processes and template agreements.

This Practical Guide ("the Guide") is intended to provide general information and understanding of the law to researches to help them understand with plain non-legal language their and their organisation's role with regard to Data Protection, as well as related responsibilities and requirements.

Authors and Acknowledgments

This Practical Guide on data Protection for Health Research (the 'Guide') was drafted by the Irish Health Research Data Protection Network (HRDPN) in consultation with the DPC.

The HRDPN thank the DPC and all investigators and researchers of its Network for their support.

Disclaimer

The views expressed in this Guide do not represent an official position of the organisations represented by members of the HRDPN and the DPC, and content of this Guide does not bind such organisations and the DPC in the exercise of their respective competences.

The Guide is intended to provide general information and understanding of the law. It should not be considered legal advice, nor used as a substitute for seeking qualified legal advice.

For legal definitions or further assistance on Data Protection, researchers shall consult with their Data Protection Officer (DPO).

Scope

The Scope of this document is as follows:

1. Clarify GDPR definitions of Personal Data (Data), Data Processing, Data Controller (Controller), Joint Data Controllers (Joint Controller), Separate Data Controllers (Separate Controller), and Data Processor (Processor).
2. Explain the roles and responsibilities of Controllers and Processors and clarify the types of contracts that should be put in place between them.
3. Provide examples of specific arrangements and requirements for research that requires clinical data; and
4. Clarify Data Protection requirements that need to be addressed before the research proceeds and outline Principal Investigator's (PI) responsibilities in that regard.

How to reference this Guide

Version 1.0 July 2022

Table of Contents

1. Types of data

1.1 Personal Data: means any information relating to an identified or identifiable natural person i.e. living individual ("***Data Subject***"), where the Data Subject can be identified or is identifiable, directly from the information in question or indirectly from that information in combination with other information(s) (see Appendix 1 for categories of Personal Data)

1.2 Special Category Personal Data: This type of data, commonly referred to as **sensitive data,** includes Personal Data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.

- **Genetic Data**: is Personal Data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

  For example: in some clinical trials, samples are taken from the subjects or patients in order to characterise their genetic profile and to use this information to correlate sub-populations of patients responding to the treatment to a specific genetic profile, which then may be studied and validated as a biomarker.

- **Data Concerning Health:** is Personal Data related to the past, current or future physical or mental health of a Data Subject, which could directly or indirectly allow his/her identification.

- **Biometric data:** means Personal Data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images, fingerprints, models, similarity scores, behaviour data and all verification or identification data excluding the individual's name and demographics

1.3 Pseudonymised Data: is data derived from Personal Data which has undergone a process of "Pseudonymisation". Pseudonymisation is a de-identification procedure by which data fields which allows the identification of an individual are replaced by a pseudonym, which could be for example a number or a code. Pseudonymised Data, therefore, can no longer be attributed to a specific Data Subject without the use of additional information (i.e. a key/code). Such additional information must be kept separate and technical and organisational measures (TOMs) for the protection of the data should be in place.

Pseudonymised Data in the hands of the Organisation holding the Identification key is to be regarded as Personal Data because it enables the identification of an individual *(albeit via a key).* Therefore, it is subject to GDPR requirements. However, provided that the "key" that enables re-identification of individuals is kept separate and secure (i.e. functionally separated) and TOMs are in place, the risks to the Data Subject associated with Pseudonymised Data are reduced.

Under Article 89 GDPR Pseudonymisation is specifically recommended as to ensure data minimisation in scientific research.

If one Organisation (Data Provider) shares with another Organization (Data Recipient) Pseudonymised Data without any identification key, so that it could be used for a project conceived by the Data Recipient, the responsibilities of the Data Recipient and Provider under GDPR and the HRR depend on whether the data being shared has to be pseudonymised for the purpose of the Recipient Organisation's project (scenario A below) or had already been pseudonymised by the Data Provider for its own purpose (scenario B below).

- <u>Scenario A: sharing of data requiring pseudonymisation prior to sharing</u>

  An organization (Data Recipient) asks another organisation (Data Provider) to share pseudonymised data for the purpose of its research and for this purpose the Provider Organisation has to pseudonymise Personal Data prior to it's sharing, the Recipient Organization is responsible as Data Controller for ensuring GDPR and HRR compliance for the pseudonymisation process.

  The role of the Provider Organization (data processor/separate controller/joint controller) in the pseudonymisation process should be assessed and agreed on a case-by-case basis (see section 7)

Whatever the case may be, the Data Provider, holding the identification key, shall be responsible for protecting the pseudonymised data which is Personal Data in its hands

Example: A university asks a hospital to share pseudonymised clinical data for the purpose of a research project conceived by an investigator of the university. The hospital is required to pseudonymise Personal Data taken from medical records so that it can be shared with the university.

The University is therefore responsible as Data Controller for ensuring GDPR and HRR compliance for the pseudonymisation process. The role of the Hospital (data processor/separate controller/joint controller) depends on the Hospital's role (if any) in the research project and determining the manner by which Personal Data is processed.

- Scenario B: sharing of data that had already been pseudonymised for another purpose

An Organization (Data Provider) agrees to share with another organisation (Data Recipient) pre-existing Pseudonymised Data which was generated from Personal Data that had already been collected and pseudonymised by the Data Provider for its own purpose and the Data Recipient contractually commits:

- not to make any attempt to identify a Data Subject from the shared dataset
- to inform your organisation immediately if any inadvertent identification occurs, thereby resulting in a data breach
- to use the data for the specified agreed purpose only
- not to share the data with any other organisations without the approval of the organisation providing the data

In this case, as long as there is a low risk of Data Linking and Personal Knowledge (i.e. expert knowledge from Recipient/its employees accessing the dataset) which would allow the Recipient to identify Data Subjects, the shared data can be regarded as anonymous in the hands of the Data Recipient

The Data Provider is responsible for ensuring that the sharing of the Pseudonymised Data in question is permissible under GDPR and HRR, and should contractually warrant to having the appropriate Consent and Lawful basis for transferring the data with the Data Recipient (i.e. the Data Subjects have given explicit consent that the data would be processed, pseudonymised and shared with third parties for a purpose that is compatible with the research of the Data Recipient).

Example: a university asks a hospital to share pre-existing pseudonymised data which had originated from Personal Data contained in the Hospital's medical records and had undergone the process of pseudonymisation so that it could be used for a clinical study conceived by the investigator of the hospital.

The hospital is responsible as Data Controller for ensuring GDPR and HRR compliance for the pseudonymisation process.

NOTE: Please note the interpretation, in scenario B, that pseudonymised data can be regarded as anonymous in the hands of the Data Recipient is accepted by many but not all European countries and organisations. Therefore, if you are the Recipient of Pseudonymised Data, it is necessary to check with the Provider whether they agree with this interpretation.

The Provider may insist that the sharing of Personal Data is subject to a GDPR compliant data sharing or processing agreement (as appropriate) (see sections 4 and 5 of this document).

1.4 Anonymised Data: is Personal Data that has been amended in such a way that no individuals can be identified from the data (whether directly or indirectly) by any means or by any person. Data that is fully and truly anonymised (i.e., data from which no individuals can be identified) fall outside the scope of both the Directive and the GDPR.

1.5 Dataset: is a collection of related, discrete items of related Personal Data that in the context of the study are subject to the same processing activities

Mixed dataset comprises both personal and non-Personal Data (including those containing health data). If the non-Personal Data parts are 'inextricably linked' the data protection rights and obligations stemming

from the GDPR fully apply to the whole mixed dataset. Inextricable link is not defined by either FFD or GDPR, however the European Commission offers a practical explanation i.e. for practical purposes, it can refer to a situation whereby a dataset contains Personal Data and non-Personal Data and separating the two would either be impossible or considered by the controller to be economically inefficient or not technically feasible. Consequently, such mixed datasets will generally be subject to GDPR obligations of Controllers and Processors.

2. Data processing

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

Processing of Personal Data may be done directly by the Data Controller (see definition below) and/or by a Data Processor under the instruction of the Data Controller (see definitions of Data controller and Processors below)

3. Data Controller

GDPR differentiates two main data protection roles: Data Controller and Data Processor, which have very different decision-making power and responsibilities. Therefore, when a research project requires processing of Personal Data it is extremely important to clarify the data protection roles of the Parties involved in the processing of Personal Data.

3.1 Role of the Data Controller – The Data Controller is normally the organisation(s) of the Investigator (s) who determine(s) the purpose and the manner by which Personal Data is processed for a research project. This commonly coincides with the organisation of the researcher who conceives a research idea and generates the project plan.

