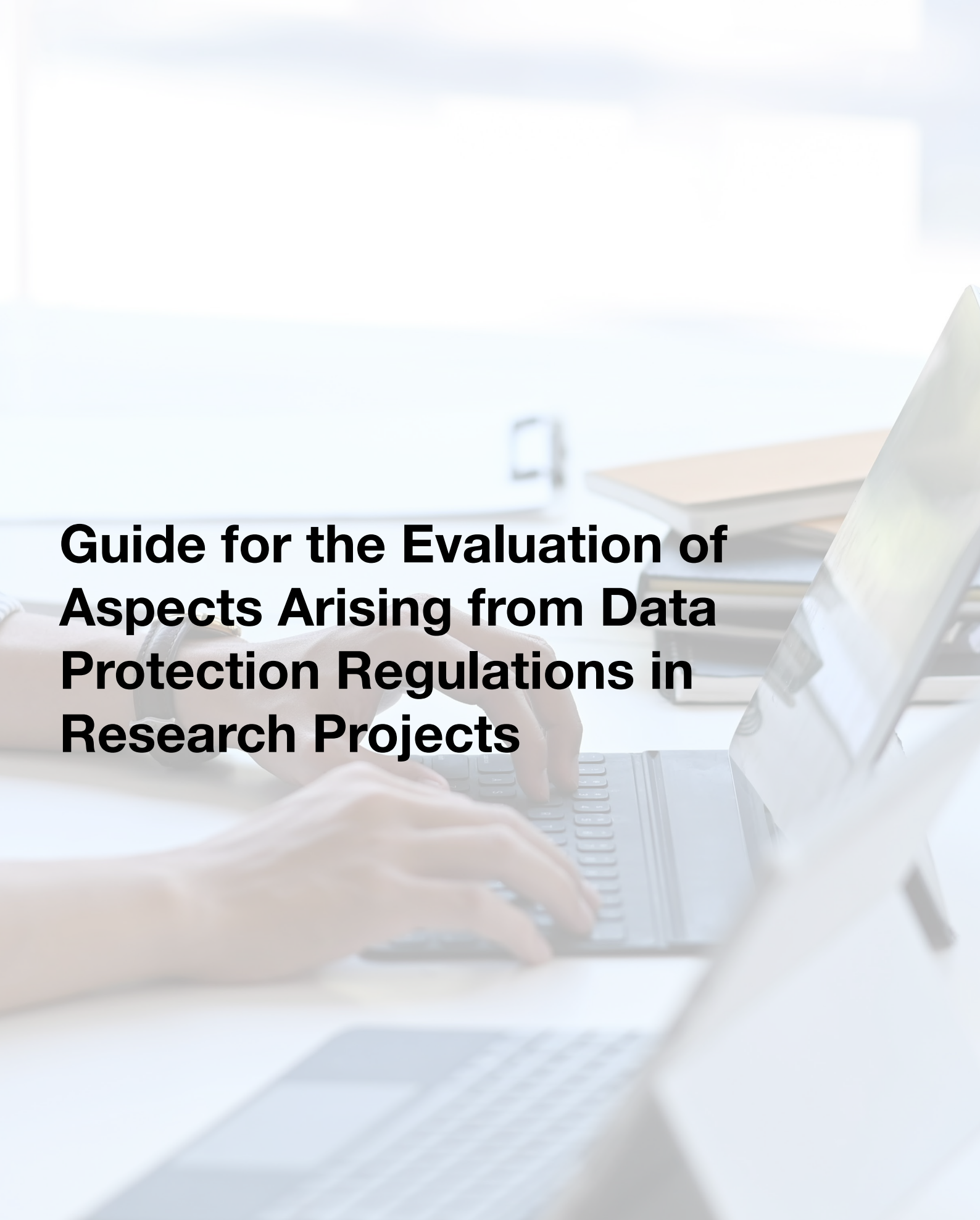




Guide for the Evaluation of Aspects Arising from Data Protection Regulations in Research Projects



**Generalitat
de Catalunya**

Some rights reserved

© 2020, Government of Catalonia. Ministry of Health.

The contents of this publication are subject to a Creative Commons Attribution–NonCommercial–NoDerivatives 4.0 International licence.

The licence can be consulted on the Creative Commons website.

Published by:

Directorate-General for Health Research and Innovation. Directorate-General for Health Planning and Regulation. DPO Office – TIC SALUT SOCIAL Foundation.

1st edition:

Barcelona, July 2020.

2nd edition:

Corporate review: December 2025
Communication Office.

Editorial registration number:

82780



SUMMARY

1.	Objectives of the Document	P. 4
2.	Introduction	P. 6
3.	Basic data-protection concepts and their interpretation in the field of research	P. 8
4.	Specific data-protection aspects in the field of research	P. 21
5.	Methodology for the Review of Personal Data Protection Aspects by Research Ethics Committees	P. 35

1.

Objectives of the Document

Five years have passed since the publication of the first version of this guide. For this reason, an updated edition has been prepared that incorporates new content and the latest criteria developed by the Research Group of the Office of the Data Protection Officer (hereinafter, DPO).

This document is an informative guide outlining the main aspects that should be considered regarding data protection when assessing research projects. It is designed for the member of research ethics committees (hereinafter, REC) responsible for data protection, for ethics committees on research with medicines (hereinafter, RECm), and for evaluation staff. It also aims to serve as a useful tool for the research team and for project managers.

To facilitate the evaluation task, it includes links to several documents that set out the main interpretative criteria and provide further information on all the topics to be assessed.

This guide comprises a first part on basic data-protection concepts applied to the field of research, and a second part covering very specific data-protection aspects related to research, such as the use of AI in research, the use of biological samples, clinical trials, and retrospective studies.

Finally, it also includes practical materials, such as a description of the elements that a research protocol must contain, the data-protection elements that must be included in an information and consent sheet, and a proposed methodology for evaluating research projects.

2.

Introduction

Carrying out a research project involves the processing of special categories of data and, therefore, the provisions of Article 9 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter GDPR), must be taken into account.

Likewise, the rules laid down in [Organic Law 3/2018, of 5 December, on the Protection of Personal Data and the Guarantee of Digital Rights](#) (hereinafter, the LOPDGDD), must be observed, in particular section 2 of the seventeenth additional provision, which develops criteria for the processing of data for research.

In addition to data-protection legislation, the specific regulations applicable to the research field must be taken into account. In this regard, the following regulatory frameworks governing the use of samples, clinical trials, or observational studies are particularly relevant, as they directly affect the data-protection regime applicable to these types of projects. Thus, the reference regulations include:

- Law 14/2007 on Biomedical Research.
- Royal Decree (RD) 1716/2011, which approves the implementing regulation of the Biomedical Research Law (hereinafter, LIB).
- Regulation (EU) 536/2014 on clinical trials on medicinal products for human use (CTR).
- Recast text of the Law on Guarantees and Rational Use of Medicines and Medical Devices, approved by Royal Legislative Decree 1/2015 of 24 July.
- Royal Decree 1090/2015 of 4 December regulating clinical trials with medicinal products, research ethics committees with medicines, and the Spanish Clinical Studies Registry.
- Royal Decree 957/2020 of 3 November regulating observational studies with medicinal products for human use.
- Royal Decree 192/2023 of 21 March regulating medical devices.

Additionally, within the package of rules adopted by the European Union under the Data Strategy, we highlight two instruments that will take effect over the coming years: on the one hand, **Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 establishing harmonised rules on artificial intelligence**; and on the other, **Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space**.

Interpretative criteria for applying data-protection law in the field of research have been established through various national and European documents, notably the following:

- EC - Guidelines on FAIR Data Management in Horizon 2020, de European Commission, 26 July 2016.
- EC - [Document Ethics and data protection, of the European Commission, 4 February 2019](#).
- EC - [Document Guidance How to complete your ethics self-assessment, of the European Commission, 14 November 2018](#).
- APDCAT - [Opinion 15/2019 concerning a query from a healthcare centre on the need for consent for the use of pseudonymised health data in biomedical research, 14 May 2019](#).
- APDCAT - [Opinion 18/2019 concerning a query from a healthcare-sector association on various aspects related to section 2 of the seventeenth additional provision of Organic Law 3/2018 of 5 December on the Protection of Personal Data and the Guarantee of Digital Rights, 14 May 2019](#).
- EDPB - [Opinion 3/2019 on questions and answers on the interplay between the Clinical Trials Regulation \(CTR\) and the General Data Protection Regulation \(GDPR\) \[Article 70\(1\)\(b\)\], adopted on 23 January 2019](#).
- EDPB - [Guidelines 03/2020 on the processing of health data for scientific research purposes in the context of the COVID-19 outbreak, adopted on 21 April 2020](#).
- APDCAT - [Opinion 14/2020 concerning a hospital's query about access to its professionals' data within the framework of a scientific study carried out at another hospital, 27 April 2020](#).
- BIOETHICS - [Report of the Spanish Bioethics Committee on the ethical-legal requirements for research involving health data and biological samples in the context of the COVID-19 pandemic, 28 April 2020](#).
- AEPD - AEPD legal report on monitoring in clinical trials.
- EDPB - EDPB document responding to the European Commission's request for clarifications on the consistent application of the GDPR, focused on health research.
- EDPB – Joint Opinion 3/2022 of the EDPB and the EDPS on the proposal for a Regulation on the European Health Data Space (EHDS).
- EDPB – Opinion 28/2024 on certain data-protection aspects related to the processing of personal data in the context of AI models.

3.

Basic data-protection concepts and their interpretation in the field of research

3.1 Types of data and application of data-protection legislation

Data-protection legislation applies “to the wholly or partly automated processing of personal data, as well as to the non-automated processing of personal data that form part of a filing system or are intended to form part of a filing system”.

Therefore, the first thing we must determine is what we understand by personal data. In this regard, data can be categorised as identified, anonymous, pseudonymised, and synthetic.

The GDPR applies to personal data, understood as information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Examples include: name, address, identification number, pseudonym, employment, email address, CV, location data, Internet Protocol (IP) address, cookie identifier, telephone number, image, or personal healthcare code (CIP).

Anonymous data are not subject to data-protection legislation. If the protocol states that the data are anonymised, the anonymisation system must be described. In this regard, the Spanish Data Protection Agency (hereinafter, AEPD) issued a document on anonymisation that provides further information: [Guidelines and guarantees in personal data anonymisation procedures](#).

This concept must be distinguished from pseudonymised data, meaning that data are considered pseudonymised when the data subject can no longer be identified without the use of additional information, which is kept separately, and a series of technical and organisational measures have been applied to prevent re-identification.

In the research context, when we talk about pseudonymised data, there must be a technical and functional separation between the research team and the persons responsible for carrying out the pseudonymisation and for retaining the information that would allow re-identification, if necessary.

If this technical and functional separation does not exist, we are dealing with what is commonly known in the research field as coding. In both cases—pseudonymisation and coding—data-protection legislation applies. Further information on pseudonymisation can be found in the AEPD report [Introducción al hash como técnica de seudonimización de datos personales](#) and in the Pseudonymisation techniques and best practices. [Recommendations on shaping technology according to data protection and privacy provisions](#) ENISA document.

