

	Research Data Management Policy	Code: POL-ITS-2
		Version: 01
		Last version date: 1/12/2025

1. Introduction and objective

IRB Barcelona recognizes that research data are not only essential for validating scientific findings but also constitute a strategic resource that must be managed responsibly and transparently under the principles of open science. From raw measurements to processed results, images and computational models, these data form the foundation upon which knowledge is built, reproduced and shared. In this context, IRB Barcelona is firmly committed to handling all data in accordance with ethical, legal and scientific standards, ensuring they remain accessible, secure and reusable over time.

The Research Data Management Policy (RDMP) has the objective to establish a comprehensive and rigorous approach to the collection, storage, protection, sharing, and preservation of research data, aligning with the FAIR principles -Findable, Accessible, Interoperable, and Reusable- and legal frameworks such as the General Data Protection Regulation (GDPR), the Spanish Organic Law 3/2018 and other applicable regulations (hereinafter “GDPR Legal Framework”). The RDMP focuses on making publicly funded data a public good and protecting intellectual property for public benefit, following the principle of “as open as possible as closed as necessary”.

2. Scope and Applicability

This Policy applies to anyone who generates, accesses, processes, or stores research data at IRB Barcelona (“Users”). All individuals subject to this policy are required to be familiar with its contents and to ensure compliance with the standards, responsibilities, and procedures established herein, regardless of their relationship with the institute. In particular this applies to all IRB Barcelona members, including laboratory, research platformys and administration members, and including those external or affiliated members under a visiting/affiliation agreement. It also applies to external collaborators operating under IRB Barcelona frameworks.

This policy represents the first step toward establishing a comprehensive framework for research data at IRB Barcelona. It will be followed by specific action plans and operational projects aimed at implementing the new standards introduced in this document. These initiatives will focus on developing tools, standardized workflows, and institutional platforms to make compliance practical and sustainable. The goal is not to increase the workload of research groups, but to provide automation, technical support, and clear processes that facilitate adoption. The policy also reflects IRB Barcelona’s institutional commitment to ensuring data preservation, security, and traceability as core scientific assets, alongside the necessary training and support.

	Research Data Management Policy	Code: POL-ITS-2
		Version: 01
		Last version date: 1/12/2025

3. Intellectual Property Rights

All research results and data generated within the framework of research activities carried out at IRB Barcelona are considered institutional property, unless otherwise stated in written agreements. This includes know-how, inventions, discoveries, software, databases, and any other Intellectual or Industrial Property (IP) creation derived from the use of IRB Barcelona's resources, facilities, or funding. All aspects about how to deal and manage IP at IRB Barcelona are handled by the institute's Industrial and Intellectual Property regulations.

4. Handling Research Data

The management of research data at IRB Barcelona is governed by principles of scientific integrity, legal compliance, and long-term preservation of institutional knowledge.

Research data include all digital or physical information or materials collected, generated, or used during the research process—such as raw measurements, processed results, laboratory records, images, software, databases, and metadata.

These data must be accurate, complete, traceable, and stored securely to ensure their reliability and reproducibility. In addition, any use of research data belonging to or deriving from data from a third party, may also be subject to the specific terms, restrictions, and approvals stipulated by the data provider.

Members involved in research are responsible for recording and organizing Research data in a consistent and documented manner. Research data must be labeled clearly, associated with relevant project information, and stored alongside contextual metadata that ensures understanding and future reusability.

Storage must be performed using institutional systems or approved platforms that guarantee data integrity, confidentiality, and controlled access.

The use of personal devices for data handling is strongly discouraged and must comply with security protocols established in the institutional policy on device use (Processing of Personal Data and Use of Corporate and Personal Devices Policy).

Backups of Research data must be performed regularly.

Personal data —particularly sensitive data, which includes health-related information—must be protected properly following the GDPR Legal Framework. Any transmission of health related personal data (or any other of sensitive classification) must be done through secure, encrypted channels, and only authorized personnel should have access.

	Research Data Management Policy	Code: POL-ITS-2
		Version: 01
		Last version date: 1/12/2025

As an example, instead of using methods like corporate email, for sensitive personal data exchange use the specific corporate systems, i.e. Globus.

In line with the FAIR principles, Research data sharing is encouraged, provided that it does not conflict with confidentiality obligations, intellectual property rights, or ethical and legal restrictions. Before sharing, Users must assess the nature of the data, verify the absence of third-party constraints, and under the appropriate licenses. Data intended for publication must be deposited in trusted repositories and accompanied by persistent identifiers to ensure traceability.

Research data should be retained for ten (10) years. In the specific case of Research data associated with publications, this period, counting from the date of publication or the assignment of a persistent identifier —whichever comes later—, is mandatory.