In other words, the Data Controller decides '**why**' and '**how**' the Personal Data should be processed and/or determines the methods of processing.

Control, rather than possession, of Personal Data is the key factor in determining who the Data Controller is.

Examples of decisions that **the Data Controller** takes:

- To collect Personal Data in the first place.
- The types of Personal Data to collect.
- The purpose or purposes the data are to be used for.
- Which individuals to collect data about.
- Pre-screening an individual to determine suitability for data collection
- Whether to disclose the data, and if so, to whom.
- What to tell individuals about the processing.
- How to respond to requests made in line with individuals' rights.
- How long to retain the data or whether to make non-routine amendments to the data.

Responsibilities of the Data Controller:

The Data Controller is ultimately responsible for the data and has the highest level of compliance responsibilities. These include:

- Compliance with GDPR Data Protection principles described in Appendix 2a and 2c.
- Compliance with all relevant laws including the Health Research Regulations.
- Identifying the appropriate legal basis for processing Data for a given purpose (your DPO can advise on the appropriate legal basis for the processing of Personal Data for your project).
- Facilitating individuals to exercise their rights (see Appendix 2b)
- Implementing technical and organisational security controls
- Obtaining adequate reassurance that your Processors are complying with regulations
- Having binding contracts with any Data Processors and joint Controllers
- Notifying the Data Protection Commissioner Office of any data breaches (typically via the DPO)
- Complying with organisational accountability obligations (see Appendix 2c)

Note: A Principal Investigator and their research team come under the umbrella of their organisation in its Data Controller capacity and have day to day responsibilities to comply with Data Protection law. PI's responsibilities/requirements are clarified in section 7 of this document.

3.2 Differentiation between Joint and Separate Data Controllers and contractual arrangements for sharing data

Data Controllers may share Personal Data as Joint or Separate Data Controllers

3.2.1 Joint Data Controllers

Joint Data Controllers is the term used to define two or more organisations who jointly determine 'why' and 'how' Personal Data should be processed and or the means of processing

For example, in the case of collaborative research, when two or more Investigators from different organisations jointly conceive a research project and the project requires that Personal Data is shared between them, their organisations may agree to assume the Joint Controller role.

Under Article 26 of GDPR, Joint Controllers must enter into an agreement, which sets out their respective data protection responsibilities and obligations, including enabling the Data Subjects to exercise their rights and knowing which joint controller to contact to do so.

This approach, however, is not necessarily taken in all collaborations. For example, an organisation who plays a greater role or have a greater responsibility in relation to the processing of Personal Data may decide to assume the sole Controller role. The other Partner organisations assume the role of Data Processors. This approach is commonly taken in clinical trials involving collaborating organisations whereby the Academic organisation taking the sponsor role assumes the sole Data Controller role.

Examples of Joint Data Controller scenarios can be found in Appendix 3

3.2.1.1 Contractual requirements for sharing data as joint Controllers

Joint Controllers sharing Personal Data must clearly set out their respective responsibilities for complying with the GDPR and must put in place a data sharing agreement. This is most commonly called a **Joint Controller Data Sharing Agreement.** The relevant features of the arrangement must be communicated to the individuals whose data is being processed (i.e. Data Subjects or study participants). This can be done in the participant information leaflet or via privacy notice*.

3.2.2 Separate Controllers

The term Separate Controller is used to define two or more organisations who set different purpose(s) for the processing of the same Personal Data. One Data Controller may share Personal Data with another organisation who determines its own/separate purpose/means of processing of Personal Data. Separate Data Controllers may sometimes be referred to as Independent Data Controllers as they make independent decisions on the processing of Personal Data. Examples of Separate Data Controller scenarios can be found in Appendix 3.

Important note: Sharing of data with another organisation for health research purposes must under the Health Research Regulations have the explicit consent of the Data Subject via participant information leaflet or privacy notice or otherwise have a consent declaration from the Health Research Consent Declaration Committee. The processing purpose of the health data must be compatible with the purpose consented to by the Data Subject.

---

* A privacy notice is a document provided by the research team that explains how the research team processes Personal Data and how it applies Data Protection principles

3.2.2.1 Contractual requirements for sharing Personal Data as Separate Controllers

If Separate Controllers share Personal Data, the Data Protection Regulation does not mandate any particular format of (data sharing) contract or arrangement (except for cross-border transfers – see section 7.2.1D). However, Irish Research Performing Organisations agree on the requirement for a **Separate Controller Data Sharing Agreement** which clarifies the roles and respective obligations of the separate Data Controllers and sets out clear procedures and systems for recurrent data sharing.

4. Data Processor

4.1 Role and responsibilities of the Data Processor - A Data Processor is the legal entity/individual which processes Personal Data on behalf of and under the instruction of the Controller. The existence of a Processor depends on a decision taken by the Controller, who can decide either to process data within his/her organisation (without the involvement of a Data Processor), or to delegate all or part of the processing activities to one or more external organisations (Data Processors).

Examples of Data Controller and Processor scenarios can be found in Appendix 3

A Data Processor does not have the same level of obligations under Data Protection legislation as Controllers. However, the Data Processor does have some direct obligations. These include:

- Only processing data in accordance with the instructions of the Data Controller and on behalf of the Controller (meaning it may not carry out processing for its own purpose(s))
- Entering into a binding contract with the Controller putting direct responsibilities on the Processor
- Not engaging a sub-processor without the written permission of the Controller
- Applying appropriate technical and organisational security measures to protect the data
- In the event of a breach, notifying the Controller without undue delay and assisting the Controller in complying with its responsibilities regarding breaches

Important notes:

- Actions can be taken directly against a Processor if the Processor breaches any of its obligations vis-à-vis the controller
- A Data Processor becomes a Data Controller if it processes Personal Data for its own purposes or in a manner that deviates from the Controller's instructions.

  For example, in instances where a Processor (who had been engaged by a Data Controller to perform the analysis of Personal Data for a defined research purpose, in accordance with the Controller's instructions) decides to use the data for its own purposes or in a manner that deviates from the Controller's instruction, the Processor (a) breaches the contract with the Controller and (b) becomes a Controller (subject to GDPR/ HRRs obligations) and may therefore breach the Controller's obligation to protect the rights of the Data Subject. This in turn would breach GDPR and/or the Health Research Regulations and be subject to GDPR penalties which are explained in webpage below

  Penalties: https://www.gdpreu.org/compliance/fines-and-penalties/

4.2 GDPR contractual requirement for engaging a Data Processor

In accordance with GDPR, Data Controllers are required to ensure that a legally binding Data Processing Agreement is in place with any parties that act as Data Processors on their behalf.

A Data Processing Agreement is a legally binding document that states the rights and obligations of each party (Controller and Processor) concerning the protection of Personal Data. Your Data Protection Officer may have a template agreement that you can use.

5. Data Processor and Controller roles for research requiring clinical data and contractual arrangements

As explained earlier in this document, the designation of Data Controller or Processor depends on who has defined the purpose and the manner by which data is processed.

Some research projects may use Personal Data, which is collected separately for another purpose.

In clinical trials, for example, Personal Data may be used at the same time for the purpose of research and delivery of care. Other types of research rely on pre-existing clinical data.

In the case of research relying on clinical data, the Data Protection arrangements differ depending on whether the Personal Data is used for a clinical study/trial or whether the Personal Data is used for research as a secondary purpose.

5.1 Personal Data for a clinical study/trial - In clinical trials where research and care delivery rely on the same Personal Data, the hospital is commonly the Controller for the data when it is used for the purpose of delivering care and the Sponsor of the clinical trial/study is usually the Controller for the data when it is used for the purpose of the clinical trial.

Therefore, the Hospital and the organisation acting as Sponsor of the clinical study/trial are Separate Controllers.

In consideration of the above, the Sponsor, as Data Controller for the purpose of the clinical trial, is responsible for data protection requirements, including, among others, completion of the DPIA and contracts for data processing and/or sharing (as applicable depending on the clinical trial context).

However, if hospital employees process Personal Data for the purpose of the clinical study/trial which is unrelated to the delivery of care, with regard to these processing activities the hospital assumes the Data Processor role working under the instructions of the Sponsor.

Likewise, if employees of the organisation sponsoring the study (e.g. research nurses) process Personal Data for the delivery of care, with regard to these processing activities, the Sponsor organisation assumes the Data Processor role working under the instruction of the hospital.

Therefore, Hospital and Sponsor organisation may have dual Data Controller and Processor role depending on what they are processing the Personal Data for.