Finally, there is a last category of data—synthetic data—which are artificial data generated from real data. They retain the attributes of the real data but are not identifiable data.

Therefore, when we talk about the processing of personal data, within the framework of data-protection legislation we will be thinking of pseudonymised or identified data.

The other important element of the definition is what we consider to be processing. This is understood as “any operation (or set of operations) performed on personal data, whether manual or automated”.

Examples include: accessing/consulting a database containing personal data; database management; publishing/placing a person's photo on a website; storing IP or MAC addresses; video recording (CCTV); creating a mailing list or a list of participants.

The concept of processing personal data includes any action that uses data for research purposes (including reviewing records to identify participants in a project or accessing data for the purpose of anonymising them). Personal data may come from any type of research activity (research in the ICT field, genetics, sample collection, tissue storage), personal records (education, finance, criminal, etc.), information about lifestyle and health, family histories, physical characteristics, sex and ethnicity, information about location tracking and home address, etc.

It should be remembered that, in accordance with Recital 27 of the GDPR, data-protection legislation does not apply to data of deceased persons. However, when we wish to use data of deceased persons for a research project, we must bear in mind that, if these data are obtained from the medical record, the provisions of Law 21/2000 of 29 December on

information rights concerning health and patient autonomy and on clinical documentation must be considered. This law provides that one of the uses of the medical record (hereinafter, MR) is research and, although no specific provision is made, it can be understood that data of deceased persons may be used if there is no recorded objection and the data are processed in a coded manner; that is, keeping identifying data separate from clinical care data.

3.2 Data-protection principles

Article 5 of the GDPR sets out the principles applicable to data protection. These principles guide the application of data-protection law and must therefore be borne closely in mind when interpreting the rules. Below, we set out the principles that most directly affect the field of research.

3.2.1 Principle of data minimisation

Data processing must be **lawful, fair and transparent**.

Only the data **necessary and proportionate** to perform the task or specific purpose for which they were collected should be included (Article 5(1) GDPR).

Thus, **only the data needed to achieve the research objectives should be collected**. Processing must therefore have a specific purpose that is relevant and limited to the project's objectives and methodology.

Data minimisation applies not only to the amount of personal data collected, but also to how they may be accessed, processed, and shared, the reasons for their use, and the retention period.

If the purpose of the data processing cannot be fully identified at the time of data collection, or it is necessary to retain the data beyond the duration of the project, this must be explained and justified.

For example, in a research project, if it is sufficient to record age, the exact date of birth should not be requested.

3.2.2 Privacy by design and by default

Article 25 of the GDPR introduces the concepts of privacy by design and privacy by default. The interpretation of this concept has been developed by the European Data Protection Board (hereinafter, EDPB) through [Guidelines 4/2019 on Article 25: Data protection by design and by default](#).

- **Privacy by design**

This means that the controller must implement, both at the time of determining the means of processing and at the time of the processing itself, appropriate technical and organisational measures designed to effectively implement the data-protection principles and integrate the necessary safeguards to meet the Regulation's requirements.

In this regard, the European Commission has agreed that technical and organisational measures shall be established at the early stages of designing processing operations so as to ensure privacy and data-protection principles from the outset ("data protection by design"). The use of pseudonymisation and encryption techniques are examples of privacy by design.

The AEPD has a [Guide to Privacy by Design](#) that sets out the principles to be considered.

- **Privacy by default**

Likewise, the controller must implement appropriate technical and organisational measures to ensure that, by default, only the personal data necessary for each specific purpose of the processing are processed. This obligation applies to the amount of personal data collected, the scope of the processing, the retention period, and data accessibility.

In this regard, the European Commission has established that it must be ensured that personal data are processed with the highest level of privacy protection (e.g. only the necessary data, a short retention period, and limited accessibility) so that, by default, personal data are not made accessible to an indefinite number of persons (“data protection by default”). The main manifestation of this principle in research projects would be to collect, by default, the minimum data necessary to carry out the project.

It is particularly important to guarantee these principles in research projects related to the development of technological solutions. In this regard, the Norwegian Data Protection Authority produced the document **Software development with Data Protection by Design and by Default**, which sets out the criteria that must be considered from the perspective of privacy by design and by default in software development.

3.2.3 Principle of transparency

Article 5 of the GDPR introduces the principle of transparency, meaning that personal data must be processed fairly and transparently in relation to the person concerned. This principle is linked to the information obligation under Articles 13 and 14 of the GDPR.

As a general rule, each data subject must be individually informed of the existence of data processing for research purposes, including all the points in Articles 13 and 14 GDPR.

The participant information sheet for the research project must allow for adequate information about the processing of the participant's personal data in the trial and must contain the minimum information laid down in Article 13 GDPR, in addition to other information relating to the processing of such data, which must include:

- The identity of the controller or joint controllers and before whom and how data subjects can exercise their rights.
- How to contact the data protection officer.
- A description of the purposes of the data processing and any planned disclosures, including international data transfers.
- The type of information collected and the period for which the data will be retained.
- The security measures to protect privacy and the risks to confidentiality.
- The right to know what their data are used for, who has them, to whom they may be disclosed, to request erasure from the controller, and the right to rectification where data are inaccurate or incomplete.
- The right to withdraw consent at any time and the removal of identifiable information from the health database, as well as the right to request and receive information about their data and its use.
- The right to lodge a complaint with the competent authority.
- A brief description of the security measures to protect privacy and the risks to confidentiality.

Sometimes, investigators process health data not obtained directly from the data subject but drawn from patient registries. In accordance with Article 89 GDPR, in cases of secondary use of personal data in research, information must be provided to the data subject within a reasonable period before implementing the new research project.

This information duty can only be excepted where the situations indicated in Article 14(5) GDPR apply. One such situation, for example, may arise where disproportionate effort would be required, as in cases where there is a large volume of information without contact details; even then, controllers must adopt measures that safeguard the rights of data subjects.

3.2.4 Purpose-limitation principle

Data must be collected for specified, explicit, and legitimate purposes and must not subsequently be processed in a way incompatible with those purposes. Under Article 89(1), further processing of personal data for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes is not considered incompatible with the initial purposes (purpose limitation). This principle is important because it introduces the concept of secondary use of data. In this regard, we must distinguish between the primary use of data and their secondary use.

- Primary use of data: when data are collected directly to be used for a specific purpose. For example, in the healthcare context, data may be collected in the public interest for care-related reasons, or, in the research context, data may be collected directly from participants in a scientific study with their consent.

- Secondary use of data: when data are used for a purpose different from the one for which they were initially collected. For example, data initially collected for care purposes are later reused in a retrospective observational study.

When we discuss the legal bases in the next section, we will return to the concepts of primary and secondary use.

3.3 Legal bases and scenarios for processing data in research

To use special categories of data, such as health data for research purposes, we must rely on one of the legal bases in Article 6 GDPR, and we must lift the prohibition on processing this special category of data laid down in Article 9(1) GDPR, by relying on one of the conditions in Article 9(2) GDPR, in conjunction with Article 89 GDPR. The use of these legal bases is reflected in several scenarios that permit the use of data in research and are developed through the seventeenth additional provision of the LOPDGDD.

To interpret this set of rules, Recitals 26, 28, 33, 34, 52, 53, 54, and 83 should also be taken into account. We must likewise consider various rulings by national and European data-protection authorities, which have interpreted and clarified the scope of these provisions.

These include:

- APDCAT - [Opinion 15/2019 concerning a query from a healthcare centre on the need for consent for the use of pseudonymised health data in biomedical research, 14 May 2019.](#)
- APDCAT - [Opinion 18/2019 concerning a query from a healthcare-sector association on various aspects related to section 2 of the seventeenth additional provision of Organic Law 3/2018 of 5 December on the Protection of Personal Data and the Guarantee of Digital Rights, 14 May 2019.](#)
- EDPB - [Opinion 3/2019 on questions and answers on the interplay between the Clinical Trials Regulation \(CTR\) and the General Data Protection Regulation \(GDPR\) \[Article 70\(1\)\(b\)\], adopted on 23 January 2019.](#)
- EDPB - [Guidelines 03/2020 on the processing of health data for scientific research purposes in the context of the COVID-19 outbreak, adopted on 21 April 2020.](#)
- APDCAT - [Opinion 14/2020 concerning a hospital's query about access to its professionals' data within the framework of a scientific study carried out at another hospital, 27 April 2020.](#)
- BIOETHICS - [Report of the Spanish Bioethics Committee on ethical and legal requirements in research using health data of 8 April 2020.](#)

As a starting point, it is relevant to note that the LOPDGDD itself, through its ninth final provision, has amended Law 41/2002 of 14 November, the basic law regulating patient autonomy and rights and obligations in matters of clinical information and documentation, which is considered basic legislation and regulates, among other things, access to the medical record and the purposes for which it may be used, including research. The amendment refers to the seventeenth additional provision of the LOPDGDD, which regulates the regime for the use of health data. Therefore, in interpreting this entire set of rules, the seventeenth additional provision of the LOPDGDD is of particular relevance, as it allows us to infer that the scenarios in which health data may be processed for research purposes are very broad.

To explain as clearly as possible the cases in which data may be processed for research purposes, we will provide a systematic explanation of the scenarios along with the legal bases under Article 6, the conditions that lift the prohibition under Article 9, and the provisions of the seventeenth additional provision of the LOPDGDD.

>> Regulatory framework in the health field [Articles 6(1)(c), (d), (e), and (f) + 9(2)(g), (h), (i), and (j)]

First, and through section 1 of the seventeenth additional provision, a series of scenarios are established in which the processing of health data for research purposes—set out in various national laws—may find coverage under different GDPR provisions (Articles 9(2)(g), (h), (i), and (j)), which lift the prohibition on processing special-category data, including health data, and authorise their processing. This is the list of laws set out in section 1 of the seventeenth additional provision:

- a) Law 14/1986 of 25 April, General Health Law.
- b) Law 31/1995 of 8 November on the Prevention of Occupational Risks.
- c) Law 41/2002 of 14 November, the basic law regulating patient autonomy and rights and obligations in matters of clinical information and documentation.
- d) Law 16/2003 of 28 May on the Cohesion and Quality of the National Health System.
- e) Law 44/2003 of 21 November on the Regulation of Health Professions.
- f) Law 14/2007 of 3 July on Biomedical Research.
- g) Law 33/2011 of 4 October, General Public Health Law.
- h) Law 20/2015 of 14 July on the regulation, supervision, and solvency of insurance and reinsurance entities.
- i) Recast text of the Law on Guarantees and Rational Use of Medicines and Medical Devices, approved by Royal Legislative Decree 1/2015 of 24 July.
- j) Recast text of the General Law on the Rights of Persons with Disabilities and their Social Inclusion, approved by Royal Legislative Decree 1/2013 of 29 November.

Therefore, when we operate within the scope of these laws, we must analyse whether the text of the relevant law is sufficient to authorise the processing of data for research purposes.

>> Consent [Articles 6(1)(a) + 9(2)(a) GDPR]

This first scenario allows the processing of special-category data, such as health data, based on consent. This consent must be explicit and freely given. It may only be relied upon where there is no imbalance between the parties.