The destruction or deletion of Research data must be duly authorized and carried out with full consideration of ethical, legal, and archival implications. Users leaving the institution may request copies of their Research data (including Lab Notebooks), subject to prior written approval and, if the case may be, a formal Material or Data Transfer Agreement (MTA/DTA). However, the original Research data and support system (i.e. Lab Notebook), must remain under IRB Barcelona's custody.

5. Responsibilities, rights, duties

The responsibility for Research data management during and after a research project lies with IRB Barcelona and its Users and should be compliant with codes for the responsible conduct of research.

All members of IRB Barcelona involved in research are responsible for ensuring the proper management of research data in accordance with this policy. This includes collecting, documenting, storing, securing, and, where appropriate, sharing data in line with legal, ethical, and institutional standards. Users have the right to be recognized as authors or inventors of their contributions, while also bearing the duty to report protectable results, prevent unauthorized disclosures, and comply with data protection regulations. The institution, in turn, guarantees access to training, infrastructure, and support to fulfill these obligations effectively.

Users are responsible for:

- Ensuring that all Research data—whether collected, generated, or reused—are accurately documented, securely stored, and consistently backed up using IRB Barcelona-approved systems. They must maintain clear records that allow the traceability, reproducibility, and validation of results, including proper annotation and metadata when applicable.

	Research Data Management Policy	Code: POL-ITS-2
		Version: 01
		Last version date: 1/12/2025

- All Research Data must be managed under a Data Management Plan (DMP). Each laboratory or core facility must establish a generic DMP that covers data types, storage solutions, access controls, sharing intentions, licensing, and preservation timelines in accordance with IRB Barcelona's standards and funders' requirements. A separate, project-specific DMP should only be developed if the needs of an individual project require modifications to the generic DMP .
- Complying with the GDPR Legal Framework and internal policies when handling personal data, including obtaining necessary ethical approvals and ensuring confidentiality through anonymization, pseudonymization, and secure access protocols. Users must avoid transferring such data through insecure channels or platforms not approved by the institution.
- Requesting prior authorization before sharing or publishing data that may be confidential, ethically sensitive, or protectable. Users are expected to use appropriate licensing, follow journal or repository guidelines, and ensure proper attribution and IRB Barcelona affiliation in all dissemination materials.
- Respecting institutional policies when leaving the Institute by coordinating with the relevant departments regarding the transfer or access to data, samples, or documentation, and by signing a Material/Data Transfer Agreement (MTA/DTA) if needed. Original data must always remain within IRB Barcelona unless otherwise approved.
- Lastly, Users must act in accordance with the principles of scientific integrity, ensuring that data are not falsified, misrepresented, or plagiarized, and must report any suspected misconduct through the appropriate internal channels.

IRB Barcelona is responsible for:

- Empowerment of organizational units, providing appropriate means and resources for research support operations, the upkeep of services, organizational units, infrastructures, and employee education.
- Support of established scientific practices from the beginning. This is possible through the drafting and provision of guidelines to elaborate the DMPs, monitoring, training, education and support, while in compliance with regulations, third-party contracts for research grants, institutional statutes, codes of conduct, and other relevant guidelines.
- Developing and providing mechanisms and services for the storage,

	Research Data Management Policy	Code: POL-ITS-2
		Version: 01
		Last version date: 1/12/2025

safekeeping, registration, and deposition of research data in support of current and future access to research data during and after the completion of research projects in accordance with the CERCA Data Management Strategy.

- Providing access to services and infrastructures for the storage, safekeeping and archiving of research data and records, enabling Users to exercise their responsibilities (as outlined above) and to comply with obligations to third-party funders or other legal entities in accordance with the CERCA Data Management Strategy.

Drawn up	Review	Approval
Roberto Riveiro Head of ITS Signed by: <i>Roberto Riveiro</i> 11A89FD25B7C4DC...	Cristina Horcajada Head of Innovation Signed by: <i>Cristina Horcajada</i> A9155896B1F04DA... Jorge Dominguez Head of Competitive Funding Strategy and Scientific Management Firmado por: <i>Jorge Domínguez</i> BB968C0F38494C2... Bibiana Cervelló Head of the Legal department Signed by: <i>Bibiana Cervelló</i> B084BE5AFDB14E1...	Margarida Corominas Managing Director DocuSigned by: <i>Margarida Corominas</i> 112629B0FC7244D... Francesc Posas Director Signed by: <i>Francesc Posas</i> 926AE2F621544C4...

Summary of Changes

Version	Date	Description of the modification
01	1/12/2025	Creation of the document