In clinical trials/studies, there are often other organisations (e.g. Universities) who are involved in a clinical trial/study in a supporting role (e.g. the University's CRC/CRF provides research nursing support at the local Hospital) and their employees process Personal Data for the purpose of the clinical trial. In this case the other organisations are also Data Processors working under the instruction of the Sponsor as Data Controller.

In the event that a clinical Investigator undertakes a clinical study without the involvement of an academic or Industry Sponsor, the Hospital assumes the Data Controller roles for the clinical Personal Data that is processed for the purposes of research and the delivery of care.

The Clinical Investigator is required to ensure in advance the Hospital's acceptance of the Data Controller role, in accordance with the Hospital's approval procedure.

5.1.1 Contractual approach

To address the arrangements outlined above, clinical trial agreements should include:

Data sharing provisions - to cater for the sharing of Personal Data between the Hospital and the Sponsor as Separate Data Controllers, each using the same Personal Data for their own separate purpose.

Data processing provisions – to cater, if applicable, for one or more of the following scenarios:

- Sponsor's employees processing Personal Data for delivery of care
- Hospital's employees processing Personal Data for the purpose of the clinical trial
- Another organisation's (e.g. University) employees processing Personal Data for the purpose of the clinical trial

5.2 Clinical data used for a research project as secondary purpose

In this instance, the research project and the delivery of care are not interdependent activities but require the same Personal Data. Therefore, the academic organisation of the Investigator conceiving the research project, and therefore setting the research purpose of the processing activity using the Personal Data, assumes the Data Controller role for the research purpose. The Hospital, on the other hand, is the Data Controller for the same data being used for the delivery of care.

The Hospital therefore shares data with the academic organisation as Separate Data Controllers and the terms of sharing of Personal Data by the Hospital with the research organisation are governed by a Separate Controllers Data Sharing Agreement (see section 3.2.2.1).

In the event that the research project is carried out by a Clinical Investigator of a Hospital and does not involve another organisation, the Data Controller role rests with the Hospital.

If a Clinical Investigator has a dual research affiliation with a hospital and an academic organisation, for each research project the Clinical Investigator is required to stipulate the organisation which he/she would like to assume the Data Controller role for the research. The acceptance of the role is subject to acceptance, in accordance with the chosen organisation's approval procedure.

If researchers from other organisations process Personal Data for the purpose of the projects under the instructions of the Data Controller, their organisations assume the Data Processor role. This arrangement is governed by a Data Processing Agreement (see section 5.1.1).

6. Data Protection Impact Assessment (DPIA)

A DPIA is a process designed to help the Data Controller systematically analyse, identify, and minimise the Data Protection risks of a project. It is a key part of the Data Controller's accountability obligations under the GDPR, and when done properly helps to assess and demonstrate how to comply with Data Protection obligations. The completion of a DPIA (if required) for the processing of Personal Data for a given research purpose is the sole responsibility of the Controller of the Data being used for that research purpose.

For the avoidance of doubt a DPIA is not required in the following instance:

1. Your project does not Process Personal Data
2. Your organisation is not the Controller of the Personal Data, which you are planning to process, and you will process the Personal Data under the instruction of another organisation, who is the Data Controller (i.e. you are a Processor).
3. You are planning to process Anonymised Data (see definition in section 1 of this document)

You are planning to process pre-existing Pseudonymised Data (i.e. the data does not require pseudonymisation for your research purpose) which will be lawfully shared with you by another organisation (without any identification key), and you/your organisation contractually commits (a) not to try to re-identify the Data Subject, (b) not to combine the shared data with another data set that would allow you to re-identify Data Subjects, (c) to process the data for the agreed purpose only, (d) not to share the data with any other organisation without the approval of the organisation providing the Data. Subject to specific organisational requirements, this assessment may need to be documented.

General guidance on the DPIA completion and review process is provided in Appendix 4.

In general Investigators should engage with the DPO of the organisation assuming the Data Controller role in advance of undertaking a DPIA to clarify the organisational requirements, such as the completion of a screening questionnaire, application form, review procedure, etc.

Please note that the DPO plays an advisory role only and should not expected to complete a DPIA.

7. Legal and Data Protection organisational requirements applicable to Investigators

Any investigator who is planning to process Personal Data should ensure compliance with the requirements below.

The requirements are dependent on the role of the Investigator's organisation with regard to the processing activities, i.e. whether the organisation is the Data Processor (Scenario 1) or Controller (Scenario 2)

7.1. Scenario 1: Data Processor

The following requirements apply to investigators who are planning to process Personal Data on behalf of and under the instruction of another organisation (and therefore his/her organisation assumes the Data Processor role).

- Ensure that a Data Processing Agreement is in place (i.e. fully signed) before any Personal Data processing activity commences.
- Process the Personal Data in accordance with the Data Controller's instructions and in compliance with the Data Processing Agreement entered into by your organisation with the Data Controller.

7.2 Scenario 2: Data Controller

The requirements outlined below apply to investigators who have defined the purpose and the manner by which Personal Data is processed for their research project and therefore their organisation has agreed to assume the role of Data Controller.

Some of the requirements are context specific (Context Specific Requirements) and others apply regardless of the context (Standard Requirements).

7.2.1 Context specific requirements (Data Controller)

The requirements below address 4 main scenarios:

A. Your research project relies on newly generated Personal Data
B. Your research project relies on pre-existing Personal Data
C. You are planning to share pre-existing Personal Data with an Investigator of another organisation based in the European Economic Area.
D. You are planning to share Personal Data with an investigator of another organisation based outside the European Economic Area

A. Your project relies on newly generated Personal Data

If the research project relies on newly generated Personal Data, the requirements change depending on whether:

A1. You have conceived the project alone (or in collaboration with an investigator of your organisations)

A2. You have conceived a project in collaboration with one or more investigators from other organisations

A3. The newly generated Personal Data will also be used for another application (purpose) determined by someone from another organisation

The requirements applicable to each context are outlined below

A1. You are planning to process newly generated data and you have conceived the project alone (or in collaboration with an investigator of your organisation)

a. Complete DPIA
b. Develop consent form (CF), PIL
c. Submit DPIA/CF and PIL to DPO for review/feedback
d. Seek ethics approval

A2. You are planning to process newly generated data and you have conceived a project in collaboration with one or more investigators from other organisations

a. Complete DPIA in consultation with your collaborator(s)
b. Develop CF, PIL making sure the planned collaboration/sharing of data is transparent.
c. Submit DPIA/CF and PIL to DPO for review/feedback and ensure that the DPIA is also deemed appropriate by the DPO(s) of your collaborator's organisation
d. Seek ethics approval
e. Ensure that a Joint Controller Data Sharing Agreement is in place or
f. In instances where Personal Data is linked to / shared with biological material, a Material Transfer and Joint Controller Data Sharing Agreement is in place.

A3. You are planning to process newly generated Personal Data (primary data collection) which will also be used for another application (purpose) determined by someone from another organisation (e.g. the clinical data required for a clinical study is also used for the delivery of care)

a. Complete DPIA for the use of data in your project
b. Develop CF, PIL making sure the planned collaboration/sharing of data is transparent.
c. Submit DPIA/CF and PIL to Sponsor's DPO for review/feedback
d. Seek ethics approval
e. Ensure that a Separate Controllers Data Sharing Agreement is in place or
f. In instances where Personal Data is linked to / shared with biological material, a Material Transfer and Separate Controller Data Sharing Agreement is in place.

In the case where Personal Data is collected in a hospital under any of the scenarios above

a. The hospital's DPO may also require review of the DPIA*
b. Ethics approval is sought via the hospital's ethics committee
c. University ethics committee is notified (please check whether this requirement applies to your university's ethics committee)

(*you need to clarify this requirement with the hospital)

B. Your project relies on pre-existing Personal Data

If you are planning to process pre-existing Personal Data the requirements change depending on whether:

B1. You (on behalf of your organisation as Data Controller) had generated the Personal Data for your own purpose (e.g. data generated for a previous project).

B2. The pre-existing data had been generated and will be shared with you by an Investigator of another organisation, and whether the pre-existing data is pseudonymised prior to being shared

The requirements applicable to each context are outlined below:

B1. Requirements applicable to the processing of pre-existing Personal Data that you had generated for your own purpose

1. Submit the Data Subject CF and PIL to the DPO to ensure that it is compatible with your planned use of the Personal Data and is compliant with the Health Research Regulations (HRR).