In this regard, the EDPB has established that, in certain situations within the framework of clinical trials, such an imbalance may exist and, therefore, another legal basis will be required, to be determined according to the specific case. See [Opinion 3/2019 on Questions and Answers on the interplay between the Clinical Trials Regulation \(CTR\) and the General Data Protection Regulation \(GDPR\) \[Article 70\(1\)\(b\)\]](#).

This consent may be obtained to process data for a specific research project or, in accordance with letter (a) of section 2 of the seventeenth additional provision, it may be obtained to process data for purposes that cover “categories related to general areas linked to a medical or research specialty”.

This provision opens the door to requesting data to be used in several research projects.

Likewise, we must also ensure compliance with letter (f) of section 2 of the seventeenth additional provision.

>> Use for public-health research purposes [Articles 6(1)(e) + 9(2)(j) GDPR]

Letter (b) of section 2 of the seventeenth additional provision allows special-category data to be processed without the consent of the data subjects, provided that two requirements are met. First, that the processing is carried out by a health authority or a public institution competent in public-health surveillance, and second, that there are circumstances of exceptional relevance and seriousness for public health.

- To analyse this scenario, we must take into account the criteria indicated in [Guidelines 03/2020 on the processing of health data for scientific research purposes in the context of the COVID-19 outbreak](#) and [Opinion 14/2020 concerning a hospital's query about access to its professionals' data within the framework of a scientific study carried out at another hospital, 27 April 2020](#).

Likewise, we must also ensure compliance with letter (f) of section 2 of the seventeenth additional provision.

>> Reuse of data [Articles 6(1)(e) + 9(2)(j) + 89 GDPR]

The reuse of data is regulated in letter (c) of section 2 of the seventeenth additional provision and in the sixth transitional provision of the LOPDGDD (in relation to data collected before the entry into force of the LOPDGDD). This legal basis relies on Article 9(2)(j), in conjunction with Article 89 GDPR, and permits the use of data obtained with initial consent for a research

study in new projects in research areas related to the initial project. This constitutes a case of secondary use of data.

In this regard, we can see the document [*Informe del Comité de Bioética de España sobre los requisitos ético-legales en la investigación con datos de salud y muestras biológicas en el marco de la pandemia de COVID-19*](#), which reflects on the secondary use of data for research.

To rely on this scenario, the information obligation to the data subject (Article 13 GDPR) must be fulfilled and a favourable opinion from the RECM must be obtained.

Likewise, we must also ensure compliance with letter (f) of section 2 of the seventeenth additional provision.

>> Use of data in research with the safeguards set out in letter (d) of section 2 of the seventeenth additional provision [Articles 6(1)(e) and (f) + 9(2)(j) + Article 89 GDPR + letter (d) of section 2 of the seventeenth additional provision]

This scenario allows us to process data that were initially collected for a care-related purpose for research reasons, applying a series of safeguards such as pseudonymisation. This is a secondary use of data.

First, note that pseudonymisation means “the processing of personal data in such a manner that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person” (Article 4(5) GDPR).

Under the GDPR, pseudonymisation is configured as a technical measure and must be distinguished from anonymisation since, unlike the latter, pseudonymised data remain fully subject to data-protection legislation [Articles 6(4)(e), 25(1), and 32(1)(a) GDPR, among others].

The authorisation underpinning letter (d) of section 2 of the seventeenth additional provision is based on Article 9(2)(j), in conjunction with Article 89(1) GDPR, and on situations where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Article 6(1)(e) GDPR), or where it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party (Article 6(1)(f) GDPR).

In other words, we may use pseudonymised data for research purposes, in accordance with letter (d) of section 2 of the seventeenth additional provision, provided that we ensure:

- A technical and functional separation between the research team and those who carry out the pseudonymisation and retain the information enabling re-identification.
- That pseudonymised data are accessible to the research team only where:
 - i) There is an express commitment to confidentiality and not to carry out any re-identification activity.
 - ii) Specific security measures are adopted to prevent re-identification and access by unauthorised third parties.

Re-identification of the original data may be carried out where, in the course of research using pseudonymised data, there is a clear and concrete danger to the safety or health of a person or group of persons, or a serious threat to their rights, or where re-identification is necessary to ensure adequate healthcare.

However, in recent times, and given the difficulty encountered by some centres, new interpretations have emerged regarding this need for separation between the technical and functional teams, such as that put forward in [Newsletter No. 6 2024 of the National Association of Research Ethics Committees \(ANCEI\)](#). This document proposes an interpretative approach based on the principle of purpose limitation and compatible use in the processing of health data for research purposes laid down in Article 5(1)(b) GDPR.

3.4 Roles

In accordance with data-protection legislation, entities that process personal data may assume one of three roles:

- **Controller:** the party that determines the purpose of the processing and therefore bears primary responsibility for ensuring compliance with the regulations. The controller is the centre conducting the research or the sponsor.
- **Processor:** the party that processes data on behalf of the controller and must follow the controller's instructions; it is also bound by the purposes and processing parameters set by the controller.
- **Joint controllers:** parties that jointly determine the purposes and essential elements of the processing.

For example, in a clinical trial, the sponsor and the healthcare centre may be independent controllers or joint controllers, depending on how the study is structured. Thus, if they determine the project's purposes jointly, we are dealing with joint controllers.

Entities participating in a research project must always assume one of these three roles. It is essential to determine the role in which an entity acts in order to know which obligations apply and what responsibilities it has.

In the research context, **the controller of patient data is usually the hospital or healthcare centre**. Healthcare professionals at the centre who are involved in the diagnosis or treatment of the patient must have access to the medical record. Each centre must establish a mechanism that ensures that, while care is being provided to a specific patient, the professionals treating that patient can access the corresponding medical record at all times.

In addition to use for care purposes, these data may be used for research by the controller—i.e., the same hospital or healthcare centre—and the controller may therefore rely on any of the legal bases set out in Articles 6 and 9 GDPR. In the research context, the most common are the public interest in research or the data subjects' consent.

As regards the **research centre**, its statutes must be reviewed to verify the scope of its powers, which may range from managing and promoting research to actually conducting research.

If the research centre is authorised to carry out research, it may act as a controller in research projects, provided it has a sufficient legal basis to access the data. In this regard, it should be emphasised that, if it wishes to access data from the medical records held by the healthcare centre or hospital, the communication of those data must itself be legitimised so that the research centre may act as a controller.

In the relationship between the hospital and the research centre, several scenarios may arise from a data-protection standpoint:

- a)** When the research centre simply acts as manager of the research and has access to data, it becomes a processor.
- b)** Sometimes, however, the research centre may also act as a controller, provided that its statutes assign it these functions. In this case, a legal basis—such as consent—must be found that allows it to be a controller for data for which it is not the initial controller, such as hospital patient data.

In this regard, consent to participate in the research project must expressly provide for the status of controller or joint controller of both the hospital and the research centre, analogous to clinical trials, in which the hospital and the sponsor act as controllers or joint controllers.

For example, in an observational study applying for a European grant submitted by the foundation that manages the research, both the hospital and the research centre act as controllers. In that case, it must be ensured that both have a legal basis for the processing of the data, such as consent.

- c)** Finally, there are scenarios in which the data do not come from the centre's medical records, and the research centre is the sole controller. For example, studies with healthy volunteers recruited directly by the research centre, or studies using biobank samples without using additional information from medical records.

It should be remembered that access to any information relating to the patient must be strictly professional. Any other access and/or disclosure of patient data is strictly prohibited and constitutes unauthorised access, which may be subject to labour, administrative, and even criminal sanctions.

3.5 Relationships with third parties, disclosures, and international transfers

In the research context, a third party is any person or entity that is neither the patient nor the responsible physician and that obtains health data for the study.

Within a research project, sending health data to the sponsor (commercial or academic) or to a registry located outside the centre's server where they are hosted is considered a disclosure of data to third parties, even if the data are coded or pseudonymised, since in both cases the information remains identifiable to a greater or lesser extent.

Disclosure of data is a form of processing and therefore requires a lawful basis—either the data subject's consent or one of the other bases provided in Article 6 GDPR—together with one of the scenarios in Article 9 GDPR that lifts the prohibition on processing special-category data.

As regards international data transfers, this means sending data outside the European Economic Area (EU Member States plus Liechtenstein, Iceland, and Norway). In these cases, in addition to having an appropriate legal basis, it must be ensured that the disclosure is carried out under the conditions set out in Articles 44 to 50 GDPR.

Accordingly, it must first be checked whether there is an [adequacy decision](#) by the European Commission in respect of the third country, i.e., whether it has been declared to provide an adequate level of protection. If there is no adequacy decision for the specific country, the controller must adopt one of the following supplementary safeguards:

- Binding Corporate Rules.
- Standard contractual clauses adopted by the European Commission or by a supervisory authority and approved by the Commission.
- Codes of conduct.
- Certification mechanisms.

Therefore, when an international transfer must be carried out in a project, its compliance should be reviewed with the data-protection expert of the REC/RECM.

With regard to international data transfers, reference should be made to the [Royal Decree-Law 14/2019 of 31 October, adopting urgent measures for reasons of public security in the areas of digital administration, public-sector procurement, and telecommunications](#), which amends several rules applicable to public-sector entities, including Law 40/2015 of 1 October on the Legal Regime of the Public Sector, to which new Article 46 bis is added.

Article 46 bis. Location of information and communications systems the registration of data.

The information and communications systems used for the collection, storage, processing, and management of the electoral roll, municipal population registers and other population registers, tax data relating to own or assigned taxes, and data of users of the national health system, as well as the corresponding processing of personal data, must be located and provided within the territory of the European Union.

The data referred to in the previous paragraph may not be transferred to a third country or an international organisation, except where an adequacy decision has been issued by the European Commission or where such transfer is required to fulfil Spain's international obligations.

Therefore, when evaluating research projects that involve international transfers, and where Article 46 bis applies, the limitation laid down in this article must be considered and its applicability to the specific research project assessed.

3.6 Data Protection Impact Assessment

Article 35 GDPR provides that, where processing is likely to result in a high risk to the rights and freedoms of natural persons, the controller must carry out a Data Protection Impact Assessment (DPIA) that assesses, in particular, the origin, nature, particularity, and severity of the risk.

Furthermore, under letter (f) of section 2 of the seventeenth additional provision of the LOPDGDD, any research project with data carried out in accordance with Article 89 GDPR requires a DPIA whenever one of the situations set out in Article 35 GDPR applies or where so provided by data-protection authorities.

Processing is considered to present a high risk to research participants' rights and freedoms where profiling, systematic monitoring of individuals, or large-scale processing of special-category data is carried out, or where intrusive data-processing methods are used (such as tracking, surveillance, audio and video recording, geolocation tracking, etc.).

The AEPD and the Catalan Data Protection Authority (APDCAT) have published lists of processing operations that require a DPIA pursuant to Article 35(4) GDPR, together with guidance and methodologies on how to conduct them.

To determine when a DPIA is necessary, the EDPB document "[*Guidelines on Data Protection Impact Assessment \(DPIA\) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation \(EU\) 2016/679*](#)" must also be taken into account.

In this regard, the AEPD and APDCAT lists set out a series of scenarios and indicate that, if two or more of the listed situations occur, a DPIA is required.