1a. If the CF is compatible with your planned use of the Personal Data and is compliant with the Health Research Regulations

a. Complete/update existing DPIA
b. Submit DPIA to the DPO of your organisation for review/feedback
c. Engage with Ethics Committee to clarify whether any approval/notification is required

1b. If the CF is not HRR compliant but it is possible to apply for consent declaration

a. Complete/update existing DPIA
b. Submit DPIA to the DPO of your organisation for review/feedback
c. Seek ethics approval
d. Apply for consent declaration
e. Complete rights balancing tests where applicable
f. Include supporting evidence where applicable.

B2. Requirements applicable to the processing of pre-existing Personal Data which had been generated and will be shared with you by an Investigator of another organisation

The requirements outlined below depend on whether the pre-existing data is or is not pseudonymised prior to being shared with you.

B2a. Requirements for processing Pseudonymised Data

If the Personal Data is pseudonymised prior to being shared with you and is shared with you without any identification key or identifying characteristics, can be regarded as Anonymised Data in your hand.

In this instance you are required to comply with any requirement that the organisation of the Investigator sharing the Data with you may set in a Data Sharing Agreement with your organisation

B2b. Requirements for processing Personal Data

1. Submit the Data Subject CF (and associated PIL) to the DPO to ensure that the original CF is compatible with your planned use of the Personal Data and is HRR compliant

1a. If the CF is compatible with your planned use of the Personal Data and is compliant with the HRR

a. Complete/update existing DPIA
b. Submit DPIA to the DPO of your organisation for review/feedback
d. Consult with the ethics committee to clarify whether any approval/notification is required
e. Comply with any requirement that the organisation of the Investigator sharing the Data with you may set in a Data Sharing Agreement with your organisation

1b. If the consent is not HRR compliant but it is possible to apply for consent declaration

a. Complete/update existing DPIA
b. Submit DPIA to the DPO of your organisation for review/feedback
c. Seek ethics approval
d. Apply for consent declaration
e. Comply with any requirement that the organisation of the Investigator sharing the Data with you may set in a Data Sharing Agreement with your organisation.

C. You are planning to share existing Personal Data with an investigator of another organisation based in the European Economic Area (EEA)

If you are planning to share with an investigator from another organisation based in the EEA existing Personal Data (Shared Data) that you or the other Investigator had generated for your/their own purpose, the requirements change depending on whether the Shared Data is Personal or Pseudonymised Data.

C1. Requirements for sharing Pseudonymised Data (which in the hand of the recipient organisation can be regarded as Anonymised Data)

If you are planning to share pseudonymised data with an investigator of another organisation please remember that, prior to sharing the Data, it is necessary to put in place an agreement between your organisation and the organisation of the Investigator you wish to share the Data with. The purpose of the agreement is to ensure that the recipient organisation contractually commits:

1. not to make any attempt to identify a Data Subject from the shared dataset,
2. to inform your organisation immediately if any inadvertent identification occurs, thereby resulting in a data breach.
3. to use the data for the specified agreed purpose only
4. not to share the data with any other organisations without the approval of the organisation providing the data.

If you are planning to share pseudonymised data please consult with your DPO to ensure that the data is truly anonymous in the hands of the Recipient organisation and the consent of the Data Subjects is in place for such sharing of data with third parties.

C2. Requirements for sharing Personal Data

a. Complete/update DPIA
b. Submit DPIA to the DPO of your organisation for review/feedback
c. Consult with the ethics committee on whether an amendment of the ethics application is required
d. Ensure that the appropriate data sharing agreement is in place before you share the data.

D. You are planning to share Personal Data with an investigator of another organisation based outside the EEA

If you are planning to share Personal Data with an investigator of another organisation based outside the EEA, you need to consult with your DPO. Your DPO will check whether the European Commission has assessed that the country of the organisation the data is to be shared with has an adequate standard of protection for Personal Data. This is known as an adequacy decision. If an adequacy decision has been made for the country in question, the requirements outlined above apply. If an adequacy decision has not been made, additional safeguards will be required, such as EU Standard Contractual Clauses.

EU Standard Contractual Clauses (SCC) are predefined template agreements which must be put in place with the recipient organisation. They address two different scenarios:

- the recipient organisation is a Data Controller
- the recipient organisation is a Data Processor

If you intend to use Standard Contractual Clauses for your international data transfers, you have to undertake an assessment if the SCCs on their own will be sufficient to offer Data Subjects privacy rights to a level equivalent to the one they enjoy in the EEA. If not, you need to put additional safeguards in place with the data importer. The need for such a data transfer assessment is rather new. Your DPO might be able to provide you with a template for such a data transfer assessment.

Other requirements include:

a. Complete/update DPIA
b. Submit DPIA to the DPO of your organisation for review/feedback

c. Consult with the ethics committee on whether an amendment of the ethics application is required
d. Ensure that the appropriate data sharing agreement is in place before you share the data.

7.2.2 Additional requirements (Data Controller)

The following requirements are in addition to those outlined in section 7.2.1 of this document and, as those in 7.2.1, apply to investigators who have defined the purpose and the manner by which Personal Data is processed for their research project and therefore their organisation has agreed to assume the role of Data Controller.

Some of the requirements set out below are set by GDPR and the HRR. The others are indirectly linked to GDPR and the HRR and are necessary to protect Personal Data and ensure that the plan to process Personal Data for the research project is ethical.

GDPR and HRR requirements

Ensure consent requirements (as a safeguard) are appropriately addressed

- Ensure compliance with the principles of data minimization, privacy by design and default (see Appendix 2c)
- Ensure that the Data Subject's CF is compliant with the HRR and GDPR
- Ensure, where applicable, that the appropriate privacy notice or PIL is in place. Privacy notices need to be informative, easy to understand and complete (req of Art 13. and 14 as appropriate).
- Ensure that each CF and PIL is individually recorded, including the version number.
- Have a clear plan as to what will happen to data after a project has finished, e.g. safe data destruction; appropriate retention periods and rational for such periods; which repository or archive would be appropriate; can data be anonymized? etc. In most cases this information will have been compiled already as part of a data management plan. In these cases, inclusion of, or link to the data management plan will be sufficient.
- Ensure that there is an access log to track who the data were disclosed to (as per GDPR Article 30 requirements)
- If data are shared beyond the EEA or a country without an adequacy decision, ensure that there is an appropriate rationale identified for doing so, and that the appropriate transfer mechanisms are put in place.
- Notify the DPO of any data breach

Other requirements

- Ensure that your project data management plan includes a plan for Data Protection: A Data Protection plan should be conceived as early as possible as part of your research plan.
- Apply to the applicable Research Ethics Committee (REC) to ensure that the plan of processing Personal Data is ethical. If you are planning to process Personal Data of hospital patients, it is sufficient that you seek ethics approval from the patient hospital ethics committee. However, the university ethics committee may also require notification (please clarify this requirement with your university's relevant ethics committee).
- Ensure that any suppliers or providers used are GDPR compliant and that Controller – Processor agreements are in place.
- Familiarize yourself with and comply with your organisational IT security policy to ensure data protection. If necessary, engage with your organisational IT Dept. to ensure that security measures are adequate to protect the project's Personal Data.
- Ensure that equipment/systems used for processing Personal Data are fit for purpose (engage with IT Services to verify that this is the case).
- Ensure that any software or cloud solution used is licensed and GDPR compliant and that contracts are put in place (engage with IT Services to verify that this is the case).
- Ensure that data collection both at rest and transmission is safe and secure, e.g. END to END encryption, encrypted laptop, encrypted wifi, password, password frequency change etc.

- Ensure that everyone involved in the project is clear about any legal or sector specific requirements, e.g. GDPR, Health Research Regulations; Clinical Trial Directives (or upcoming Regulation); and more.
- Ensure that there is a clear policy and process for who the data can be sent to and who can access them.
- Ensure that there is a clear policy and procedure on who is authorized to modify and update data, including logging of changes made.
- Ensure that everyone in the team handling Personal Data can access appropriate training in Data Protection.
- Ensure that data are only stored on designated equipment, which is tracked by a list or log.
- Liaise, throughout the project, with the relevant units in the PIs' organisation and to keep them up to date with any changes to the project that are material to GDPR considerations, e.g. DPO, Research Office and more.
- In the event that a member of the team leaves or moves on, ensure that all data are retrieved from that person. If new arrangements need to be made as a consequence, that they are appropriately documented and supported by contracts. This includes making any updates to privacy notices, where required.

APPENDIX 1: CATEGORIES OF PERSONAL DATA

CATEGORY OF PERSONAL DATA									
Identifying Information	**Location/ Contact Information**	**Device/ Account Information**	**Historical Information**	**Physical Characteristics**	**Family Information**	**Professional Information**	**Behavioural Information**	**Financial Information**	**Biometric Information**
Examples									
First name Last name Maiden name Other names used Username Face Photographs Other identifying photographs Date of Birth Medical card number Passport information Social security / social insurance number Driver's license / state ID Professional license records Recreational license records	Personal email address Work email address Website Work address Current home address Cell phone Work phone Contacts list	Third-party login Cookies IP address ISP Device ID / MAC address Browser Operating system Location history (physical) Phone call records Text message history Vehicle registration records	City of birth Birth certificate	Hair colour Age Weight Height Gender Eye colour	Marital status Spouse name Parents' names Number of people in household Children's names Siblings' names Friends' names	Occupation Current employer Employment history Performance evaluations Reference interviews HR issues & disciplinary actions Email Records Postal activity Curriculum Vitae	Daily life activities Event attendance Media preferences Topics of interest Activity on the site	Current income Life insurance records Health insurance records Transactional records Credit rating	Dactyloscopic data Fingerprints Facial recognition Video recordings Audio recordings

APPENDIX 2A – GDPR DATA PROTECTION PRINCIPLES

Lawfulness, fairness and transparency

Personal Data must be processed lawfully, fairly and transparently. Organisations should read this transparency requirement in light of the requirement to provide more detailed privacy notices to Data Subjects. The Controller is required to take appropriate measures to provide information, in advance of any data collection, to a Data Subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language

Purpose limitation

Personal Data must be collected for specified, explicit and legitimate purposes. It cannot be further processed in a manner incompatible with those purposes

Exceptions: Further processing of Personal Data for scientific and historical research purposes or statistical purposes will not be considered incompatible with the original processing purposes. The GDPR adds that further processing of Personal Data for archiving purposes in the public interest will not be considered incompatible with the original processing purposes. Further processing is subject to the implementation of appropriate technical and organisational measures.

Accuracy

Personal Data must be accurate, and where necessary kept up to date. Reasonable steps must be taken to ensure that inaccurate Personal Data is erased or rectified without delay.

Storage limitation

Personal Data must be kept in a form that permits identification of Data Subjects for no longer than is necessary

Exceptions: Personal Data may be stored for longer periods for scientific or historical research purposes or statistical purposes, or archiving purposes in the public interest, provided appropriate technical and organisational measures are implemented.

Integrity and confidentiality

Personal Data must be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. While this requirement existed under the Directive, the GDPR now specifically categorises it as a Data Protection principle.

Accountability

Accountability is a new concept introduced by the GDPR. It requires Controllers to be able to demonstrate how they comply with the Data Protection principles listed. This is significant as it shifts the burden of proof to the Data Controller in the event of a compliance investigation by a Data Protection authority. Organisations should view this principle in light of the record keeping obligation, the requirement to prove that consent was obtained and the concept of Privacy by Design and Default (see Appendix 2c).

APPENDIX 2B – GDPR DATA SUBJECTS RIGHTS

The GDPR provides Data Subjects with additional rights and protections, which equate to new obligations for Controllers and Processors. It also strengthens the concepts of rectification, erasure, restriction of processing that existed under, or were derived from the Directive.

- **Right to be informed** (in a clear, concise, intelligible, easily understandable, and accessible manner)
- **Right of access**

The Data Subject shall have the right to obtain from the Controller confirmation as to whether or not Personal Data concerning him or her are being processed, and, where that is the case, access to the Personal Data and the following information:

- the purposes of the processing;
- the categories of Personal Data concerned;
- the recipients or categories of recipient to whom the Personal Data have been or will be disclosed, in particular recipients in third countries or international organisations;
- where possible, the envisaged period for which the Personal Data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from the Controller rectification or erasure of Personal Data or restriction of processing of Personal Data concerning the Data Subject or to object to such processing;
- the right to lodge a complaint with a supervisory authority;
- where the Personal Data are not collected from the Data Subject directly, any available information as to their source;
- the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the Data Subject.

Where Personal Data are transferred to a third country or to an international organisation, the Data Subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

- **Right of data rectification** - A Data Subject is entitled to have inaccurate Personal Data concerning him or her rectified without undue delay. Data subjects are also entitled, taking into account the purposes of the processing, to have incomplete Personal Data completed.

- **Right to object** _Data Subjects have the right to object to certain types of processing of their Personal Data where this processing is carried out in connection with tasks:
    - in the public interest,
    - under official authority, or
    - in the legitimate interests of others.

  Data Subjects may also object to processing of their Personal Data for research purposes, unless the processing is necessary for the performance of a task carried out in the public interest.

  In order to object to processing, a Data Subject must contact the data controller and state the grounds for his/her objection. These grounds must relate to the Data Subjects particular situation. Where a Data Subject has made a valid objection, the Data Controller must cease processing the Data Subject's Personal Data, unless the data controller can provide compelling legitimate reasons to continue processing the data. Data Controllers can also lawfully continue to process the Data Subject's Personal Data if it is necessary for certain types of legal claims.

  Where the right to object applies, Data Controllers are obliged to notify the Data Subject of this at the time of their first communication with Data Subject. Where processing is carried out online, data controllers must offer an online method to object.

- **Right to restriction of processing** The GDPR introduces a Data Subject's right to restrict processing. This right replaces the right to block certain uses as contained in the Directive.

  There are four instances in which a Data Subject is entitled to restrict processing of his or her Personal Data as an alternative to erasure:

    - The accuracy of the Personal Data is contested by the Data Subject, in which case the processing is restricted for a period enabling the Controller to verify the accuracy of the Personal Data.
    - The processing is unlawful and the Data Subject opposes the erasure of the Personal Data and requests the restriction of its use instead.
    - The Controller no longer needs the Personal Data for the purposes of the processing, but the Personal Data is required by the Data Subject for the establishment, exercise or defence of legal claims, and
    - The Data Subject has objected to processing pending the verification whether the legitimate grounds of the Controller override those of the Data Subject.

  When processing has been restricted, continued processing, with the exception of storage, may only occur in the following cases:

    - The Data Subject consents
    - The processing is necessary for the exercise or defence of legal claims
    - The processing is necessary for the protection of the rights of other individuals or legal persons, or
    - The processing is necessary for public interest reasons

  A Data Subject is entitled to be notified by a Controller before a restriction on processing is lifted.

- **Right to data portability**: The GDPR introduces a new right of data portability which enables a Data Subject to receive Personal Data concerning him or her, in a structured, commonly used and machine-readable format, and to transmit that data to another Controller without hindrance from the Controller which provided the Personal Data.The right only applies to Personal Data that a Data Subject has provided to a Controller (applicable only to processing of automated data.)

  In order to facilitate Data Subjects in the exercise of this right, Controllers and Processors will be required to develop procedures and tools so as to comply with the requests of Data Subjects.
  The Data Subject may only exercise the right to data portability where the processing is based on the Data Subject's consent or is for the performance of a contract to and the processing is carried out by automated means. The right to data portability will not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller.

- **Right to erasure:** A Data Subject is entitled to have Personal Data concerning him or her erased in specified circumstances. This is known as the right of erasure or 'the right to be forgotten'. This entitlement is an extension of the right protected in the Directive.The Directive gave Data Subjects a right of erasure where their data was being processed in breach of the Data Protection principles, in particular because of the incomplete or inaccurate nature of the data.

  Where the Controller has made the Personal Data public and is subsequently obliged to erase the Personal Data the Controller may have further obligations. Taking account of available technology and the cost of implementation Controller is required to take reasonable steps, including technical measures, to inform third party Controllers who are processing the data, that the Data Subject has requested the erasure by such Controllers of any links to, or copies of, those Personal Data.

  When is there a right to erasure?

  - The Personal Data is no longer necessary in relation to the purposes for which they were collected
  - The Data Subject withdraws consent and there is no other legal ground for the processing
  - The Data Subject objects to the processing and there are no overriding legitimate grounds for the processing
  - The Personal Data has been unlawfully processed
  - The Personal Data has to be erased for compliance with a legal obligation under EU or Member State law, or
  - The Personal Data has been collected in relation to the offer of information society services to a child

  However, the right to erasure may not be available where the processing of the relevant Personal Data is necessary:

  - For exercising the right of freedom of expression and information,
  - For compliance with an EU or Member State legal the obligation which requires processing by law to which the Controller is subject or for the performance of a task the carried out in the public interest or in the exercise of official authority vested in the Controller,
  - For certain archiving purposes in the public interest scientific or historical research purposes or statistical purposes
  - For the establishment, exercise or defence of legal claims.