Given the characteristics of research projects, it is highly likely that a DPIA will be necessary under Article 35(3) GDPR, since in research it is very common for two or more of the situations listed by the AEPD and APDCAT to arise.

The RECM should not carry out the DPIA itself; rather, it should verify that a DPIA exists and that its outcome does not reveal any GDPR non-compliance within the project. The controller, with the advice of the Data Protection Officer, must conduct the DPIA.

Finally, it should be noted that it is not necessary to carry out a separate DPIA for every individual research project; certain research projects may share a single DPIA. In each case, the need for a project-specific DPIA must be assessed, which will depend on the presence of unique, characteristic elements of that project—such as a high technological component (e.g., evaluation of an algorithm, the use of an app in the research project, or the use of big-data technologies).

3.7 Security in the processing of data for research purposes

Data security is regulated by Article 32 and, specifically in the research context, by Article 89 GDPR, and is closely linked to the principle of integrity and confidentiality set out in Article 5 GDPR.

In addition, Royal Decree 311/2022 of 3 May, which regulates the National Security Framework (and which, under the first additional provision of the LOPDGDD, applies to processing carried out by public-sector entities), defines security by default, meaning that IT systems must be designed to guarantee security by default, which entails the following:

- a)** The system must provide the minimum functionality required for the organisation to achieve its objectives.
- b)** Operational, administration, and logging functions must be limited to what is strictly necessary, and it must be ensured that they are only accessible to authorised persons, locations, or equipment. Where appropriate, time restrictions and designated access points may be established.
- c)** In an operational system, functions that are irrelevant, unnecessary, or even unsuitable for the intended purpose must be removed or disabled by configuration control.
- d)** The ordinary use of the system must be simple and secure, so that any insecure use requires a deliberate act by the user.

At a minimum, the data-processing system must ensure that:

- It has the technical and organisational measures necessary to safeguard the rights of research participants throughout the entire data-processing lifecycle.
- The data-processing system has the technical and organisational measures necessary to prevent unauthorised access to personal data.

Indicative security criteria to be taken into account in the research context include:

- a) Pseudonymisation, confidentiality agreements, access logs, and strict segregation of access roles.
- b) Carrying out a DPIA in accordance with Article 35 GDPR where processing may “present a high risk to the rights and freedoms of natural persons” within the meaning of Article 35(1) GDPR.
- c) Consulting the DPO and seeking advice where necessary. In this regard, all RECM must have an expert data-protection role, which may or may not coincide with the DPO.
- d) Measures adopted to protect data (including during transfers) must be appropriate and recorded in the register of processing activities.

When institutional resources are used in research projects, the institution’s security guidelines must be followed. For this reason, it is important for the institution to have a data-protection policy (Article 24 GDPR).

When external resources are used within the research project, it must be possible to verify that the tools used meet the security criteria indicated above. Some practical indications are as follows:

- If data are stored on external servers, those servers must be secure and the access-security measures must be detailed, including a description of who accesses the data, when and how they access them, and where the data are stored.
- The use of insecure commercial cloud-storage tools that do not guarantee GDPR compliance must be avoided.
- If the project processes data using non-institutional software, the code developed for applications must employ code-obfuscation techniques, especially for mobile apps, and developed applications must follow secure development methodologies.

Applying the principle of privacy by design and by default, as well as carrying out a DPIA, helps ensure that these security measures are appropriate for the data processing undertaken.

Below, and to clarify the elements to be considered for security, we set out a question-and-answer format covering the relevant aspects from a security standpoint.

3.7.1 What elements must we consider when using technological tools to process special-category data?

From a data-protection perspective, several elements must be considered when deciding to develop or use a technological tool for processing special-category data.

First, in the institutional sphere it is essential to have a data-protection policy (Article 24 GDPR) setting out the security guidelines adopted by the institution to ensure compliance.

Likewise, when innovative technologies are used to process special-category data, this entails a high risk to the rights and freedoms of research participants. In such cases, under Article 35 GDPR, a DPIA must be carried out. To conduct the DPIA, the DPIA platform is available to entities affiliated with the DPO Office.

Applying privacy by design and by default, together with conducting a DPIA, helps ensure that the security measures are appropriate for the processing undertaken.

3.7.2 What additional requirements must we consider when using external resources?

- a)** Legitimacy for data processing, third-party access, and secondary uses. It must be ensured that, if a third party has access to data (e.g., by hosting on servers), the appropriate processor agreement is in place in accordance with Article 28 GDPR, and that no secondary uses of data are carried out.
- b)** International data transfers. An international transfer of data is the sending of data outside the European Economic Area. In these cases, in addition to having an appropriate legal basis, it must be ensured that the disclosure is carried out under the conditions set out in Articles 44 to 50 GDPR. In this regard, it should be noted that the Privacy Shield (the informal agreement under data-protection legislation between the US and the EU) has recently been invalidated. This mechanism was what allowed international data transfers to the United States.

Some practical indications are as follows:

- When data are stored on external servers, those servers must be secure and the access-security measures must be detailed, including a description of who accesses the data, when and how they access them, and where they are stored.
- The use of commercial cloud-storage tools or platforms that do not guarantee GDPR compliance must be avoided. In this regard, we note that the European Union Agency for Cybersecurity (ENISA) has a report entitled “Cloud Security for Healthcare Service”, which provides a set of security and data-protection tips and best practices for using cloud services in the healthcare domain.

3.7.3 What collaborative tools can we use when processing personal data?

There are many collaborative tools and platforms for storing and sharing data, some very well known, such as Google Drive, Microsoft OneDrive, Dropbox, WeTransfer, Mega, etc.

Despite their ease of use, these tools should not be used for processing personal data (storage, publication, sharing, etc.) because they do not provide sufficient guarantees of privacy, information security, or regulatory compliance.

Under Instruction 8/2020 on the use of ICT within the Administration of the Government of Catalonia, non-corporate tools may not be used when professional solutions exist and when the information involved is confidential (personal data). Accordingly, we advise against using these tools or applications to process personal data (storage, publication, sharing, etc.) unless they have been internally approved by the department or entity. The main reasons are the lack of guarantees in terms of privacy, information security, and regulatory compliance offered by these tools in their commercial versions.

Examples of these shortcomings include loss of control over the data, possible leakage or alteration of information, the risk of unauthorised access, the absence of backups to ensure data availability, or potential non-compliance — such as international transfers to countries without an adequacy decision or appropriate safeguards, the absence of a processor agreement when a third party accesses data as part of a service (Article 28 GDPR), or the inability to fulfil data subjects’ rights under the GDPR (rights of access, rectification, erasure, objection, restriction of processing, and data portability).

However, the Cybersecurity Agency of Catalonia recommends not using the Generalitat’s Office 365 service (Teams, OneDrive, SharePoint, Power BI, etc.) for processing sensitive or confidential data unless additional security measures are applied.

Therefore, when using services from Google, Microsoft, Dropbox, or others, we recommend verifying that they are corporate tools and, if so, accessing them via the work email account. If any collaborative tool is used to process personal data, available security measures must be applied, such as encryption, two-factor authentication, proper permission management, and activity monitoring to prevent unauthorised access.

Tools for questionnaires

From a data-protection and GDPR/LOPDGDD compliance perspective, we have analysed some of the platforms most commonly used in research projects. Below we list those we consider most suitable for processing personal and/or health data, to help you choose the option that best fits the project’s needs.

Survey platforms

For surveys that involve processing special-category personal data, we recommend platforms that can be installed on the institution's local servers, such as:

- REDCap
- LimeSurvey
- EUSurvey
- QuestionPro (also offers a cloud version with data-protection guarantees)

For broader-reach surveys that do not process special-category data and do not require authentication, we recommend Microsoft Forms (using the corporate tool via the institutional account). This tool forms part of Microsoft's Office 365 suite provided by the CTTI, with a current processor agreement in place. In its corporate version, this suite of applications is certified under the National Security Framework (ENS) and ISO 27001/27018.

For clinical data collection, we recommend <https://www.clinicoverly.com/>

We advise against using commercial tools such as Dropbox, SurveyMonkey, WeTransfer, or GSuite (including Google Analytics, Google Forms, Google Cloud, Google Drive, Google Docs, etc.), and Microsoft Office, whether free commercial versions or paid, due to loss of data control, the absence of a processor agreement, or possible international transfers that may occur.

Platforms for biomedical and research data analysis:

<https://www.datashield.org/> (installed on the entities' servers)

Tools for sharing sensitive information:

- By encrypted email (sending a decryption code via a separate channel).
- Via the organisation's shared file systems.
- Via the corporate version of OneDrive (accessed with an institutional email address).

Finally, and more generally, the following information-security recommendations should be borne in mind:

- Install REDCap or similar software in on-premise environments, i.e., on servers hosted in the research entity's data processing centre (DPC).
- Identify project databases and categorise the data processed in each.
- Include only the data necessary and essential to carry out the research project and delete unnecessary data.
- Pseudonymise or anonymise data before importing them into REDCap.
- In the case of pseudonymisation, ensure proper separation of the data that would allow association with personal identifiers so that the research team has no access to them.
- Communicate and store personal data using secure encryption.
- Establish a robust, well-defined access-control system for the application database: strong password policy, secure authentication (2FA), role and privilege assignment, and least-privilege policies.
- Keep the server up to date and apply security patches.
- Protect access to the REDCap server with a firewall and set access policies to block remote connections originating outside the entity (IP filtering). Customise the REDCap server in line with the entity's security policy and user needs.
- Keep the software and dependencies updated and apply available security patches as soon as possible.
- Conduct security testing (pentesting) to identify any new vulnerabilities in the database and software (REDCap).
- Implement access-monitoring systems and maintain logs of actions performed on the data.
- Have redundancy systems and database backups in place.

4.

Specific data-protection aspects in the field of research

In the research field — particularly with new advances in information technologies — there are a number of aspects that must be taken into account. Although they should be analysed in every context, they play a particularly important role in research.

On the one hand, the data-protection implications of involving minors in research projects must be considered, as well as the specific factors to bear in mind when processing their data.

On the other hand, we find projects that incorporate elements of artificial intelligence, especially where profiling and automated decision-making are envisaged.

There are also research-specific aspects which, while not part of the data-protection framework as such, are particularly relevant when aligned with data-protection requirements — for example, the specific domains of clinical trials or the use of samples for research.

The main elements to be considered in these specific areas are set out below.

4.1 Minors in research

Processing personal data of minors in the research context is increasingly common. In this regard, Article 7.1 of the LOPDGDD provides that minors may themselves give consent for data-protection purposes from the age of 14. However, the law provides an exception for cases in which legislation requires the assistance of holders of parental responsibility or guardianship to carry out the act or legal transaction in the context of which consent for processing is requested. That is, there will be situations in which the minimum age for data-protection consent will not be the 14 years established by the law but will be ancillary and subject to the principal act's requirements.

It is often the case that consent as the legal basis for processing minors' data (Article 6(1)(a) and/or 9(2)(a) GDPR) is confused with the informed consent required for the biomedical activity to be undertaken, which is governed by the applicable sectoral regulations. This informed consent has features that are specific and distinct from consent as the legal basis for processing personal data.

A table follows with the different scenarios, depending on the context and the type of study concerned.

Scope/purpose	Scenario	Minimum age to give consent for the processing of personal data when this is the legal basis [Articles 6(1)(a) + 9(2)(a) GDPR]	Minimum age to give informed consent for the procedure	Legal references
RESEARCH	Research in general, where there is no intervention	14 years, except: >> Where the minor is not deemed intellectually and emotionally capable of understanding the scope of the intervention.	No informed consent is requested, as there is no intervention affecting their health.	- Law 41/2002, of 14 November 2002 - Law 21/2000, of 29 December 2000 - LOPDGDD - GDPR
	Clinical trials	18 years*, except: >> Over-14s* who are deemed intellectually and emotionally capable of understanding the scope of the intervention. *This is the interpretation applied by the APDCAT in its Opinion CNS 41/2020, which indicates that the general regime laid down by the legislation on patient autonomy applies, i.e., consent for the processing of their data depends on the competence to understand the scope of the intervention on their health, regardless of whether they are under or over 16 years of age.	18 years*, except: >> Over-14s* who are deemed intellectually and emotionally capable of understanding the scope of the intervention. - For minors over 12, they must also give their consent together with their legal representatives. - For minors under 12, their opinion must be heard.	- Royal Decree 1090/2015, of 4 December, regulating clinical trials with medicinal products, research ethics committees with medicines, and the Spanish Clinical Studies Registry - Law 41/2002, of 14 November 2002 - Law 21/2000, of 29 December 2000 - LOPDGDD - GDPR
	Biomedical research	18 years	18 years - Minors must participate, to the extent possible and in line with their capacities, in decision-making throughout the research process.	- Law 14/2007, of 3 July, on Biomedical Research - LOPDGDD - GDPR
	Observational studies with medicinal products	18 years	18 years	- Royal Decree 957/2020, of 3 November, regulating observational studies with medicinal products for human use - LOPDGDD - GDPR

4.2 Studies with data that incorporate elements of artificial intelligence. Profiling and automated decision-making

In studies that incorporate elements of artificial intelligence, in addition to personal data-protection legislation, the following regulations must be taken into account:

- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June establishing harmonised rules on artificial intelligence (AI Act)
- Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February on the European Health Data Space (EHDS)

Although the AI Act excludes research a priori, it is essential to take this legislation into account once actions relating to the use of AI in clinical practice are envisaged. In this sense, if the AI Act's requirements are not considered from the outset (at the design stage), it will be difficult later to incorporate, for example, AI algorithms used in research that do not comply with the Regulation.

Additionally, with regard to its scope of application, point 2.3 of the Commission Guidelines on prohibited AI practices, published on 4 February 2025, states:

30) In accordance with Article 2(8) of the AI Act, it does not apply “to any research, testing or development activity related to AI systems or models prior to their being placed on the market or put into service.” This exclusion aligns with the market-based logic of the AI Act, which applies to AI systems once they are marketed or put into service.

For example, during the research and development (R&D) phase, AI developers are free to experiment and test new functionalities that could involve techniques which, if used in consumer-facing applications, might be considered manipulative and fall under Article 5(1)(a) of the AI Act. The AI Act allows such experimentation by recognising that early-stage R&D is essential to refine AI technologies and ensure they meet ethical and safety standards before being marketed.

(31) As clarified in Recital 25 of the AI Act, it aims to support innovation and recognises the importance of scientific research in advancing AI technologies and contributing to scientific progress and innovation. Therefore, Article 2(6) of the AI Act establishes an exclusion for AI systems or models, including their outputs, developed specifically and put into service for the sole purpose of conducting scientific research and development.

For example, research into cognitive and behavioural responses to subliminal or deceptive AI-driven stimuli can provide valuable insights into human–AI interactions, forming the basis for safer, more effective AI applications in the future. Despite the prohibition established by Article 5(1)(a) of the AI Act, such research is allowed because it is excluded from the scope of the Act.

(32) However, the exclusion in Article 2(8) of the AI Act is without prejudice to the obligation to comply with the Act where an AI system is placed on the market or put into service as a result of that research and development activity. Real-world testing within the meaning of the AI Act is also not covered by this exclusion.

For example, a municipality wishing to test facial-recognition software using an RBI system in the streets during a carnival may recruit volunteers for the system to identify them in real-world conditions. Since real-world testing does not fall within the exclusion in Article 2(8) of the AI Act, the planned tests must fully comply with the requirements established for RBI systems in the AI Act, unless the system is tested in a regulated AI sandbox or under the special regime for real-world testing outside such a sandbox, as set out in Articles 60 and 61 of the AI Act.

(33) In any case, any research and development activity (even when excluded from the scope of the AI Act) must be conducted in accordance with recognised ethical and professional standards for scientific research, as well as applicable Union law (for example, data-protection legislation, which continues to apply).

That is, the AI Act is deemed to apply to tests with real data, even where they form part of research. The noteworthy aspect here is that it recognises the possibility that tests conducted with real data may be regarded as research.

In this regard, one of the innovations that has generated the greatest debate can be found in Article 27 of the AI Act: the requirement to carry out a fundamental rights impact assessment (FRIA), which should not be confused with the DPIA, although they may overlap on some points. In this context, the Catalan Data Protection Authority (APDCAT) has published its [Applied methodology for the fundamental rights impact assessment in the design and development of AI](#) for conducting this type of assessment.

However, in the health domain, this requirement applies only in very specific cases of high-risk AI systems, listed in Annex III of the AI Act, which include:

- AI systems intended to be used by, or on behalf of, public authorities to assess the eligibility of natural persons to benefit from healthcare services, or to modify or withdraw such services.
- AI services intended to be used for the assessment and triage of emergency calls made by natural persons in medical assistance services, as well as patient-triage systems in emergency departments.

Therefore, the impact of this obligation on health research projects is likely to be low.

This obligation, while it may share common ground, is independent of the need to carry out the corresponding DPIA, which—where projects use personal data and AI-based technologies—is a requirement under the GDPR.

Legal bases:

Algorithm design goes through several maturity phases during development, ranging from code creation, the collection of personal data for training, training itself, and validation.

As for lifecycle and classification, a first reference point is the TRL scale, which measures technology maturity. This scale ranges from TRL 1 to TRL 9 and covers everything from the technology's basic principles (TRL1) to successful testing in real-world environments (TRL9). The scale is used in various European research calls.

More recently, EDPB Opinion 28/2024 on certain data-protection aspects related to processing personal data in the context of AI models proposes a two-phase classification: the development phase and the deployment phase.

The development of an AI model covers all stages prior to any deployment of the model and includes, among other things, code development, collection of training personal data, preprocessing of personal data for training, and training. The deployment of an AI model covers all stages related to the use of an AI model and may include any operation carried out after the development phase.

It is crucial to determine whether the data processing performed with the AI algorithm can be considered research or should be classified differently. As a general rule, the training, validation, and testing—including testing with real data—of AI algorithms falls within the field of research.

As with any research project, personal data may be processed in these phases and, in such cases, it will be necessary to determine the legal basis for data processing in each phase, directly linked to the purpose of the processing. For the processing to be lawful, one of the legal bases under Article 6 GDPR must apply. Furthermore, where special-category data such as health data are processed, one of the exceptions in Article 9 GDPR that permits such processing must also apply.

In the health domain, this is framed as research, whether because the work lies in the development phase of an algorithm that will ultimately become a medical device, or because the data are used to conduct comparative efficacy studies against standard diagnostic tools. In such cases, the ground commonly used in the public sector is public interest for research purposes (Article 6(1)(e) + Article 9(2)(j) GDPR), in accordance with Article 89 GDPR and section 2 of the seventeenth additional provision of the LOPDGDD. However, as noted in the section on legal bases, this processing may also rely on other scenarios, such as the participant's consent.

AI in data-protection law:

The GDPR introduces two concepts — profiling and automated decision-making — which can sometimes be complex to identify but frequently occur in research projects and are particularly relevant for applying data-protection law, especially Article 22 GDPR.

Profiling occurs where the following elements are present: there is an automated form of processing, relating to personal data, and the objective is to evaluate personal aspects relating to a specific natural person (Article 4(4) GDPR).

Profiling must be distinguished from the mere classification of people, since the definition includes the element “to evaluate”, which entails analysing or making predictions about individuals.

Profiling may entail that:

- i) a decision is taken based solely on automated processing;
- ii) profiling does not involve any decision based solely on automated processing; or
- iii) profiling does not involve any decision at all.

Article 22 GDPR applies only to the first case, where the **right not to be subject to a decision based solely on automated processing is established**.

Accordingly, the key lies in the concept of an automated decision, i.e., decision-making based solely on technological means **without** human involvement — the **presence of human participation** would rule out the application of Article 22 GDPR.

To determine whether there is **human involvement**, that oversight must be **meaningful** for the decision-making process, not merely symbolic. It must be carried out by an **authorised and competent person** who has **sufficient authority to alter** the decision and who is capable of understanding all the data and taking them into account when performing the relevant analysis. In such situations, when conducting the DPIA to justify the non-application of Article 22, **the degree of human involvement in the decision-making process must be identified**.

This concept should be included as a factor in the DPIA methodology. It is necessary to determine how human participation affects the decision-making process and whether this rules out the application of Article 22 GDPR.

Therefore, the concepts of automated decision and profiling overlap, but they can occur independently. That is, automated decisions can occur without profiling, and profiling can occur without automated decisions.

We can conclude that Article 22 GDPR is applicable only when there is an automated decision that affects data subjects' rights; profiling does not always fall within the scope of this article — it will do so only where an automated decision is taken on the basis of that profiling.

In both automated decisions and profiling, aside from Article 22 GDPR, the principles in Article 5 GDPR and the legal bases must be considered. To ensure the principles are correctly applied in these situations, the [Article 29 Working Party's Guidelines on Automated Individual decision-making and Profiling](#) include an annex of good practices to ensure compliance with the Article 5 GDPR principles.

4.3 Clinical trials

When analysing the legal framework for clinical trials, both the specific rules on clinical trials and data-protection law (GDPR and LOPDGGD) must be taken into account. From the perspective of the specific rules for this area, the following must be considered:

- Regulation (EU) 536/2014 on clinical trials on medicinal products for human use (CTR).
- Recast text of the Law on Guarantees and Rational Use of Medicines and Medical Devices, approved by Royal Legislative Decree 1/2015 of 24 July.
- Royal Decree 1090/2015 of 4 December regulating clinical trials with medicinal products, research ethics committees with medicines, and the Spanish Clinical Studies Registry.

Additionally, given the complexity of interpreting the rules, we must also consider AEPD Report 038/2021 on data processing in the context of clinical trials, as well as EDPB Opinion 3/2019 on questions and answers on the relationship between the Clinical Trials Regulation (CTR) and the GDPR.

Legal bases:

As in any research project, the controllers (sponsor and centre) must have a legal basis enabling the different processing operations carried out in the trial, in accordance with Article 6 GDPR. Moreover, because health data are involved, **one of the conditions in Article 9(2) GDPR must also apply to lift the prohibition on processing health data in Article 9(1) GDPR.**

Following the EDPB's approach, we can distinguish two types of data processing during a trial:

1. Operations directly related to the research activity: these are processing activities carried out by the centre's research team and the sponsor in their respective roles as controllers, concerning the collection and processing of data relating to the trial master data archive. As the EDPB notes, in the context of trials, scientific research must be understood in line with sector standards and methodological and ethical norms, in accordance with Good Clinical Practice rules.

In this case, the EDPB indicates the following legal bases may be used:

- a)** Explicit consent of the data subject: Articles 6(1)(a) + 9(2)(a) GDPR
- b)** Task carried out in the public interest: Article 6(1)(e) + Article 9(2)(i) or 9(2)(j) GDPR
- c)** Legitimate interests of the controller: Article 6(1)(f) + Article 9(2)(i) or 9(2)(j) GDPR

From the standpoint of public-sector research centres, options (a) and (b) would apply; option (c) would, in any case, apply to the pharmaceutical industry acting as sponsor.

2. Operations related to the aim of protecting health and ensuring the quality and safety of medicinal products by generating reliable and robust data (reliability and safety purposes): the EDPB considers that the appropriate legal basis is compliance with a legal obligation by the controller (Article 6(1)(c) GDPR). This basis would apply to the fulfilment of formal and procedural obligations, including:

- the investigator's notification of adverse events to the sponsor;
- retention of the trial master file and subjects' medical records as required by national law; and
- disclosure of clinical trial data to the competent authorities in the course of an inspection.

Allocation of roles:

With regard to the roles of the various actors in clinical trials, there is currently no unanimous position at the European level. Both joint controllership between the sponsor and the hospital and the approach whereby the sponsor and the research centre are independent controllers, each with their own functions and obligations, are possible.

Choosing one option or the other will depend on the context and configuration of the trial. In this regard, it is worth noting that the Farmaindustria Standard Code favours configuring the trial with two independent controllers.

Bear in mind that, if opting for a joint-controllership arrangement, the corresponding agreement required by Article 28 GDPR must be signed.

Special consideration for monitors:

First, note that **monitors are considered processors of the sponsor**, in accordance with AEPD Report 0038/2021.

However, the monitor must access the centre's medical record in performing their legally assigned functions. In this sense, **healthcare centres are the controllers of the personal information in patients' medical records** and, therefore, what must be established is the legal basis that allows an external person to the centre to access the data necessary for verification as part of monitoring. This applies regardless of whether access occurs on site at the centre or remotely. Assessing and deciding whether such a legal basis exists is the responsibility of the controller of the medical record, i.e., the centre where the trial is conducted.

Thus, as regards the relationship between the monitor and the centre, the above-mentioned report maintains that the monitor does not act as a processor of the centre, and that the legal basis enabling the monitor's access to medical record data derives from the controller's **legal obligation** (Article 6(1)(c) GDPR).

Therefore, the confidentiality and good-practice documentation that centres require to be signed becomes part of the relationship between the centre (as controller of the medical record, which must adopt the security measures it deems necessary) and the monitor — not part of a processor relationship between the monitor and the sponsor. **Therefore, it does not become an element that the sponsor must assess and/or oppose signing.**

Third parties contracted by the sponsor:

If a third-party entity (a supplier contracted by the sponsor) accesses personal data to provide its services, even if it has been hired by the sponsor, it is necessary to assess on a case-by-case basis who is the controller of the data to which this third entity would have access. The controller must then formalise a data-processing agreement with the third party. Unlike in the case of monitoring, this situation is not covered by any legal provision of a higher rank.

Participant information rights:

As in all research projects, it is essential to inform project participants of the details required under Article 13 of the GDPR, bearing in mind that clinical-trial regulations also include additional information that must be provided. This information must be communicated in a complete, concise, clear, relevant and comprehensible manner.

From the perspective of specific clinical-trial legislation, participants must be informed of:

- The nature, objectives, benefits, implications, risks and disadvantages of the clinical trial.
- The rights and safeguards of the trial subject, in particular their right to refuse participation and to withdraw from the trial at any time without having to provide any justification and without suffering any detriment as a result.
- The conditions under which the clinical trial will be conducted, including the expected duration of the subject's participation.
- The possible alternative treatments, including follow-up measures should the trial subject decide to discontinue participation.

From the perspective of data-protection legislation, in accordance with Article 13 of the GDPR, the following must also be provided:

- Name of the processing activity.
- Data controller. In this case, the site where the trial is carried out must be identified as the controller of the identifiable data, and the sponsor as the controller of the pseudonymised data.
- Contact details of the Data Protection Officer (DPO). Both the DPO of the sponsor and that of the site must be identified, as each acts as a controller.
- Purpose of processing.
- Legal basis or lawful ground for processing. It should be noted that consent is not always the most appropriate legal basis for the various data processing activities within a clinical trial. Depending on the circumstances, public interest or compliance with a legal obligation may be more suitable.
- Other recipients to whom the data may be disclosed.
- Data-retention period. The master file of the clinical trial must be retained for at least 25 years, which therefore represents the minimum data-retention period to be indicated.
- Exercise of data-subject rights and the right to lodge a complaint with the competent authority (AEPD/APDCAT).

All this information, while it must be explained in a preliminary interview with a member of the research team, must also be set out in writing and made available to the participant.

In this regard, reference is made to [AEPD Report 040931/2019](#), which analyses the content of the Spanish Agency for Medicines and Medical Devices (AEMPS) guideline entitled Guide for the correct preparation of a model patient information sheet and informed consent form (PIS/ICF), detailing the required content of these documents from the standpoint of data processing within clinical trials.

Use of investigators' data beyond the research activity:

The processing of investigators' data for purposes not necessary to the conduct of the clinical trial — such as storage by sponsors in order to contact them for future projects — cannot rely on legitimate interest as the lawful basis. In such cases, the researcher's consent would be required.

Moreover, responsibility for informing investigators about the processing of their personal data cannot be delegated to the principal investigator, since this situation does not fall within any of the exceptions provided for by law. Accordingly, the controller — in this case the sponsor — is obliged to inform the data subjects of all the aspects required by Article 13 of the GDPR.

Retention of the trial master file:

The trial master file consists of all essential documents relating to the trial, enabling verification of its conduct and the quality of the data obtained, taking into account all the characteristics of the trial. This file must be retained for 25 years.

4.4 Use of samples for research

As previously noted, this section addresses not only the data-protection regime applicable to the data obtained from biological samples, but also the framework governing the management of biological samples themselves — which are not, strictly speaking, personal data, but rather sources from which personal data may be derived.

The regulation of sample use for research purposes can be found in the following instruments:

- Law 14/2007 on Biomedical Research (LIB).
- Royal Decree 1716/2011, approving the implementing regulation of the LIB (hereinafter, RDLIB).
- Recommendation (2016)6 of the Committee of Ministers to member states on research on biological materials of human origin (hereinafter, RecCM).

In addition, given that biological samples are considered a form of personal data, the following data-protection legislation also applies:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation — GDPR).
- Organic Law 3/2018 on the Protection of Personal Data and the Guarantee of Digital Rights.

The following sections cover: the legal grounds for using samples in research (consent and exceptions to consent), the various regimes for sample storage, how samples must be transferred between institutions, and an analysis of the implications of data-protection law for research using samples.

Use of samples for research:

As a general rule, all samples used for research purposes must be supported by the corresponding **informed consent** of the source subject, containing the information required by Article 59 of the LIB and Article 23 of the RDLIB.

Thus, as a general principle, the use of samples for research must always **be based on the subject's consent and authorised by the Research Ethics Committee (REC)**.

In certain situations, the REC may exceptionally authorise the use of samples for which consent is not available, provided specific conditions are met. This exceptional regime is set out in various provisions of the LIB and RDLIB:

CONSENT FOR THE USE OF BIOLOGICAL SAMPLES

	Requirements	Legal framework
GENERAL REGIME	All samples used for research purposes must be supported by the corresponding informed consent of the source subject, including: ● Regime of use and storage of samples (project, collection or biobank). Purpose of the research, identification of the controller and location of analyses. ● Expected risks and benefits, and the possibility of re-contacting the source subject. ● Right of withdrawal, confidentiality, and right to be informed of relevant genetic findings. ● Notification that research may yield information relevant to the subject's health and their right to receive or not receive such information, together with a reminder that these findings may also affect family members and that it may be advisable to inform them. ● Destination of the sample once the project has concluded.	Articles 4, 13, 58 and 59 of the LIB Article 23 of the RDLIB
OTHER CONSENT REGIMES	Subjects unable to write may give consent by any legally valid means that records their will.	Articles 4.1, 4.2 and 20 of the LIB
	Persons declared legally incapacitated or minors must give consent through their legal representatives, but should participate in the research process to the extent possible and, according to their age or capacity, in the decision-making process.	
EXCEPTIONS TO THE CONSENT REGIME	Research conducted in clinical emergency situations involving persons unable to give consent, provided that: ● Comparable research cannot be carried out in non-emergency subjects. ● If the research is unlikely to benefit the patient directly, it must aim to significantly improve understanding of the disease or condition to benefit others with the same condition and involve minimal risk and discomfort. These are exceptional, justified cases; once the person regains capacity, consent must be obtained.	Article 21 of the LIB
	Authorisation by the REC to use samples when obtaining consent is impossible or would involve disproportionate effort, provided that: ● No viable alternative sample set is available for the project. ● The research is of general interest. ● The research is authorised and conducted by the same institution that obtained the samples. ● If the samples are identifiable, the research would be less effective or impossible without identification. ● No explicit objection exists from the source subject or their legal representative. ● Confidentiality is guaranteed. ● The effort, time and resources required to obtain consent have been assessed.	Articles 58 of the LIB and 24 of the RDLIB
	In the case of deceased donors, with prior favourable REC opinion, samples may be used provided no express objection was recorded, consulting the subject's last wishes. If no record exists, relatives and attending professionals must be consulted to determine any opposition. If the project has clinical implications for family members, they must also be asked whether they wish to be informed of relevant findings.	Article 26 of the RDLIB
SAMPLES COLLECTED BEFORE ENTRY INTO FORCE OF THE LIB	Anonymous sample: may be used with prior REC authorisation. Identified sample: may be used with REC approval if: ● The research is of general interest. ● It would be less effective or impossible without identifiable data. ● No explicit objection exists. ● Confidentiality is guaranteed.	Transitional Provision 2 of the LIB

Regime of sample storage:

In accordance with Article 22 of the RDLIB, biological samples may be collected and used for a specific **research project**, included in a **collection**, or incorporated into a **biobank**:

- **A specific research project:** Samples preserved for use in a specific research project may only be used for that project, unless the source subject provides new express consent for their use in other projects or for incorporation into a collection or biobank.
- **A collection:** A collection is an organised, long-term set of human biological samples, preserved outside the organisational scope of a biobank and intended for biomedical research.

These samples may only be used for a defined line of research and by the institutions or persons identified in the consent document, unless new express consent from the source subject is obtained for another purpose or for transfer to a third party. It may, however, be acceptable to share samples in collaborative projects in which the collection's principal investigator participates, provided this is clearly stated in the informed-consent document.

- **Biobank:** A biobank is a non-profit establishment that holds one or more collections of human biological samples for biomedical research purposes.

Samples stored in a biobank may be used for any research authorised under the LIB, provided that the source subject — or their legal representatives, as applicable — has given consent for the sample to be stored in the biobank.

Sample-transfer agreements:

It should be noted that samples sometimes need to be used outside the centre where they were obtained. In order to send such samples externally, the sample-use regime must permit it, the patient's consent must be in place, and a Material Transfer Agreement (MTA) must be signed.

A distinction must be made between MTAs that are legally required (Articles 33 and 34 of the RDLIB) and those that, although not mandatory under law, are considered necessary to ensure proper use of the samples. Article 17 of the Recommendation CM also sets out principles governing sample transfer, which must be taken into account when interpreting Spanish legislation.

- **Mandatory MTAs:** Articles 33 and 34 RDLIB.
 - When a sample held in a biobank, collection, or project is transferred to a biobank or collection.
 - When a sample held in a biobank or collection is incorporated into a project.
- **Non-mandatory MTAs:** Article 31 RDLIB.
 - Use of biological samples obtained in other countries. The law provides that the RECM is responsible for ensuring that samples collected abroad comply with the LIB. This is the only way to guarantee compliance.
 - Sending samples to international repositories that are not biobanks or collections within the meaning of the LIB. This case is not expressly regulated, so it is likewise necessary to ensure that the sample will be treated in accordance with the minimum legal standards.
 - Multicentre studies in which samples collected under a project or collection will be used in several contexts, provided that this is foreseen in the consent.

The minimum content of such MTAs must include:

- Identification of the provider and recipient, and the legal framework governing the samples.
- Definition of the authorised uses of the samples and their final disposition once the project concludes.
- Regime for the personal data associated with the samples.

- In the case of coded samples, an obligation to communicate relevant findings.
- Costs related to obtaining the samples, to be passed on where appropriate (without profit).
- Provisions on intellectual-property rights relating to the project.

While this represents the minimum content, each MTA must be expanded and adapted to reflect the specific circumstances of the project.

Data protection in the use of samples for research:

As in all cases, from a strictly data-protection perspective, the applicable legal basis that allows the processing of data associated with the sample for research purposes must be identified.

Before addressing this point, it is worth noting that when samples are used within a biobank, ownership of the biobank often lies with the foundation or entity responsible for the research, whereas the medical records from which data are extracted belong to the hospital.

Therefore, when seeking consent for data processing, it must be borne in mind that consent for the use of samples and associated data within a biobank does not include consent to access clinical-record data for research purposes, even where such data are linked to the sample.

It should also be noted that when consent is obtained to store samples in a biobank, a minimal amount of personal data associated with the sample must be collected — since without these data the sample would have no utility.

Finally, in regulatory terms, it is important to distinguish between: the informed consent described above, which is essential for the treatment and use of the sample itself, and the data-protection consent, which serves as a lawful basis for processing personal data. Thus, there may be cases in which informed consent exists for the use of the sample, while the lawful basis for processing the associated data is not consent but another ground provided by law.

LAWFUL BASES FOR THE USE OF SAMPLES IN RESEARCH

	Requirements	Legal framework
CONSENT	General regime: permits the processing of special-category data, such as health data, on the basis of consent. Consent may only be used when it is truly freely given and there is no imbalance of power between the parties. Under the GDPR, consent may cover a broad scope without being tied to a specific project; however, as interpreted by the Article 29 Working Party, it cannot be a “blank” or open-ended consent with no limits.	Articles 6(1)(a) + 9(2)(a) GDPR; Recital 33 GDPR; and paragraph 2(a) of Additional Provision 17 LOPDGDD
	Pre-GDPR consent: There is no legal obligation to re-obtain consent provided that the personal data are used for the specific purpose for which consent was originally granted or for research areas related to the scientific field of the original project.	Sixth Transitional Provision LOPDGDD
	Minors: Consent given by individuals aged 14 or over is valid. However, if the data processing could significantly affect the minor, consent from legal representatives is required. In all cases, if the child is under 14, parental consent is mandatory, though minors over 12 should also give their assent.	Article 7 LOPDGDD
PUBLIC HEALTH	Permits the processing of special-category data, such as health data, on the basis of public interest in the field of public health. This basis applies when research is conducted by public-health authorities or institutions and only in extraordinary situations of special significance and seriousness.	Articles 6(1)(e) + 9(2)(i) or 9(2)(j) GDPR; paragraph 2(b) of Additional Provision 17 LOPDGDD
DATA REUSE	The reuse of personal data for health or biomedical research is considered lawful and compatible when, having been obtained with consent for a specific purpose, they are used for purposes or research areas related to the scientific field of the initial study. This requires a prior favourable opinion from the REC.	Articles 6(1)(e) + 9(2)(j) GDPR; paragraph 2(c) of Additional Provision 17 LOPDGDD
DATA PSEUDONYMISATION	Unlike the previous case (where pseudonymisation is not required), pseudonymised data may be used for research if certain conditions are met: ● Technical and functional separation between the research team and the team that pseudonymises the data and holds the re-identification key. ● Access to pseudonymised data by the research team only where: ○ A confidentiality and non-re-identification undertaking ○ Is in place and specific security measures are adopted to prevent re-identification or unauthorised access. However, data may be re-identified when there is a real and specific danger to the safety or health of a person or group, a serious threat to their rights, or when necessary to ensure appropriate medical care.	Articles 6(1)(e) or 6(1)(f) + 9(2)(j) + Article 89 GDPR; paragraph 2(d) of Additional Provision 17 LOPDGDD

5.

Methodology for the Review of Personal Data Protection Aspects by Research Ethics Committees

5.1. Scope of Application and Need

5.1.1 Justification of the Need

The evaluation of projects by the REC and RECM entails verifying that the project complies with data-protection legislation, and in particular with paragraph (h) of Additional Provision Seventeen of Organic Law 3/2018, of 5 December, on the Protection of Personal Data and the Guarantee of Digital Rights. Specifically, this provision states:

(h) Within one year from the entry into force of this law, research ethics committees operating in the fields of health, biomedicine or medicinal products must include among their members a data protection officer or, if none is available, an expert with sufficient knowledge of Regulation (EU) 2016/679, where they are involved in research activities that involve the processing of personal data, pseudonymised data or anonymised data.

Research projects, in compliance with the principle of privacy by design and by default established in Article 25 of Regulation (EU) 2016/679, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, must be designed in such a way that the controller ensures data privacy and applies appropriate security measures and safeguards.

However, Royal Decree 1090/2015, of 4 December, regulating clinical trials with medicinal products, research ethics committees on medicinal products and the Spanish Register of Clinical Studies, establishes in Article 3.1 that:

A clinical trial subject to this regulation may only commence once the RECM and the AEMPS have confirmed that all the following conditions are met:

[...] (d) The rights of the subject to physical and mental integrity and to privacy are respected, and personal data relating to them are protected in accordance with Organic Law 15/1999, of 13 December, on the Protection of Personal Data, and its implementing regulations, as well as with the applicable European legislation.

Consequently, when projects reach the REC/RECM, they should already include prior verification demonstrating compliance with data-protection requirements—including the corresponding Data Protection Impact Assessment (DPIA). In practice, however, it is common for the research team to omit this initial review, with the result that the REC/RECM must assess data-protection compliance during its evaluation of the project.

It is worth noting that there are more than twenty RECM in Catalonia, and in the case of multicentre projects, several of these committees may evaluate the same project — resulting in the application of diverse assessment criteria for data-protection aspects. The workload of these committees varies by centre but frequently exceeds 200 projects per year, counting both REC and RECM evaluations.

In conclusion, the resources currently allocated to project assessment from a data-protection perspective are insufficient given the complexity of applying data-protection principles in the research context and the sheer number of projects.

This situation underscores the need to establish an agile procedure ensuring a harmonised review of compliance with data-protection legislation across all projects submitted to the various REC/RECM. Such review must include the elements derived from Article 35 of the GDPR, structured as follows:

- a systematic description of the envisaged processing activities;
- an assessment of the necessity and proportionality of the processing in relation to its purpose; and
- an assessment of the risks and the measures envisaged to address them, including security measures and mechanisms to ensure personal-data protection.

Given the nature of the data processed in health-related research projects, these projects typically involve elements that present a high risk to the rights and freedoms of data subjects. It is therefore necessary to guarantee the application of a methodology that allows the main aspects derived from data-protection law to be reviewed effectively. In addition, where **deemed appropriate by the controller**, the methodology of the Office of the Health DPO should be applied for conducting DPIAs.

5.1.2 Scope of Application

This methodology applies to investigators, members of the RC and RECM, data-protection coordinators, and data controllers.

For the methodology to be effective, it is essential that the controller — as the guarantor of compliance with data-protection legislation within its sphere of responsibility — be actively involved, together with research institutes, in their role as research managers.

Each institution may decide which research projects are subject to this methodology and which are excluded.

The application of this methodology does not preclude the use of other tools that institutions may consider appropriate to ensure compliance with data-protection regulations.

5.2. Process and Structure of the Methodology

The following phases describe the process.

I. Preparation of the Protocol and Submission of the Project to the REC/RECM

The process begins when a research team prepares the documentation to be submitted to the relevant REC/RECM. At this point, in addition to the protocol, the REC/RECM must request that the research team complete the document containing the information necessary for the project to be assessed from a data-protection perspective. This document — Annex 1 — must be completed by the research team.

It is recommended that Annex 1 be made available on the REC/RECM intranet and that initial guidance be provided to facilitate its use by research teams. It is also advisable to establish a contact point to assist investigators in resolving queries relating to the project.

II. Evaluation of the Project by the REC/RECM

Project evaluators must review Annex 1 completed by the research team and identify the elements of the project that may present a risk, in order to request appropriate clarifications. In case of doubt, they may consult the data-protection expert assigned to the REC/RECM.

III. Issuance of the Opinion and Coordination with Other REC/RECM

Once the REC/RECM considers that all data-protection aspects have been satisfactorily addressed, it may issue a favourable opinion. The following consensus criteria have been agreed among the various REC/RECM regarding the evaluation of data-protection aspects in research projects:

1.Type of opinion. It is recommended not to issue opinions that are conditional on the fulfilment of the requirements listed in Annex 1, as the difficulty of verifying actual compliance may result in projects proceeding without the effective implementation of such requirements.

Where it is necessary to sign any form of legal instrument—such as a data-processing agreement or standard contractual clauses—and these are not available at the time of issuing the opinion, this should be communicated to the investigators so they can forward the information to their legal departments. The responsibility of the REC/RECM ends once the research team has been informed of the need to formalise these legal instruments, as it is the team's responsibility to ensure that all legal requirements for the project are duly processed and executed.

2. Submission of the DPIA by the sponsor. The REC/RECM must analyse the different data-processing activities carried out within the project. Accordingly, this methodology must be applied without prejudice to the DPIAs submitted by the sponsors or controllers of the project, which examine and assess the processing performed within their remit. When the sponsor or controller provides a DPIA relating to the processing under its responsibility, it may be accepted by the REC/RECM regardless of the specific methodology used, provided that the risk level identified is low.

3. Coordination with other RECM. To facilitate evaluation, when a research project has been reviewed by a REC/RECM that has applied this methodology and completed Annex 1, it should be presumed that the project's data-protection assessment is correct, without prejudice to the controller's authority to make its own determinations. Annex 1 must be shared with all other REC/RECM involved in evaluating the project.

4. Coexistence with other tools. The application of this methodology involves reviewing the basic aspects established by Article 35 of the GDPR. However, for certain projects — due to their size, international scope or complexity — the controller or the RECM itself may deem it necessary to conduct a DPIA, in line with the DPO Office's DPIA methodology or another suitable approach chosen by the controller.

The following criteria can assist the controller or the RECM in deciding whether to apply the DPIA methodology of the Office of the Health DPO:

- The project is a European multicentre study in which the evaluating centre acts as the coordinating centre.
- The project involves the validation of an artificial-intelligence or biometric-technology tool.
- The project involves the use of large volumes of data.

5. Recruitment . In the preliminary phase of a research project, the investigator must review patients' medical records to identify potential candidates and invite them to participate.

This procedure, essential for recruiting participants, entails accessing and segmenting medical-record data for non-care purposes.

Any person not involved in the patient's care may not access such data. Access must be restricted to users authorised by the centre (the data controller), such as medical personnel attending the patient or information-systems staff.

This does not preclude the RECM's responsibility to evaluate which form of contact is least invasive of the patient's privacy — for example, whether recruitment should occur during a medical visit or whether a phone call inviting participation in the research project is permissible.

In all cases, this methodology does not replace the obligation to carry out a DPIA where required by law.



Annex I:

Form to be completed

on the protection of

personal data

Project identification

Principal Investigator

Date

Annex I: Form to be completed on the protection of personal data

In this section, the proposed form that researchers must complete when designing the project for submission to the CER is reproduced, together with a brief explanation and examples that facilitate its completion and subsequent review.

1. Systematic description of data processing

An exhaustive description of the processing must be provided, as this will be the basis for assessing the necessity, proportionality, and risks of the processing. Data processing means the use made of the data.

Description of the data and the reasons for processing them

In this section, a brief explanation must be provided of which data are used for the project, how they are processed, where they come from, and where they are sent.

Example: In this project, data originating from SAP are used and incorporated into a database owned by the European Consortium. These data will include variables related to participants' heart conditions, data regarding their lifestyle habits, and their area of residence.

These data will be cross-referenced with data from other hospitals participating in the project. The data will be anonymized and will be accessible to all members of the European Consortium. The anonymization will be carried out by company XXX.

Data format

In this section, it must be indicated what form the data take: coded, pseudonymized, or anonymous. A brief explanation should be provided of how the coding, pseudonymization, or anonymization procedure is carried out. Pseudonymized data are personal data in which an attribute has been replaced with a pseudonym, meaning the individual cannot be identified without additional information. Unlike coding, the research team does not have access to this additional information. The difference between pseudonymization and coding is that pseudonymization is performed by a third party external to the research team. Anonymous or anonymized data are data that can no longer be used to re-identify the original data subject.

Description of the parties involved in data processing

In the field of data protection, we mainly distinguish between:

- 1.** Data controller: the entity that determines the purpose of the processing and, therefore, bears the primary responsibility for ensuring compliance with regulations. The data controller is the center conducting the research and/or the sponsor.
- 2.** Data processor: the entity that processes the data on behalf of the controller. It must follow the controller's instructions and is bound by the purposes and processing elements defined by the controller.

Example: In a clinical trial, the sponsor and the healthcare center act as data controllers.

Are data communications taking place?

A data communication is considered to occur when the data are processed by a third party that is not considered a data processor. It must be indicated whether the data leave the scope of the data controller.

- ☐ YES
- ☐ NO

If yes, indicate where and for what reason:

Are international data transfers taking place?

An international transfer is considered to occur when data are sent outside the European Economic Area (EU countries plus Liechtenstein, Iceland, and Norway).

☐ YES

☐ NO

Comments (if applicable):

How long will the data be retained?

The number of years or a criterion that allows the retention period to be determined must be indicated.

Example: Once the research project has been completed, the data will be retained for the time necessary to respond to any claims made by the participants in the trial.

Automated decisions and artificial intelligence

Does the processing systematically or extensively evaluate personal aspects of individuals (economic situation, health, etc.) based on automated processing, such as profiling?

☒ YES

☐ NO

Description:

Does the processing include artificial intelligence (AI) systems?

☐ YES

☐ NO

Description:

2. Necessity and proportionality

Analysis of the legal basis.

A legal basis is the ground that permits the use of personal data. To be lawful, the use of personal data must be based on one of the legal basis listed in Article 6 of the GDPR. As for health data or genetic data — which are especially sensitive — the GDPR generally prohibits their use but provides several exceptions (Article 9.2 of the GDPR), including: (1) Explicit consent, (2). Public interest in the field of public health, and (3). Research purposes (subject to certain safeguards).

Example: An oncologist decides to obtain consent from all patients under their care to use their data for research purposes in the field of oncology.

Select the reason justifying the processing of data:

- ☐ **a)** The data subject — or their legal representative — has given consent for the processing of their personal data for one or more specific purposes.
- ☐ **b)** The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller within the field of public health.
- ☐ **c)** The data were initially collected for another purpose and are being reused for research in a pseudonymised form.
- ☒ **d)** Other (please specify).

Compliance with the principle of data minimisation and accuracy.

It must be verified that only the data necessary for the project are processed.

Data used in a research project must always be adequate, relevant and limited to what is necessary. Thus, only the data required to achieve the research objectives should be processed. Collected data must respond to a specific, relevant purpose limited to the project's objectives and methodology. Data minimisation applies to the quantity and type of data collected, as well as to the way they are accessed, by whom, for what reason, and how long they are retained.

Example: In a research project, one could choose to collect the subject's exact date of birth, an age range (e.g. 30–40), or simply age in years. To comply with the principle of data minimisation, one should analyse which information is truly necessary.

- ☐ YES
- ☐ NO

Comments (if applicable):

Have you defined a strategy or a set of procedures to prevent the creation or reinforcement of unfair bias in the AI system, both in relation to the use of input data and the design of the algorithm?

- ☐ YES
☐ NO

Have you planned for human intervention to evaluate the AI system, both in the training phase and in the application phase?

- ☐ YES
☐ NO

Have you taken into account the diversity and representativeness of users in the data? Have you conducted testing for specific populations or potentially problematic use cases?

- ☐ YES
☐ NO

Have you established processes to verify and monitor potential biases during the development, deployment, and use of the system?

- ☐ YES
☐ NO

Have you ensured that the design of the AI systems is fair?

- ☐ YES
☐ NO

Description:

Justification:

3. Controls to ensure individuals' rights

Duty to inform.

At this stage, we must indicate when information about the use of data is provided—either at the time consent is obtained or, if the project does not require consent, through the information that was provided at the initial stage of data collection. In both cases, the information requirements set out in Articles 13 and 14 of the GDPR must be fulfilled.

This means that, in a research project, each participant must be informed of:

- 1.** The identity of the data controller.
- 2.** The purpose of the data processing and the data retention period.
- 3.** The exercise of participants' rights. Participants must be informed about how they can exercise their personal data protection rights (*ARSO-POL), as well as their right to lodge a complaint with the supervisory authority if they consider that their rights have been infringed.
- 4.** The identity of the Data Protection Officer (DPO). This is the natural person responsible for safeguarding the fundamental right to personal data protection and for supervising compliance with the applicable regulatory framework.

Does the collection of personal data include direct collection from the data subject?

- ☐ YES
☐ NO

Is information on all aspects set out in Article 13 of the GDPR provided?

- ☐ YES
☐ NO

Comments (if applicable):

Information to the data subject when personal data originate from other sources

Does the collection of personal data include obtaining data from other sources (i.e., not directly from the data subject)?

☐ YES

☐ NO

Is information on all aspects set out in Article 14 of the GDPR provided?

☐ YES

☐ NO

Comments (if applicable):

Exercise of rights.

In this section, it is necessary to explain how the exercise of the rights established under the GDPR is organised. The GDPR provides that data subjects may exercise the following rights before the data controller: the right of access, the right to rectification, the right to erasure (right to be forgotten), the right to object, the right to restriction of processing, and the right to data portability. When drafting the information and consent form for study participants, an email address must be provided to enable the efficient management of these rights. Generic email addresses are discouraged; therefore, a good option may be to provide the email address of the principal investigator (who must be familiar with the applicable procedures).

Has a standard procedure or protocol been established for handling requests to exercise data protection rights?

☐ YES

☐ NO

Is the response time less than thirty days?

☐ YES

☐ NO

Annex I: Form to be completed on the protection of personal data

Comments (if applicable):

Right not to be subject to automated individual decision-making (including profiling)

Is automated processing carried out that produces legal effects or similarly significant effects for individuals?

☐ YES

☐ NO

What legal basis allows this processing?

☐ It is necessary for the performance of a contract between the data subject and the controller.

☐ It is authorised by Union law or by the law of a Member State.

☐ The data subject has given explicit consent.

Comments:

Is there a procedure that allows individuals to request human intervention, express their point of view, and contest the decision?

☐ YES

☐ NO

Comments:

Are special categories of data used in automated processing?

☐ YES

☐ NO

Is there staff within the organisation with the capacity to review decisions and change them?

☐ YES

☐ NO

Comments:

If so, what legal basis allows this? *Please mark with an X.*

☐ The data subject has given explicit consent.

☐ The processing is carried out to protect the vital interests of the data subject or of another person.

Comments:

4. Data security risks

Technological environment for data processing

Where are the project data hosted? Is the database located on the institution's servers (Yes) or on the sponsor's servers (No)?

If the data are processed exclusively within the institution's environment and the database is hosted on the institution's servers, it is considered that the security measures defined by the data controller in its institutional security policy are applied.

☐ YES

☐ NO

Have appropriate access controls been established to ensure that only authorised persons can access the project information?

☐ YES

☐ NO

Does the development of the project involve any type of integration with the patient management system?

In this case, the question refers, for example, to whether SAP is connected to any kind of application that extracts data.

☐ YES

☐ NO

Are the members of the research team aware of their responsibilities regarding information security in the processing of these data?

☐ YES

☐ NO

Is the processing system certified under the National Security Scheme (Royal Decree 311/2022) or under the ISO 27001 information security standard?

This question should be addressed in consultation with a data protection expert or with the information systems department.

☒ YES

☐ NO

Will regular backups of the project data be performed?

This question should be addressed in consultation with a data protection expert or with the information systems department.

☐ YES

☒ NO

Justification:

Use of devices or applications

Are applications or devices external to the institution and the sponsor used for the development of the project?

In this section, all data processing activities carried out outside the institution's servers must be specified, along with the security measures applied.

Example: the data are hosted on an external server belonging to the sponsor.

☐ YES

☒ NO

Are applications or devices external to the institution and the sponsor used for the development of the project?

In this section, all data processing activities carried out outside the institution's servers must be specified, along with the security measures applied.

Example: the data are hosted on an external server belonging to the sponsor.

☒ YES

☐ NO

Is the use of these external applications or devices approved by the IT department?

If there is a corporate application that can perform the same functionality, it must be used in accordance with the internal policy on the use of devices and applications.

☒ YES

☐ NO

Indicate which these devices or applications are, as well as their purpose in the context of the project.