  The right to erasure may also not be available where erasure would render impossible or seriously impair the achievements of research carried out in the public interest. If feasible, this point should be considered and explained to Data Subjects when they are asked to consent.

As the scope of the right to erasure is extended under e GDPR, organisations will be required to comply with a wider spectrum of erasure requests.

It is important for technology driven businesses to ensure that their database architecture facilitates deletion. As Data Controllers are also required to make reasonable efforts that information relating to a Data Subject is erased not only on their systems, but also that of third-party systems, that have copied, replicated or linked to the original information. Building in processes for notifying third parties should also be considered.

APPENDIX 2C – GDPR PRINCIPLE OF ACCOUNTABILITY

The introduction of the 'accountability principle' means that affected organisations will have to work on their internal compliance, including record keeping and, for some, the appointment of a Data Protection Officer.

In order to be able to demonstrate compliance with the GDPR, the Data Controller should implement measures which meet the principles of Data Protection by design and Data Protection by default.

Privacy by Design (Article 25)

GPDR requires that Data Protection technical or organisational measures are designed into the development of business processes for products and services which are designed to apply the Data Protection principles in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of Data Subjects. Such measures include pseudonymising Personal Data, by the Controller (Recital 78).

Technical or organisational measures *"could consist, inter alia, of minimising the processing of Personal Data, pseudonymising Personal Data as soon as possible, transparency with regard to the functions and processing of Personal Data, enabling the Data Subject to monitor the data processing, enabling the controller to create and improve security features" (GDPR recital 78)*

A. Organisational Measures

Such measures can be considered as the approach an organisation takes in assessing, developing, and implementing controls that secure information and protect Personal Data. They can include, but are not limited to:

- **Information Security Policies** – scope and content will depend on the size of the organisation and type of processing activities. Smaller firms may only require a standard information security policy; whilst more complex or larger firms may require policies in specific areas such as remote access, asset management and password controls.
- **Business Continuity** – regardless of size, all organisations should have protocols and measures in place to back-up Personal Data and ensure that it can be recovered and maintained in the event of an incident.
- **Risk Assessment** – assessing high risk data and processing activities and developing mitigating solutions to prevent or reduce risks is a preventative measure that is highly effective and, in some industries, a legal requirement.
- **Policies and Procedures** – having robust policies and procedures helps an organisation and its employees to know what their obligations are and what to do if certain situations occur. They should be easy to follow to provide intent, objectives, and guidelines for adhering to regulations.
- **Management Information & Reporting** – regular reports and information passed to upper management is essential for ensuring that the adequate resources and funding are made available for accountability at all levels.

- **Awareness & Training** – a culture of security and data protection awareness ensures that employees, contractors and any third-party working for or with the organisation, know what is expected of them and how to maintain compliance. Regular and ongoing training sessions will ensure that the latest information, guidance, legislations and regulations are known and understood.
- **Reviews & Audits** – an organisation may have all of the policies, controls and measures in place, but how does it know that they are working and are still relevant? Reviewing and auditing functions, activities and systems against procedures and regulations help to know if they are still effective and fit for purpose.
- **Due Diligence** – who you are working with is just as important as what an organisation does itself. There is little point putting extensive security and data protection measures into place if you are going to pass data to a third-party who cannot guarantee its safety or protection. Carrying out due diligence checks on suppliers and service providers (*and in some sectors, customers)*; is an essential and often legal requirement *(i.e. fraud checks, anti-money laundering measures)*

Technical Measures

Usually defined as the measures and controls afforded to systems and technological aspects of an organisation, such as devices, networks, and hardware. Protecting such aspects is vital to data security but goes above securing access to devices and systems. ***The points below are just a few of the areas that could be considered as 'technical measures' and are by no means exhaustive:***

- **Building Security** – organisations should have robust measures and protocols for securing access to any office or building and ensure that all employees are aware of such controls, which can include CCTV, security lighting and alarms. Visitors should wear ID badges and be escorted at all times and sign in/out of the building. Access to areas processing Personal Data can be further secured with biometric locks, restricted access, and access logs.
- **Disposal** – correct disposal of paperwork and devices, along with protections for those that are lost, also form part of the technical measures required by the GDPR. Shredding and certified disposal of hard-copy records is essential where Personal Data is contained in paper formats. IT departments or knowledgeable persons should be in charge of IT disposal to guarantee effective and complete erasure of any Personal Data or access.
- **Cyber Security** – this is an area too large to cover in this article, with today's technology lending itself to advanced forms of hacking, vulnerabilities, and constantly evolving threats. At the most basic level, firewalls, malware scans, anti-virus protection and patches and updates are essential on all devices and networks allowing access to confidential and Personal Data.
- **Passwords** –forcing strong passwords that are changed on a regular basis should be a standard part of the organisational approach to security. This includes employees being aware that they must not be sharing passwords or leaving systems unlocked when unattended. Password consideration should also be given to new devices, hardware and applications that often come with *'default'* logins and passwords when first used, which must be changed immediately,
- **BYOD & Remote Access** – it is quite commonplace now for employees to *'bring their own device'* to work or to use a company laptop or tablet when outside the office. These devices are often used to access the organisations network and common applications such as emails, and so must be protected, secured, and regularly reviewed.
- **Restricted access: access** to Personal Data is Personal Data restricted to authorised individuals only
- **Approved Devices:** Storing Personal Data only on your organisation's approved storage solutions and encrypted devices

- **Encryption:** Encrypting files when sending them to another organisation.

Compliance with the requirements of privacy by default and design may be demonstrated by an approved certification mechanism.
Privacy by default and design will require organisations to review their processing activities and ensure that Data Protection compliance is embedded within their products and business processes.

It is the responsibility and liability of the Data Controller to implement effective measures and be able to demonstrate the compliance of processing activities even if the processing is carried out by a Data Processor on behalf of the Controller. (Recital 74).

APPENDIX 3 - SAMPLE SCENARIOS and FAQ

A. Data Controller/Processor

Example 1: The University has many employees. It signs a contract with a payroll company to pay the wages. The University tells the payroll company when the wages should be paid, when an employee leaves or has a pay rise, and provides all other details for the salary slip and payment. The payroll company provides the IT system and stores the employees' data. The University is the Data Controller and the payroll company is the Data Processor.

Example 2: A hospital hires an IT services firm to store archived data on its behalf – having ensured that the IT firm has given sufficient guarantees about the security of its systems and processes. The hospital will still control how and why the data is used and determine its retention period. In reality the IT services firm will use a great deal of its own technical expertise and professional judgement to decide how best to store the data in a safe and accessible way. However, despite this freedom to take technical decisions, the IT firm is still not a Data Controller in respect of the hospital's data – it is a Processor. This is because the hospital retains exclusive control over the purpose for which the data is processed, if not exclusively over the manner in which the processing takes place.

Example 3: A GP surgery uses an automated system in its waiting room to notify patients when to proceed to a GP consulting room. The system consists of a digital screen that displays the waiting patient's name and the relevant consulting room number, and also a speaker for visually impaired patients that announces the same information. The GP surgery will be the Controller for the Personal Data processed in connection with the waiting room notification system because it is determining the purposes and means of the processing.

Example 4: A mail delivery service is contracted by a local hospital to deliver envelopes containing patients' medical records to other health service organisations. The delivery service is in physical possession of the envelopes but may not open them to access any of the Personal Data or other content they contain.

The delivery service will not process the Personal Data in the envelopes and packages it handles. It is in possession of the envelopes and packages but, as it cannot access their content, it cannot be said to be processing (it is not even 'holding') the Personal Data they contain. Indeed, the delivery service will have no idea as to whether the items they deliver contain Personal Data or simply other information.

This means that, regarding the content of the envelopes and packages it delivers, the delivery service is neither a Controller in its own right nor a Processor for the clients that use its services, because:

- it does not exercise any control over the purpose for which the Personal Data enclosed in the items of mail entrusted to it is used; and
- it has no control over the content of the Personal Data entrusted to it.

The Controller (the hospital) that chooses to use the delivery service to transfer Personal Data is the party responsible for the data. If the delivery service loses a parcel containing highly sensitive Personal Data, the Controller that sent the data is responsible for the loss. Therefore, the Controller will need to think carefully about the type of service that is most appropriate in the circumstances.

B. Separate Controllers

Example 1: It is the sponsor who determines what data is collected for the research study through the protocol, case report form and/or structured data fields in a database. The sponsor therefore acts as the Controller in relation to the research data. In many cases, participants will be patients and the same information may also be provided to the hospital. The hospital therefore acts as the Controller in relation to the data provided for health-care purposes. This means that there may be two Controllers for the same information – but for two different purposes. These are called Separate Data Controllers (as opposed to Joint Data Controllers).

This distinction between the purpose for which data is collected is important in determining whether the sponsor is collecting Personal Data directly from the Data Subjects (i.e. participants) or indirectly. If the purpose of the collection at the time it was obtained was only to support the delivery of care and the individual was not participating in the study, then the Controller is the hospital. If that Personal Data is then transferred to a separate research sponsor, the sponsor has obtained the data indirectly, and becomes the Controller for the processing of that data for research purposes.

It is important that you understand for your study whether Personal Data is collected indirectly from a third party or directly; when information is Personal Data; and who the Controller is, as these determine the actions you will need to take.

Example 2: Where a sponsor (B) obtains Personal Data collected previously for research purposes by a different sponsor (A), then sponsor B is obtaining the Personal Data **indirectly**. In this scenario, sponsor A is Controller for the first research activity and sponsor B is the Controller for the second research project.

If a sponsor obtains Personal Data previously collected for clinical purposes by another Controller, for example a GP practice, the information is also obtained **indirectly** from another party.

Example 3: In some cases, particularly interventional research, information will be collected from participants and recorded in both the medical records for care purposes and in the Case Report Form or equivalent for research purposes. In this situation the sponsor is obtaining the data **directly** from the Data Subject and is the Controller for processing for research (with the hospital being a Processor acting in accordance with the instructions of the sponsor). The hospital is also a Controller for processing the data for care purposes. If a sponsor re-uses for research purposes Personal Data that the sponsor previously obtained directly from a Data Subject, even if the original purpose was different, the Personal Data is still classed as being obtained directly, because it is the same Controller.

During interventional studies, participants may have tests undertaken. Any information from such tests would be Personal Data for the sponsor, even if the test results are not identifiable to those analysing the test, since the results would be associated with an identifiable individual by the sponsor or site. This Personal Data would be classed as being obtained directly, whether the test was undertaken at the site or a subsidiary site, since they would be acting as Processors on behalf of the sponsor.

C. Processing Personal Data

The sponsor is processing Personal Data if any of the data collected into case report forms, data collection tools, questionnaires, surveys, databases or other tools relates to identified or identifiable living individuals. In health and care research it is common practice to apply a unique number to each participant in a study, in order to restrict access to confidential patient information. The code list showing the participant's name or other identifying information is then stored separately from the research data. As the site will have access to the code list as well as the research data, it will be processing Personal Data. This means that even if the site only deals with Pseudonymised Data with no access to the code list, if their organisation still has the code list (even if in another department), it is processing Personal Data. While participants are taking part in the study, the sponsor may have access or has the possibility of access to the code or to personal information e.g. for monitoring and is therefore processing Personal Data.

D. Identifying the Controller

Research databases, research tissue banks and other biorepositories do not have a research sponsor. The Controller will be the organisation responsible for the management and oversight of the resource.

E. I am processing data as part of a collaborative health research project, who is the Data Controller?

If at the start of a collaborative research project, you and one or more other researcher(s) jointly determine the purposes and means of data processing, then you and those other researcher(s) (and your employing research organisations) are Joint Data Controllers.

As above, if you are a Joint Data Controller with one or more other researchers/organisations, then it is necessary to agree your respective responsibilities for compliance with GDPR. This agreement should be transparent and must identify an agreed **Data Protection contact point** to allow individuals exercise their Data Protection rights.

F. Who is the Data Controller? Is it the principal investigator or the organisation where the data is held?

A Data Controller is the individual (e.g. single GP) or the legal entity who controls and is responsible for the collection, storage and/or use of personal information. Where the Data Controller is an organisation, *e.g.* a hospital or a university, the responsibilities of the Data Controller extend to all of its employees (including *e.g.* principal investigators, academics, postdoctoral researchers, technicians, research students *etc*.) that control and are responsible for the data processing. GDPR Article 5(2) requires that the Data Controller be responsible for, and be able to demonstrate, compliance with the principles of Data Protection. Consequently, there is **both individual and organisational** responsibility to comply with the regulations. If the controller is an organisation, for example a university or hospital, it is the legal responsibility of the organisation to put in place and resource overarching frameworks, policies and procedures to enable data protection. At the same time the organisation's units, teams and employees have the obligation to operate within those frameworks, policies and procedures when processing Personal Data within the context of their employment. If employees disregard data protection measures put in place by their organisation, they could face disciplinary repercussions. The DPC will always link in with the organisation, via the DPO, and will expect the organisation to do what is necessary internally, to make any interaction between the organisation and the Data Subjects data protection compliant. In addition, under Article 82, GDPR, Data Subjects can take civil actions against controllers or processor for any damage suffered by them as a result of any infringement of the GDPR.

G. Can a university/hospital be both Data Controller and Data Processor in respect to health research?

Yes. It is not uncommon that an organisation might be both a Data Controller and a Data Processor. The Data Controller is the person or organisation who determines the purposes for which, and the way in which, Personal Data is processed (for example the hospital determines the purpose and way for the primary patient care file). By contrast, if the hospital codes patient data on instruction from a third-party controller, it may be a Data Processor, if none of its employees are involved in the research A Data Processor is anyone who processes Personal Data on behalf of the Data Controller (for example the health research project sponsor). The decision as to whether an organisation or individual is a Data Controller or a Data Processor relates to the type of data processing involved and the extent of control that the organisation or individual has over that processing.

The examples in this note have been sourced from the Irish Data Protection website, the HRB website, the UK ICO, and the UK HRA.

APPENDIX 4 – DATA PROTECTION IMPACT ASSESSMENT PROCEDURE

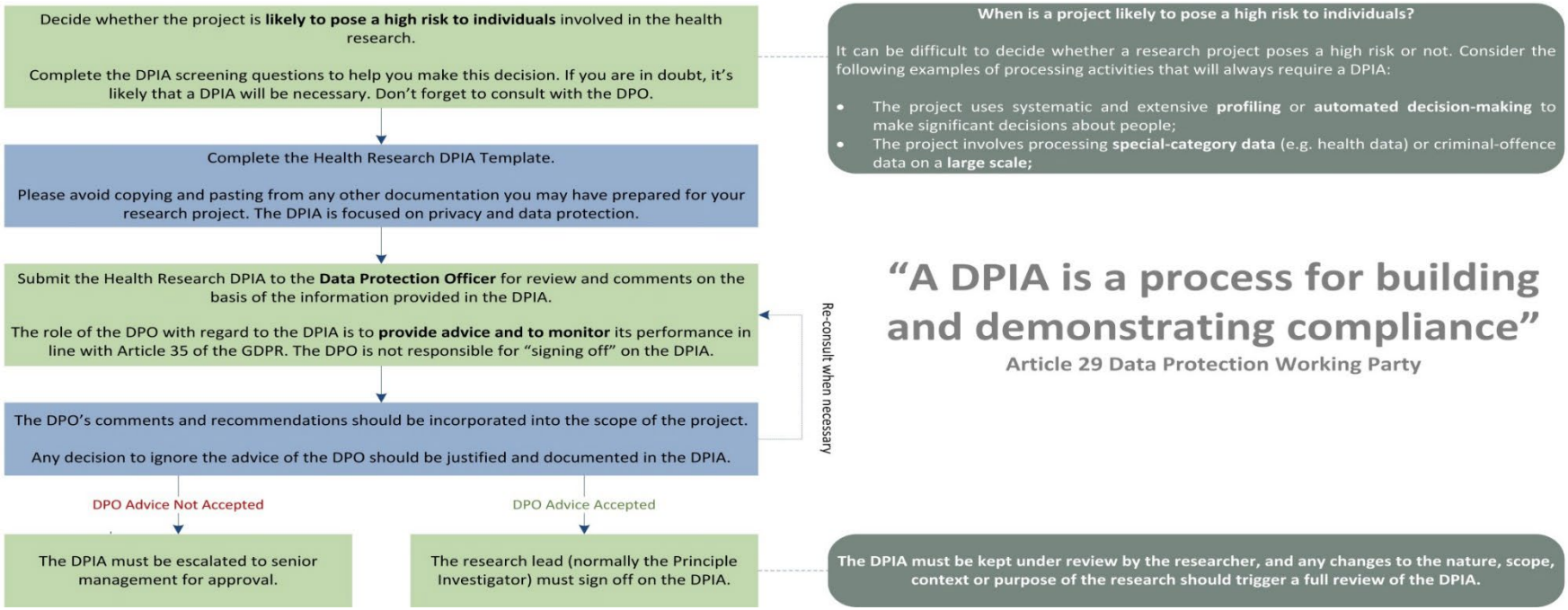
HEALTH RESEARCH DATA PROTECTION IMPACT ASSESSMENT (DPIA) PROCEDURE

A Health Research Data Protection Impact Assessment (DPIA) is a process to help researchers **identify** and **minimise** the data protection risks of a research project. You must do a DPIA for research projects that involve processing of personal data that is **likely to result in a high risk to individuals**. You can use the screening checklists to help you decide when to do a DPIA.

This Health Research DPIA Template will help you to:

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

You should consult the data protection officer (DPO) and, where appropriate, individuals and relevant experts. If there are any other organisations involved in the project, they should also be involved in completing the DPIA.

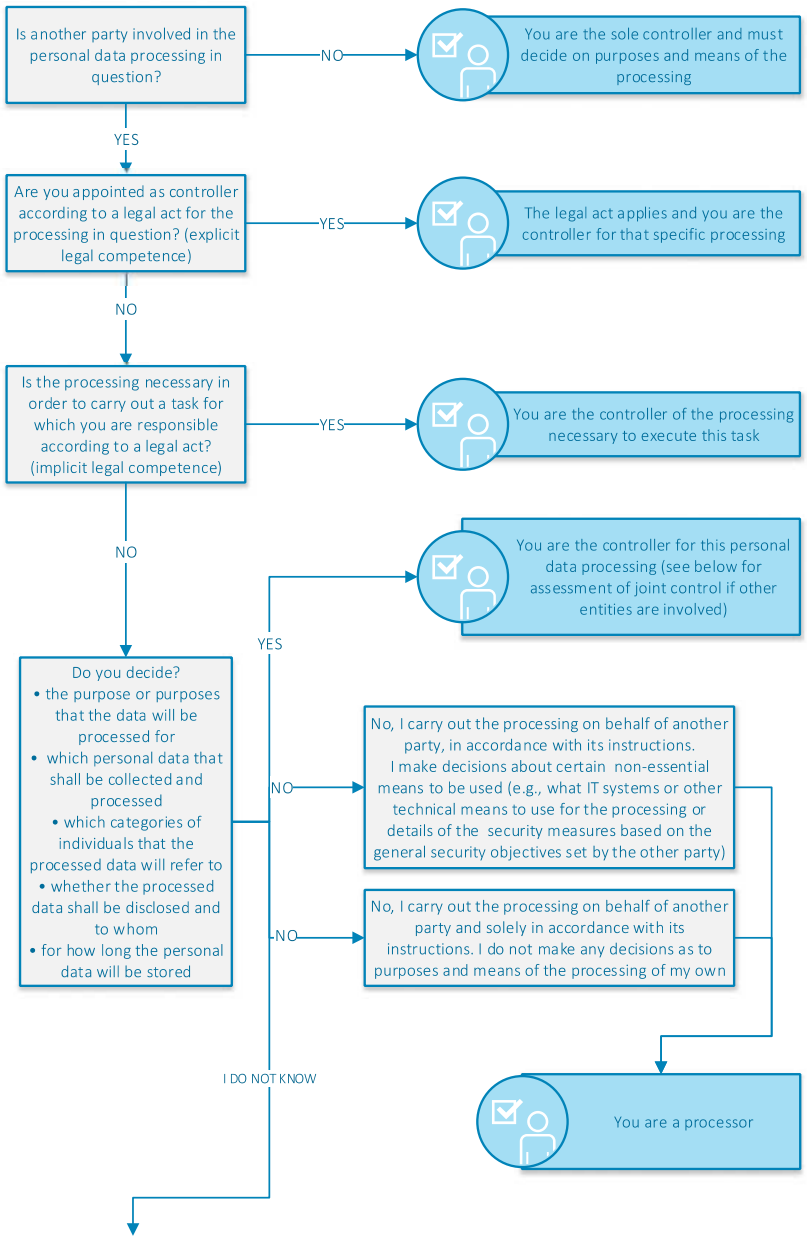


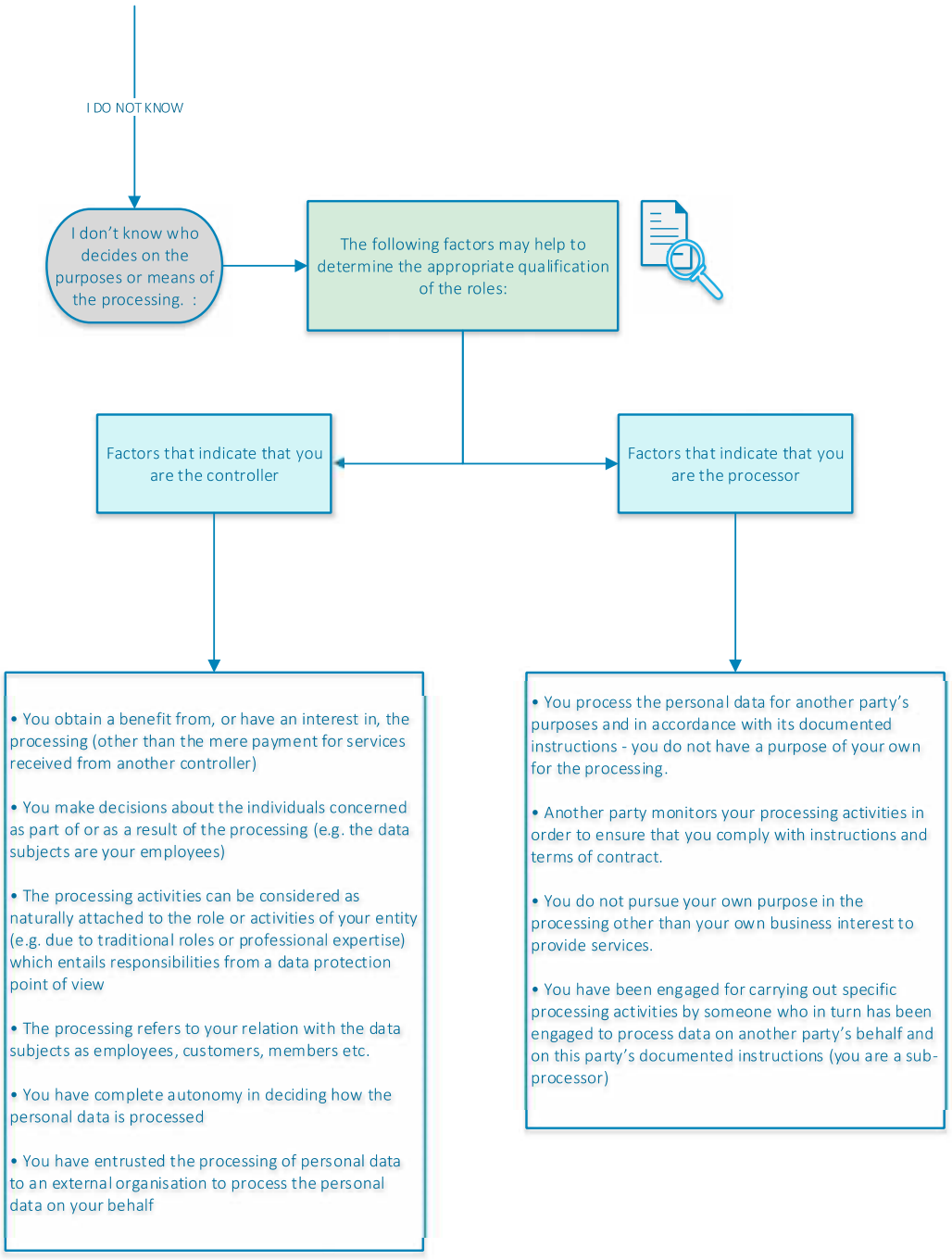
APPENDIX 5 - Flowchart for applying the concepts of controller, processor and joint controllers in practice

Source: Annex I of the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.0, Adopted on 07 July 2021 (p49-51)

Annex I – Flowchart for applying the concepts of controller, processor and joint controllers in practice

Note: in order to properly assess the role of each entity involved, one must first identify the specific personal data processing at stake and its exact purpose. If multiple entities are involved, it is necessary to assess whether the purposes and means are determined jointly, leading to joint controllership.




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
Factors that indicate that you are the processor
• 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
• 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: