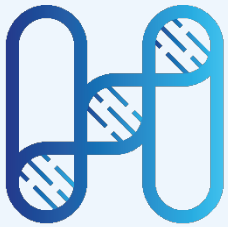

HEREDITARY

HetERogeneous sEmantic Data integratIon for the guT-bRain interplaY

Deliverable 2.1

ETHICAL GUIDELINES, DATA COLLECTION AND SHARING

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No GA 101137074. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

Funded by the European Union

EXECUTIVE SUMMARY

This deliverable examines the research ethics principles to address the legal and ethical issues arising from the research activities conducted within the HEREDITARY project. Ethics is a primary concern for researchers, and ethical standards, such as the European Code of Conduct for Research Integrity – Revised Edition 2023, are crucial for guiding research and development, especially in unregulated areas such as Artificial Intelligence (AI). Ethics plays a critical role in determining appropriate actions under conditions of uncertainty.

The development, testing, and validation of the HEREDITARY project must comply with ethical principles to respect the individuals involved and prevent harm. HEREDITARY adheres to the ethics adopted throughout the European Union (EU), embedding them in the planning, development, testing, and implementation of its socio-technical solutions. This report aims to introduce the ethical landscape applicable to HEREDITARY by analyzing relevant ethics obligations, such as the Horizon Europe ethics code of conduct, and highlighting project-specific concerns, such as the use of AI systems.

First, we discuss research ethics to provide an overview of the moral norms that researchers must respect. This includes the EU Regulation No 695/2021, which outlines the rules for participation and dissemination in "Horizon Europe – the Framework Programme for Research and Innovation".

Second, we present the ethical foundations of data protection. We provide a comprehensive overview of the legal sources that the consortium must comply with in developing the HEREDITARY project. The applicable legal framework includes international treaties such as the European Convention on Human Rights, the Convention for the Protection of Individuals regarding Automatic Processing of Personal Data (Convention 108), Convention 108+, and the Budapest Convention. The European Convention on Human Rights recognizes the right to privacy as a fundamental human right, which is further concretized by EU regulations such as the GDPR and the ePrivacy Directive.

Third, given HEREDITARY's aim to combine formal methods and reasoning techniques with inductive methods such as machine learning (ML), we discuss the ethical concerns around AI. After years of intensive international debate on the ethical and human rights implications of AI-related technologies, numerous proposals have emerged to regulate these technologies. These documents reveal a common understanding of principles, including respect for human autonomy, prevention of harm, fairness, and explicability. We focus on two key documents: the AI HLEG Guidelines on Trustworthy AI and the OECD's Recommendation of the Council on Artificial Intelligence.

This document provides a step-by-step explanation of the main data protection and ethics-related concepts relevant to the project lifecycle. These include ethical issues in using data (e.g., confidentiality, informed consent) and managing and sharing data (e.g., initial and further processing, lawful basis). We describe strategies proposed to mitigate the risks related to AI applications, particularly in healthcare settings, to discuss how all partners in HEREDITARY will address these challenges. Additionally, we attach relevant documents related to the processing of personal data within the project activities.

We consider this ethics deliverable a comprehensive set of measures aimed at ensuring compliance with ethics requirements within the HEREDITARY project. However,

maintaining compliance with ethics and legal requirements is an ongoing effort by all partners throughout the project's duration.

DOCUMENT INFORMATION

Deliverable ID	D2.1
Deliverable Title	Ethical guidelines, data collection and sharing
Work Package	WP2
Lead Partner	UNITO
Due date	30.06.2024
Date of submission	27.06.2024
Type of deliverable	R
Dissemination level	PU

AUTHORS

Name	Organisation
Adriano Chiò	UNITO
Maurizio Grassano	UNITO
Erij Kamenjasevic (Reviewer)	KU Leuven

REVISION HISTORY

Version	Date	Author	Document history/approvals
1.0	07.06.24	Adriano Chiò	First Draft
1.1	11.06.24	Erik Kamenjasevic	Revision
2.0	24.06.24	Adriano Chiò	Final

Contents

List of Tables

1 INTRODUCTION

1.1 Mapping Projects' Outputs

This report presents the findings of the ethical and legal analysis of the HEREDITARY project's research activities. HEREDITARY aims to improve disease detection, treatment response preparation, and medical knowledge exploration by developing a robust, interoperable, trustworthy, and secure framework. This framework integrates multimodal health data, including genetic information, while ensuring compliance with cross-national privacy-preserving policies.

HEREDITARY is harmonizing and linking various sources of clinical, genomic, and environmental data on a large scale. By utilizing advanced federated analytics and learning workflows, HEREDITARY aims to identify new risk factors and treatment responses. This enables clinicians, researchers, and policymakers to better understand these diseases and develop more effective treatment strategies. Adhering to the citizen science paradigm, HEREDITARY ensures that patients and the public play a primary role in guiding scientific and medical research while maintaining full control of their data.

The HEREDITARY consortium aims to develop a federated, scalable, secure, and privacy-preserving system for linking health data, enabling the querying of multimodal data across various sources and disease groups. Specifically, it will:

- Develop advanced analytics and learning methods to better understand the risk factors, causes, development, and optimal treatment for disorders related to the gut-brain interplay. In HEREDITARY, an ontology based on multilingual medical text, genomics, and other health data modalities forms the backbone for supporting multimodal, multicenter, and multidomain analyses.
- Demonstrate and realize the potential of the HEREDITARY interactive system by integrating and exploring multimodal biomedical and environmental data through five use cases targeting the gut-brain interplay with a specific focus on neurodegenerative diseases.

By achieving these objectives, HEREDITARY aims to provide a comprehensive, secure, and ethically sound approach to advancing medical research and improving patient outcomes.

1.2 Deliverable Overview and Report Structure

This report focuses on international and EU law, excluding national legislation at this stage due to the extensive analysis required across the various jurisdictions of the partners, which is beyond the scope of this document. If legal and ethical questions concerning national regulations arise, partners will refer these inquiries to their internal legal departments. Although HEREDITARY includes non-EU partners, none of these partners will provide genetic data, nor is any data transfer to a non-EU country anticipated, as further specified in the HEREDITARY Data Management Plan (see Deliverable 1.1). The Federated Networking Infrastructure ensures that sensitive data do not leave their premises. Nevertheless, we will briefly discuss the legal and ethical concerns related to non-EU member states.

This report, resulting from Task 2.1 (Legal and Ethical Guidelines for Data Collection and Sharing), aims to provide an overview of the ethical and legal framework applicable to the consortium's activities. Practical requirements of some principles will be detailed in

WP7 deliverables, which cover the legal inventory for HEREDITARY, present an in-depth legal and ethical study of the project, and provide evaluation and recommendations at the project's conclusion.

The ethical and legal frameworks identified in this report were chosen based on the scope of the HEREDITARY project, focusing on data protection, privacy law, and security relevant to the project. The aim of this report is threefold:

- To outline the ethical principles guiding research activities within the EU: These principles cover areas such as privacy, data protection, and the use of AI, which should be considered by partners involved in related activities.
- To elaborate on the international legal framework relevant to HEREDITARY: This includes an overview of laws and treaties that impact the project's operations.
- To describe the EU sources of law applicable to the project activities: This includes detailing the relevant EU legislation and regulations.

The structure of this report is as follows:

- Section 2: Provides background on the processing of personal data within the HEREDITARY project.
- Section 3: Elaborates on ethical norms applicable to research activities, offers guidelines on the ethical use of AI and ML systems, and presents the ethical foundations of data protection.
- Section 4: Describes the applicable legal framework and core principles of data protection, including international treaties and EU primary and secondary legislation.
- Section 5: Provides a step-by-step explanation of data protection obligations.

2 BACKGROUND

During the research activities and the rollout of the HEREDITARY project, personal information will inevitably be processed. Personal data within the HEREDITARY project are processed to pursue the legitimate interests of the consortium. These interests are outlined in Grant Agreement No 101137074, which the HEREDITARY Consortium signed with the European Commission (REA Agency) for a duration of four years until 31 December 2027. Additional legal rules relevant to our research activities are found in Article 89(1) of the GDPR and the European Union Regulation No 1291/2013 of 11 December 2013, establishing Horizon 2020 - The Framework Programme for Research and Innovation (2014-2020).

The internal ethical guidelines presented here are intended to assist all HEREDITARY consortium members throughout the project. They promote a shared understanding of the importance of high research standards, integrity, and adherence to guidelines concerning ethical conduct in research. Legal, ethical, and regulatory frameworks relevant to the project's outcome (i.e., technological solutions of the project) are described in more detail in the deliverables of WP7.

HEREDITARY plans the following use cases where personal data will be processed:

- **Use Case 1: Phenotyping and Prognosis Evaluation of Neurodegenerative Diseases.**
  The HEREDITARY consortium will utilize specialized knowledge extraction methods on extensive multimodal data focused on Amyotrophic Lateral Sclerosis (ALS) to infer potential correlations and conditional dependencies among diverse clinical and biological variables.
- **Use Case 2: Advancing Diagnosis and Treatment Response for Neurodegenerative Diseases.**
  Clinical diagnoses will be integrated with the functional characteristics of disease-associated genetic variants, linking them to biological and anatomical entities. This use case will investigate whether combining multimodal and genomic data can inform clinical practice towards a more molecular-based diagnosis, thereby improving patient stratification.
- **Use Case 3: Identifying Parkinson's Disease through Multimodal Data.**
  This use case aims to create classifiers that identify Parkinson's Disease (PD) patients based on ophthalmic imaging, examines associations between ocular biomarkers and other biomarkers, and leverages multimodal PD data to identify patient sub-groups.
- **Use Case 4: Characterizing the Gut-Brain Axis in Healthy Individuals to Understand Disorder Deviations.**
  This use case will provide a comprehensive evaluation of the gut-brain axis in a large, deeply phenotyped healthy population sample, which will serve as the baseline to identify disorder-related deviations. The bacterial genera relative abundance in the microbiota will be determined from fecal samples, summarizing each subject's microbial community composition and mapping metabolic functionality onto specific pathways.
- **Use Case 5: Exploring Gut-Brain Linkage and Disease Relevance.**
  The methodology outlined in Use Case 4 will be applied to existing samples from various clinical disorders.

2.1 Project's Policy and Personal Data Processing Methods

The HEREDITARY project implements numerous safeguards and proactive measures to protect patient privacy rights. The partners in the HEREDITARY project will process all personal data according to the following principles:

- *Fairness and Lawfulness*: Personal data will be processed fairly and for the purposes for which it was originally collected. The project coordinator will assess the legality of all personal data processing operations.
- *Security of Processing*: Personal data processing operations will adhere to stringent security measures, both technical and organizational. The project employs a federated network infrastructure to avoid centralizing health data and implements access control and authentication-based environments for accessing datasets containing personal data. The need-to-know principle is enforced to vet researchers involved in HEREDITARY's data processing operations. The project design prioritizes privacy and confidentiality, ensuring secure communication channels between clients and the central server.
- *Minimization*: Personal data processing will follow the principle of data minimization, ensuring that only the essential amount of data is processed. Testing of HEREDITARY technologies will be confined to specific boundaries, with pseudonymization and anonymization maintained throughout the project.
- *Data Retention Period*: Data will only be retained if there is a legal obligation or a research purpose for archiving it for contractual reasons or scientific research. Data may be retained until the end of the project, after which it will be deleted. Anonymization and minimization techniques will be applied to reduce the risk of confidentiality breaches or unintentional data exposure.
- *Third-Party Non-Disclosure*: Personal data will not be disclosed to third parties (i.e., non-consortium entities) without the explicit authorization of the individual concerned.
- *Use-Case-Based Access*: Personal data will remain within the consortium and will only be accessed by partners involved in the specific use case relevant to the individual. Partners without an interest or involvement in a use case will not have access to the personal data processed therein, adhering to the need-to-know principle.
- *No Long-Term Identification*: The project does not aim to retain personal data for extended periods or to aggregate such data for identifying individuals. Personal data processed for research purposes will primarily be used during the testing phase and deleted immediately afterwards unless otherwise specified.
- *Accuracy*: The HEREDITARY consortium will regularly review datasets containing personal data to ensure accuracy and reliability. Systems will be in place to update the information, ensuring both security and controlled access to datasets.

2.2 Rights of Data Subjects

If an individual believes their personal data is being processed by the HEREDITARY project, they have the right to request the following actions from the data controller:

- *Right to Access*: Individuals can request information regarding their personal data, including its purposes, categories, recipients, retention period, source of collection, and any transfer to non-EU countries. They are also entitled to receive a copy of their data.
- *Right to Erasure or Rectification*: Individuals may request that their personal data be amended, updated, or erased at any time.
- *Right to Restrict Processing*: Individuals can request the suspension of their data processing if the data is inaccurate, unlawfully processed, or unnecessary.

- *Right to Object*: Individuals can object to the processing of their personal data, unless the processing is conducted on public interest grounds in accordance with Article 89(1) of the GDPR.
- *Right against Automated Decision-Making or Profiling*: Individuals have the right not to be subject to automated decision-making processes, including profiling, that result in legal consequences for them.
- *Right to Lodge a Complaint with a Supervisory Authority*: Individuals have the right to file a complaint with a supervisory authority if they believe their data protection rights have been violated.

2.3 Embedding Privacy within the Consortium

The HEREDITARY project values privacy and data protection as both a legal requirement and an ethical standard. To ensure ongoing compliance with privacy standards, the project undertakes the following actions and initiatives:

- *Adherence to GDPR*: HEREDITARY strictly follows the General Data Protection Regulation (GDPR) and its obligations within the scientific research domain. Activities involving personal data processing for scientific research are continuously evaluated against individuals' rights and legal obligations under the GDPR.
- *Accountability*: The HEREDITARY consortium maintains and regularly updates internal policies to keep records and documentation of personal data processing operations. This includes assessing risks to individuals' rights and freedoms during research, identifying mitigation measures, and implementing safeguards against privacy violations. These processes will be documented in the Data Protection Impact Assessment (DPIA) incorporated in the revised Data Management Plan (D.1.2).
- *Awareness Raising*: Consortium partners are regularly informed about data protection obligations and standards. This includes periodic activities such as webinars, presentations, and ad-hoc sessions on privacy, data protection, and respect for fundamental rights in research activities. Privacy sessions are organized during every face-to-face general assembly of the consortium. A webinar discussing privacy guidelines included in this deliverable has been held on 27 May 2024.
- *Ethical Standards*: HEREDITARY considers personal data protection obligations as an ethical standard of best practice beyond mere legal compliance. Privacy is implemented and assessed as a by-design principle in the development of technology and its integration within use-case scenarios.
- *Guidance from Ethical Guidelines*: The HEREDITARY project extensively uses ethical guidelines issued by the European Commission as benchmarks and codes of conduct. These guidelines inform researchers and projects funded under HORIZON and similar EU programs about best practices for processing personal data in research.

3 ETHICS

3.1 Overview

The EU commission introduces ethics as a fundamental key within its Horizon 2020 Research and Innovation Programme. The European Code of Conduct for Research Integrity aims to guide researchers in their work with the practical, ethical and intellectual challenges of the research process and describes good research practices for research activities.

All activities in the HEREDITARY project will comply with ethical principles and relevant national, EU and international legislation. This means that HEREDITARY adheres to the ethical standards adopted throughout the EU, embedding them in the planning, development, testing, and implementation of its technical solutions. The purpose of this section is to introduce the ethical landscape of HEREDITARY by analyzing relevant sources of moral obligations and highlighting areas of concern within the project, such as the use of AI techniques.

This section is structured as follows:

- *Research Ethics*: An overview of the moral norms that researchers must respect when conducting their activities.
- *AI Ethics*: A discussion on the ethical issues surrounding AI, particularly as HEREDITARY plans to utilize advanced federated analytics and learning workflows. State-of-the-art AI tools and methods will be developed by the technical partners, necessitating a broad discussion on AI ethical concerns to inform the consortium.
- *AI in Healthcare*: The ethical challenges of translating AI into the healthcare setting.

3.2 Research Ethics

Throughout the development of HEREDITARY, particular attention must be given to upholding fundamental norms of ethical research. This section introduces the sources of these relevant norms and summarizes the principles that should be central to research activities conducted within the EU.

Under Article 19 of Regulation 695/2021[1], all research and innovation activities of Horizon Europe projects must comply with ethical principles. This section examines the principles relevant to the research activities outlined in the proposal. Ethical principles are inherently broad and comprehensive, which may lead to some overlap with other sections of this report.

To understand the ethics of HEREDITARY, it is crucial to start from the sources of applicable ethical principles. This section examines the European Code of Conduct for Research Integrity (ECCRI) and the European Commission Decision C(2020)1862 of 25 March 2020. The following paragraphs examine each of these sources.

Article 1 of the European Code of Conduct for Research Integrity (ECCRI) outlines four ethical principles that the consortium must adhere to, as they are fundamental to ethical research:

[1] Regulation (EU) No 1290/2013 of the European Parliament and of the Council of 11 December 2013 laying down the rules for participation and dissemination in "Horizon2020 - the Framework Programme for Research and Innovation (2014-2020)" and repealing Regulation (EC) No 1906/2006, OJ L 347, 20.12.2013, p. 81.

- *Reliability*: Ensuring the quality of research is reflected in the design, methodology, analysis, and use of resources.
- *Honesty*: Conducting, reviewing, reporting, and communicating research in a transparent, fair, complete, and unbiased manner.
- *Respect*: Valuing colleagues, research participants, society, ecosystems, cultural heritage, and the environment.
- *Accountability*: Being responsible for the research from conception to publication, including its management, organization, training, supervision, mentoring, and broader impacts.

The ethical aspects of research practices have a particular significance in the European legal framework as the EU is founded on a common ground of shared values as laid out in the European Charter of Fundamental Rights[2], which contains important principles that should inspire the activities of HEREDITARY partners. While a more detailed discussion of the relevant ethical issues is provided in WP7, it is necessary to describe the ethical principles enumerated in this document that might be relevant to HEREDITARY's activities.

The most salient overarching ethical principles include:

- Respect for human dignity and integrity
- Ensuring honesty and transparency towards research subjects
- Respecting individual autonomy and obtaining free and informed consent
- Protecting vulnerable individuals
- Ensuring privacy and confidentiality

These principles should guide all activities carried out in HEREDITARY. Many of these principles, such as privacy, are also part of the legal framework applicable to the project. Consent from the subjects involved in the project is crucial to uphold the highest ethical standards. Whenever it is required or possible to obtain it, consent plays an important role in various aspects of research, from recruiting participants to establishing the legal basis for processing personal data. The role of consent is crucial in clinical research, and its requirement also extends to other areas, such as data protection.

The basic elements of consent relevant to HEREDITARY can be summarized as follows:

- *Freedom*: Subjects must be in a situation where they do not fear undesirable consequences if they refuse to participate in the research. Real free choice cannot be made when external pressure is exerted on participants, especially if they are in a subordinate position to the entity promoting the research.
- *Specificity*: Subjects must be able to clearly understand the research activities they are consenting to, including the purpose, duration, description of procedures, and research activities.
- *Informed*: Subjects must be informed about the possible implications of the research, including expected benefits, risks, and mitigation strategies. For data protection, informed consent is ensured by describing the purpose, duration, and policies to respect data protection regulations.

Lastly, European Commission Decision C(2020)1862 of 25 March 2020[3] is part of the work programme for Horizon concerning science with and for society. This document references the responsible research and innovation (RRI) framework, which cuts across

[2] Charter of Fundamental Rights of the European Union, Official Journal of the European Union (30.3.2010) No. C 83/389 – 403.
[3] https://ec.europa.eu/research/participants/data/ref/h2020/wp/2018-2020/main/h2020-wp1820-swfs_en.pdf

all Horizon research activities. The Commission regards RRI as a process for better-aligning research and innovation with the values, needs, and expectations of society. The RRI framework aims to avoid irresponsible innovation characterized by:

- Technology push: Introducing technological innovations to the market without prior consultation or suitable deliberative mechanisms.
- Negligence of fundamental ethical principles
- Policy pulls: Drawing technologies from research for political reasons.
- Lack of precautionary measures and technology foresight

These instances prevent innovation activities from being responsible. Some of the strategies usually adopted to promote RRI include:

- Technology assessment and oversight
- Application of the precautionary principle
- Multi-stakeholder engagement
- Codes of conduct
- Standards, certifications, and self-regulation
- Ethics by-design approach

3.3 Artificial Intelligence Ethics

HEREDITARY leverages and advances the latest developments in federated learning and machine learning methods, which have proven effective for making inferences from multimodal data with minimal or no human supervision. Specifically, unsupervised and self-supervised learning approaches will be fundamental in creating effective data representations across various domains, including text, images, sequences, and genomics. Thus, this section will first assess whether the tools developed by the consortium qualify as artificial intelligence. Secondly, it will provide an overview of the expanding subfield of applied ethics related to AI.

Although there is no universally accepted binding AI definition, the Communication from the Commission on Artificial Intelligence for Europe (25.04.2018 COM(2018) 237) states that: “Artificial Intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals”[4]. The high-level expert group on artificial intelligence of the Commission (AI HLEG) expanded the above definition of AI. Indeed, the in the Ethics Guidelines for Trustworthy AI: “Artificial Intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge or processing the information, derived from the data and deciding the best action(s) to achieve a given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behavior by analysing how their environment is affected by their previous actions […]”[5].

The recent EU AI Act[6] provide a clearer definition of AI, stating that "AI system means software that is developed with one or more of the techniques and approaches listed ([a] machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning; [b] logic- and

[4] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Artificial intelligence for Europe COM/2018/237 final

[5] Available at: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

[6] Artificial Intelligence Act, Corrigendum, 19 April 2024, Interinstitutional File: 2021/0106(COD)

knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems; [c] statistical approaches, Bayesian estimation, search and optimization methods) and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with.

The rapid increase in AI applications has spurred numerous contributions concerned with the ethical requirement for its good use. The next paragraphs expose the high-level core principles of ethical AI that ought to inspire the consortium.

The AI HLEG's Ethics Guidelines for Trustworthy AI emphasize the need for ethical AI as one of three key components to build trustworthiness in AI, alongside lawfulness and robustness. The Guidelines advocate for AI systems to be human-centric, aimed at serving humanity and enhancing human welfare and freedom. This approach focuses on maximizing the positive outcomes of AI systems while minimizing their risks to prevent harm. In alignment with these guidelines, the consortium is dedicated to these objectives, as demonstrated by the tasks devoted to the ethical assessment of the sociotechnical solution. The ethical manager should be involved in evaluating different architectural choices of the systems to select the option least likely to have a negative ethical impact.

The AI HLEG bases ethical AI on the respect for fundamental rights enshrined in international human rights law, the EU treaties, and the EU Charter. These legal sources will be analyzed in more detail below. The core of the four ethical principles is human dignity, reflected in the human-centric approach adopted by the expert group. These principles, considered ethical imperatives, are:

- *Respect for Human Autonomy*: In practice, this principle means that humans interacting with AI systems must retain full and effective self-determination. AI systems should not unjustifiably subordinate, coerce, deceive, manipulate, condition, or herd humans.
- *Prevention of Harm*: This principle mandates that AI systems and their operating environments must be safe and secure. They must be technically robust and should not cause or exacerbate adverse impacts due to power or information asymmetries, such as those between businesses and consumers or governments and citizens. Preventing harm also involves considering the natural environment and all living beings.
- *Fairness*: Fairness implies a commitment to ensuring an equal and just distribution of both benefits and costs, and to protecting individuals and groups from unfair bias, discrimination, and stigmatization. The procedural aspect of fairness includes the ability to contest and seek effective redress against decisions made by AI systems.
- *Explicability*: Explicability requires that AI processes be transparent, the capabilities and purposes of AI systems be openly communicated, and decisions be explainable to those directly and indirectly affected, to the extent possible.

The Recommendation of the Council on Artificial Intelligence by the OECD (OECD/LEGAL/0449[7]) reinforces and expands upon the principles outlined in the AI HLEG Guidelines, aiming to establish a framework for trustworthy AI through ethical, legal, and technical guarantees. The OECD's relevant principles include:

- Inclusive growth, sustainable development, and well-being
- Human-centered values and fairness
- Transparency and explainability

[7] https://oecd.ai/assets/files/OECD-LEGAL-0449-en.pdf

- Robustness, security, and safety
- Accountability
- Human agency and oversight
- Privacy and data governance
- Diversity, non-discrimination, and fairness
- Societal and environmental well-being

The scope of these principles is broader than that of the AI HLEG due to the wider mandate of the OECD. However, to achieve the highest levels of ethical acceptability for AI systems, these principles should be considered by the partners.

Based on fundamental rights and ethical principles, the Guidelines list seven key requirements that AI systems should meet to be considered trustworthy.

3.4 Artificial Intelligence Ethics in the Healthcare Setting

The potential for enhanced clinical outcomes and more efficient health systems has driven a rapid increase in the development and evaluation of AI systems over the last decade. Most AI systems in healthcare are designed as clinical decision support systems rather than autonomous agents. Consequently, the interactions between AI systems, their users, and the implementation environments are crucial components of the overall effectiveness of these AI interventions.

Given the swift adoption of AI and machine learning (ML) in clinical research and their accelerating impact, the establishment of guidelines, such as SPIRIT-AI[8], CONSORT-AI[9], and more recently, DECIDE-AI[10], has helped address a significant regulatory gap.

Here, we will briefly discuss the main challenges associated with translating AI from research to clinical practice:

- *Avoiding Overuse*: The term 'overuse' refers to the unnecessary adoption of AI or advanced ML techniques when alternative, reliable, or superior methodologies already exist. In such cases, the use of AI and ML is not inherently inappropriate, but the justification for such research is unclear or artificial. For instance, a novel technique may be proposed that does not provide meaningful new insights. Unlike engineering, where performance improvements can enhance the entire system, modest improvements in medical prediction accuracy are unlikely to significantly impact clinical actions.
- *Rationalizing Usage*: Researchers should begin any ML project with clear goals and an analysis of the advantages that AI, ML, or conventional statistical techniques offer for the specific clinical use case.
- *Avoiding Misuse*: In contrast to overuse, 'misuse' refers to more problematic applications of ML, ranging from flawed methodologies that lead to incorrect inferences or predictions to attempts to replace physicians in roles that should still require human input. Blindly accepting an AI algorithm based solely on its performance, without scrutinizing its internal workings, constitutes misuse, even though not every clinician decision is fully explainable.

[8] Cruz Rivera, S., Liu, X., Chan, AW. *et al.* Guidelines for clinical trial protocols for interventions involving artificial intelligence: the SPIRIT-AI extension. *Nat Med* **26**, 1351–1363 (2020). https://doi.org/10.1038/s41591-020-1037-7

[9] Liu, X., Cruz Rivera, S., Moher, D. *et al.* Reporting guidelines for clinical trial reports for interventions involving artificial intelligence: the CONSORT-AI extension. *Nat Med* **26**, 1364–1374 (2020). https://doi.org/10.1038/s41591-020-1034-x

[10] Vasey, B., Nagendran, M., Campbell, B. *et al.* Reporting guideline for the early-stage clinical evaluation of decision support systems driven by artificial intelligence: DECIDE-AI. *Nat Med* **28**, 924–933 (2022). https://doi.org/10.1038/s41591-022-01772-9

- *Data Constraints*: Using ML despite data constraints, such as biased data and small datasets, is another misuse of AI. Training data can be biased, amplifying sexist and racist assumptions. Deep learning techniques require large amounts of data, but many medical publications use techniques with much smaller sample and feature-set sizes than those typically available in other industries. As a result, well-trained ML algorithms may lack a complete understanding of the clinical problem of interest.
- *Human-Machine Collaboration*: The roles of humans and algorithms in healthcare delivery are distinct. Algorithms help clinicians make the best use of complex, large, and granular data to inform practice. ML algorithms can complement, but not replace, physicians. Therefore, clinician-investigators must create a cohesive framework where big data drives a new generation of human-machine collaboration and where even the most sophisticated ML applications exist as discrete decision-support modules supporting specific aspects of patient care rather than competing with their human counterparts. Therefore, ML should be studied and implemented as part of a comprehensive system of care.

4 LEGAL FRAMEWORK

The following sections outline the legal framework applicable to HEREDITARY, providing an overview of the legal sources that the consortium must comply with during the development and piloting phases of the project.

4.1 International Treaties

The HEREDITARY partners operate under various legal obligations derived from international treaties. These treaties apply primarily to ratifying states, obligating them to uphold the rights enshrined in these agreements. HEREDITARY, established in such ratifying states, must consider these conventions, as they form the basis for EU and national legislation. Below is an overview of the relevant international legal instruments for HEREDITARY.

4.1.1 The European Convention on Human Rights (ECHR)

The ECHR[11], ratified by all EU Member States and Israel, protects fundamental human rights and liberties. Article 8, which covers the right to respect for private and family life, states:

> "*1. Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> *2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others*."

Article 8 establishes the fundamental right to privacy, including activities such as collecting and processing personal data for research. Violations of the ECHR can be brought before the European Court of Human Rights (ECtHR). However, violations of Art. 8 are justified in case of necessity; it should be noted that necessity implies proportionality, meaning that *"corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued"*[12]

4.1.2 The Council of Europe's Convention 108

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) is a key international instrument for data protection[13]. Adopted in 1981, it serves as the cornerstone for several data protection legal frameworks. Signatories, including the states where HEREDITARY partners are established, must implement the convention's principles into national law. Article 5 of Convention 108 outlines principles such as:

- Lawful and fair processing
- Purpose limitation
- Data quality and accuracy

---

[11] Council of Europe, European Convention on Human Rights, 1950 as amended, available at: https://www.echr.coe.int/Documents/Convention_ENG.pdf

[12] ECtHR, *Leander v. Sweden,* No9248/81, 26 March 1987, para. 58.

[13] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108, 1981.

The convention also distinguishes between personal and sensitive data and establishes data subject rights, including the *right to information* and the *right to rectification or erasure*. Chapter III addresses the international transfer of personal data, introducing the principle of equivalent protection.

Convention 108 has been updated to reflect technological changes, resulting in the Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+). Notably, Convention 108+ includes an updated definition of special personal data and the right for data subjects not to be subject to decisions based solely on automated processing.

4.2 Primary EU Legislation

This section introduces the primary EU legislation applicable to HEREDITARY, including the Charter of Fundamental Rights of the European Union (the Charter), the Treaty on the European Union (TEU), and the Treaty on the Functioning of the European Union (TFEU).

4.2.1 The Charter of Fundamental Rights of the European Union

The Charter, effective since 2009, synthesizes the constitutional traditions of EU Member States and serves as a primary source of EU law[14]. Relevant provisions for HEREDITARY include Article 8 (right to personal data protection), which states:

"1 *Everyone has the right to the protection of personal data concerning him or her.*

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority."

Article 52(1) of the Charter outlines the scope and limitations of fundamental rights, emphasizing that any limitations must *provided by law, respect the essence of the rights, be proportionate and necessary, and the objectives of general interest recognized by the EU or the need to protect the rights and freedoms of others*.

4.2.2 The Treaty on the European Union and the Treaty on the Functioning of the European Union

The TEU and TFEU, collectively known as the Lisbon Treaties, form the foundation of EU primary law. Article 16 of the TFEU restates data protection as a fundamental right and provides the legal basis for related legislation:

"*1. Everyone has the right to the protection of personal data concerning them.*

2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data.

[14] Charter of Fundamental Rights of the European Union, OJ C 202, 7.2.2016, p. 389.

3. Compliance with these rules shall be subject to the control of independent authorities."

These treaties establish the competency of the European Parliament and the Council to legislate on data protection matters and emphasize the control of compliance by independent authorities. Although secondary EU legislation provides the framework for data protection, Article 16 TFEU directly protects individuals, even in the absence of secondary legislation.

In cases of legal uncertainty, the implementation of primary EU law and international treaties will guide interpretation and application for HEREDITARY's activities.

4.3 Secondary EU Legislation

Secondary legislation in the EU includes regulations, directives, and decisions. It operates under the principles and objectives enshrined in the EU Treaties, based on the principle of conferral. The following sections outline the sources of secondary EU law applicable to HEREDITARY, providing an overview of the most important norms and principles. A more detailed discussion of HEREDITARY legal requirements will be implemented in the deliverables of WP7.

4.3.1 The General Data Protection Regulation

4.3.1.1 Background

Based on Article 16(2) TFEU, the European Parliament and the European Council adopted the General Data Protection Regulation (GDPR) in 2012. The GDPR regulates the processing of personal data in various contexts and is directly applicable within the EU. The GDPR is directly applicable to HEREDITARY and thus applies to all partners and actions within the project.

The GDPR applies when personal data is processed "wholly or partly by automated means" or when non-automated processing forms "part of a filing system" or is intended to do so.

The GDPR application is delimited by the notions of personal data and processing, which are defined in Article 4 as follows:

- Personal data: "any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly."
- Processing: "any operation or set of operations which is performed on personal data, whether or not by automated means."

As noted, the concept of personal data is broad, encompassing both subjective and objective information related to a natural person "by content, purpose, or effect."

4.3.1.2 Definition and Scope of Personal Data

Article 4(1) GDPR defines 'personal data' as 'any information relating to an identified or identifiable natural person ('data subject')'. An 'identifiable natural person' is further clarified as someone who can be identified, directly or indirectly, particularly by reference to identifiers such as a name, identification number, location data, online identifier, or specific factors related to physical, physiological, genetic, mental, economic, cultural, or social identity.

To ensure a consistent interpretation of 'personal data', the Article 29 Working Party adopted an opinion clarifying this concept. This opinion aligns with the broad notion of 'personal data' from the Council of Europe's Convention 108, allowing for a flexible and future-proof interpretation. However, the document emphasizes that data protection rules

should not be overstretched to cover unintended situations. The opinion identifies four main components of the definition:

a) *The notion of personal data includes 'any information'.*
The Working Party does not define 'information' but focuses on the types of information that fall under personal data. It clarifies that the nature, content, medium, or format of the information is irrelevant. Any statement about a person, whether objective, true, or unproven, may be considered personal data. This broad approach brings a vast number of data categories under the ambit of personal data.
b) *The information must be about an individual.*
This requires assessing the relationship between a specific piece of information and a person. The information must pertain to the individual in question
c) *The information must relate to an 'identified or identifiable' person.*
An individual is identified when they can be distinguished from others in a group. Identifiable means that, although not currently identified, the individual could still be identified. The Working Party differentiates between direct and indirect identification. Direct identification involves a name (and possibly additional information), while indirect identification refers to the 'unique combination' phenomenon, where multiple pieces of information can single out a person. Recital 26 GDPR specifies that 'account should be taken of all the means reasonably likely to be used' to identify a person, considering objective factors like the costs, time, and available technology.

This component is crucial in the context of analytics tools and methods that combine data from various sources. The increasing availability of data and advancements in analytic technologies enhance the likelihood of linking specific information to a person, thereby triggering the applicability of the GDPR.

4.3.1.3 Pseudonymisation and Anonymisation within the Meaning of the GDPR

Pseudonymization of Personal Data

The GDPR applies to pseudonymized data, defined by Article 4(5) GDPR as the processing of personal data such that it can no longer be attributed to a specific data subject without additional information, provided this additional information is kept separately and protected by technical and organizational measures. The Article 29 Working Party explains that pseudonymization involves disguising the identity of data subjects, allowing information collection without needing their names, which is particularly relevant for research and statistics. Pseudonymization can be done in two ways:

- Retraceable: Using correspondence lists or two-way cryptography algorithms, where identities can be traced back using additional information.
- Non-retraceable: Using one-way cryptography algorithms, where identities cannot be traced back, effectively creating anonymized data not subject to data protection rules.

In the first case, individuals remain indirectly identifiable, meaning such data is still considered personal data under the GDPR. In the second case, individuals are no longer identifiable, and the data is considered anonymized, thus falling outside the scope of GDPR.

The key criterion distinguishing pseudonymized data from anonymized data is whether individuals are identifiable. This requires assessing the ‘means reasonably likely to be used by the controller or another person’. Depending on the processing context, the

technology used to separate identifiers from raw datasets, and the entity processing the data, the assessment outcome may vary, necessitating a case-by-case analysis.

Anonymization of Personal Data

Recital 26 GDPR states that data protection principles do not apply to anonymous information, which does not relate to an identified or identifiable person or has been rendered anonymous so that the data subject is no longer identifiable. This necessitates a case-by-case assessment to determine whether individuals remain identifiable given the 'means reasonably likely to be used'. If identification is no longer possible, the data is considered anonymized and falls outside the GDPR's scope. However, if it is still possible to identify the individual, the data remains subject to GDPR.

The Article 29 Working Party acknowledges that creating a truly anonymized dataset from rich personal data without losing its informational value is challenging. The focus should be on the concrete means necessary to reverse the anonymization technique, the knowledge to implement those means, and the likelihood and severity of their use. Additionally, the means assessed should include those available to both the controller and any other person. True anonymization is thus a rigorous standard, requiring careful consideration and vigilance.

4.3.1.4 Sensitive Data within the Meaning of the GDPR

The GDPR imposes specific, stricter provisions for the protection of "sensitive data," which include: (1) "special categories of personal data" as defined in Article 9 GDPR and (2) "personal data relating to criminal convictions and offences" as defined in Article 10 GDPR.

Given the nature of HEREDITARY, we will briefly treat Special Categories of Personal Data. These data include data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for uniquely identifying a natural person, health data, and data concerning a natural person's sex life or sexual orientation. The processing of such data is generally prohibited. However, exceptions are permitted under certain conditions outlined in Article 9(2) GDPR, such as when the data subject has given explicit consent, unless EU or national law provides otherwise, or when the data has been made manifestly public by the data subject.

The prohibition on processing sensitive data can also be overridden when necessary for scientific research purposes, provided this is based on EU or national law and subject to specific legal safeguards. Among these special categories, genetic data, biometric data, and health data are particularly highlighted, as Member States can impose additional regulations on their processing.

4.3.1.5 Definitions and actors

The GDPR identifies several key entities: data controllers, data processors, and data subjects. Briefly:

- Data controller: The natural or legal person that determines the purpose and means of processing personal data, alone or jointly with others.
- Data processor: The natural or legal person that processes personal data on behalf of the controller.
- Data subject: A natural person who can be identified, directly or indirectly, through personal data.

The GDPR also introduces the role of the Data Protection Officer (DPO). The DPO operates independently within an organization and reports directly to the board or management. The DPO's responsibilities include overseeing the application of data protection rules, procedures, and policies, as well as ensuring the effective enforcement of data subjects' rights.

Given HEREDITARY involvement in extensive data processing, we will provide a short description of role of DPO as outlined by the GDPR.

- **Designation of a DPO.** According to Article 38 GDPR, a data protection officer must be designated in the following scenarios:

a) Processing is carried out by a public authority or body, except for courts acting in their judicial capacity.
b) The core activities of the controller or processor involve processing operations requiring regular and systematic monitoring of data subjects on a large scale.
c) The core activities of the controller or processor involve large-scale processing of special categories of data (Article 9) or personal data related to criminal convictions and offenses (Article 10).

- **Tasks of a DPO.** Article 39 GDPR outlines the tasks of a DPO, which include:

a) Informing and advising the controller, processor, and employees who process data about their obligations under the GDPR and other Union or Member State data protection provisions.
b) Monitoring compliance with the GDPR, other data protection provisions, and the controller or processor's policies regarding personal data protection.
c) Providing advice on data protection impact assessments and monitoring their performance according to Article 35.
d) Cooperating with the supervisory authority.
e) Acting as the contact point for the supervisory authority on processing-related issues, including prior consultation referred to in Article 36, and consulting on any other relevant matters.

- **Professional Qualifications and Support.** As stipulated in Article 38(5) GDPR, the DPO should be appointed based on professional qualities, particularly their expert knowledge of data protection law and practices. The controller and processor must support the DPO by providing necessary resources and should not interfere with the DPO's performance of their tasks (Article 38(2)(3)).

Overall, the appointment of a DPO strengthens controllers' accountability by ensuring compliance with GDPR, serving as a contact point for data subjects and supervisory authorities.

4.3.1.6 Data protection principles

The GDPR provides a set of rights for the data subject, including transparency, information and access to personal data by the data subject, the right to rectification and erasure.

When it comes to data protection principles, the GDPR expands international and primary sources that established the framework for the EU legislation on data protection. The main principles are the following:

- Purpose limitation (collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes);
- Fairness, lawfulness and transparency (processed lawfully, fairly and in a transparent manner in relation to the data subject)
- Data minimization (adequate, relevant and limited to what is necessary in

relation to the purposes for which they are processed);
- Data accuracy (accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay);
- Storage limitation (kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed);
- Integrity and confidentiality (processed in a manner that ensure appropriate security of personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organization measures);
- Accountability (the controller is responsible for, and must be able to demonstrate, their compliance with all of the above-named Principles of Data Protection);

The practical requirements of some data protection principles are outlined in WP1 deliverables (Data Management Plan) and will be further developed in WP7, which addresses the legal requirements for the HEREDITARY platform and provides recommendations at the project's conclusion. Here we provide a general description of the key principles:

- **Purpose Limitation**
  Personal data can only be collected for predetermined and specific purposes. Any processing outside the original purpose is prohibited unless exceptions apply, such as those in Article 89 GDPR for archiving purposes in the public interest, scientific or historical research, or statistical purposes.
- **Fairness and Lawfulness**
  Fairness points to the ethical dimension of data protection, while lawfulness requires a lawful basis for processing personal data. Article 6 of the GDPR enumerates the lawful bases for processing, which include:
    - The data subject consents to the processing for one or more specific purposes.
    - The processing is necessary for the performance of a contract to which the data subject is a party, or for pre-contractual steps.
    - The processing is necessary to comply with a legal obligation to which the controller is subject.
    - The processing is necessary to protect the vital interests of the data subject or another person.
    - The processing is justified for the public interest.
    - A legitimate interest pursued by the controller or a third party justifies the processing.
- **Data Minimisation**
  Data minimisation requires that personal data be processed only to the extent necessary for the processing.
- **Data Accuracy**
  Data accuracy mandates that personal data be correct and kept up to date.
- **Storage Limitation**
  Storage limitation, a corollary of purpose limitation, requires that personal data be kept in a form allowing identification for no longer than necessary. This is evaluated on a case-by-case basis depending on the processing purpose.
- **Integrity and Confidentiality**
  Integrity and confidentiality require appropriate technical and organisational measures to safeguard personal data from unauthorized access, accidental loss, tampering, destruction, or damage.
- **Accountability**

The principle of accountability requires the data controller to demonstrate compliance with the fundamental principles of data protection. Controllers must proactively show their adherence to the GDPR, making the respect for these principles explicit in their data protection policies.

4.3.1.7 Lawfulness and Lawful Basis within the GDPR

Article 5(1)(a) of the GDPR states that personal data processing must be "lawful." Article 6 ("lawfulness of processing") further clarifies that 'lawfulness' means having a legitimate basis for data processing, as listed in the GDPR. Processing personal data is lawful only if it is based on a legitimate ground.

a) Consent

Consent means “any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her” (Article 4(11)). High standards principles are complemented by specific clarifications. If consent is given in a written declaration concerning other matters, the request for consent must be clearly distinguishable, intelligible, and in plain language (Article 7(2)). For sensitive data, consent must be explicit (Article 9(2)(a)). When requested electronically, the consent request must be clear, concise, and not disruptive (Recital 32). The CJEU clarified that pre-ticked boxes do not qualify as valid consent under the GDPR, which requires 'an active behavior with a clear intention' from the data subject to consent to data processing. The notion of "freely given" implies genuine choice and control for data subjects. Enticements, inducements, or rewards for consent may question its validity as 'freely given'. Consent can be withdrawn at any time (Article 7(3)). Consent bundled with contracts or services is not deemed freely given (Article 7(4)). Assessing whether bundling occurs requires determining the scope of the contract and necessary data.

b) Processing Necessary for the Performance of a Contract

Processing based on this legal basis must be necessary for contract performance or pre-contractual steps. This necessity limits the personal data that can be lawfully processed. Necessary data must be determined case-by-case. Data not strictly necessary can only be processed if another legal basis is available.

c) Processing Necessary for Compliance with a Legal Obligation

The legal obligation can be established in EU or national law to which the controller is subject. While the GDPR does not require specific laws for each processing, the law should determine the processing purpose (Article 6(3)). It may also specify general conditions, such as data disclosure entities, purpose limitations, storage periods, and types of data processed (Recital 45).

d) Processing Necessary to Protect Vital Interests

The 'vital interests' lawful basis is for exceptional, emergency situations, such as when someone is in danger. It does not justify regular processing activities.

e) Processing Necessary for the Performance of a Task in the Public Interest or Exercise of Official Authority

There should be a basis in EU or Member State law (Article 6(3)). The controller may be a public authority or another natural or legal person governed by public law, or, where public interest dictates, by private law. The GDPR does not require specific laws for each processing, but the law should determine the processing purpose (Recital 45).

f) Processing Necessary for Legitimate Interests

This legal ground cannot be used by public authorities in the performance of their tasks. The GDPR does not provide an exhaustive list of what constitutes a “legitimate interest.” Recital 47 suggests that a legitimate interest may exist when there is a relevant and appropriate relationship between the data subject and the controller, such as a client or service relationship. This legal ground requires balancing the controller's legitimate interest and the data subjects' rights and freedoms. The "reasonable expectations of data subjects based on their relationship with the controller" must be considered. This balancing exercise is highly context-specific.

4.3.1.8 The Purpose Limitation Principle

Article 5(1)(b) GDPR stipulates that personal data must be "*collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes.*"

The Article 29 Working Party identifies two main components of this principle, which apply at different stages of personal data processing:

a) Specified, Explicit, and Legitimate Purposes

Personal data can only be collected for purposes that are specified, explicit, and legitimate. This means:

- Specified: The purposes must be clearly defined before or at the time of data collection (e.g., collecting a postal address for delivery purposes).
- Explicit: The purposes must be unambiguous and clearly expressed.
- Legitimate: The purposes must align with the legal expectations of data subjects (distinct from lawfulness).

b) **Further Processing Compatibility**

Personal data collected for specified purposes should not be further processed in a manner incompatible with those purposes. However, further processing is allowed if it is compatible with the initial purposes (Recital 50 GDPR). When personal data are used for compatible purposes, no separate legal basis is required beyond the original one. This is based on the reasonable expectations of data subjects regarding the further use of their data (Recital 50 GDPR).

An assessment of compatibility involves several criteria (Recital 50 GDPR): (a) the link between the initial purposes and the purposes of further processing; (b) the context of data collection and the reasonable expectations of data subjects regarding further use; (c) the nature of the personal data and the impact of further processing on data subjects; (d) the safeguards applied by the controller to ensure fair processing and prevent undue impact on data subjects.

In such cases, the controller must demonstrate that the further processing is compatible with the initial purposes on a case-by-case basis, adhering to the principle of accountability.

However, further processing is considered compatible with the initial purpose in three specific situations:

- Consent: The further processing is based on the data subject's consent (Art. 6(4)).
- Legal Basis: The further processing is based on EU/national law that constitutes a necessary and proportionate measure in a democratic society to safeguard various objectives (Art. 6(4) and 23(1)), including:

- Further processing for archiving in the public interest, scientific or historical research, or statistical purposes is considered compatible if subject to appropriate safeguards, such as data minimization and pseudonymization (Art. 5(1)(b) and 89(1)). Further details on processing personal data for scientific purposes are discussed in the "scientific research purpose" section.

4.3.1.9 Legal Regime for Processing Personal Data for Scientific Research Purposes

When processing data concerning individuals in the EU, scientific research must adhere to applicable rules, including the GDPR. The GDPR provides a special regime for genuine research projects operating within an ethical framework, offering flexibility through specific derogations and appropriate safeguards as outlined in Article 89.

There is no universally agreed definition of scientific research. Academic researchers, not-for-profit organizations, governmental institutions, and profit-seeking commercial companies can all conduct scientific research. The GDPR introduces a special regime for scientific research, comprising specific derogations from certain controller obligations and requiring appropriate safeguards.

The GDPR identifies two scenarios for processing personal data for scientific research:

Data Initially Obtained for Scientific Research:

The GDPR does not specify a separate lawful ground for processing data initially collected for scientific research. Depending on the context, one of the lawful grounds provided in Article 6 must be identified. Refer to the "lawfulness" section for details. The legitimate interest of the controller or a third party (Article 6(1)(f)) could be a lawful ground if the processing is necessary and balanced against the interests or fundamental rights and freedoms of data subjects. Additionally, processing may be considered necessary for tasks carried out in the public interest (Article 6(1)(e)), which requires a legal basis in EU or Member State law.

When dealing with Sensitive Data (special categories of personal data), such as those revealing racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic data, biometric data, health data, and data concerning sex life or sexual orientation, are subject to stricter rules. Their processing is generally prohibited unless one of the justifications in Article 9(2) applies. For example, explicit consent from the data subject (Article 9(2)(a)) or processing necessary for scientific research purposes based on EU or Member State law with appropriate safeguards (Article 9(2)(j)).

Data Initially Collected for Another Purpose, Then Further Processed for Scientific Research:

Refer to the "purpose limitation principle" section. Any reuse of data for scientific research, even if deemed compatible, requires the data to have been initially processed based on a lawful ground.

Further processing of personal data for scientific research must comply with safeguards outlined in Article 89. Appropriate safeguards ensure the rights and freedoms of data subjects, including technical and organizational measures to uphold data minimization. Measures like pseudonymization should be used whenever possible. If further processing can be achieved without identifying data subjects, it should be done that way.

Note of Caution

While the GDPR aims to harmonize data protection laws, Member States may derogate from certain data subjects' rights, such as the right of access (Article 15), right to rectification (Article 16), right to restriction of processing (Article 18), and right to object

(Article 21), subject to conditions and safeguards laid down in Article 89(1). Additionally, EU law may provide specific regulations for scientific research where appropriate.

4.3.1.10 Data Minimisation

Data minimisation involves evaluating whether the same purpose can be achieved with a narrower collection of data. Article 5(1)(c) GDPR requires ensuring that personal data are “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.”

This principle calls for a necessity and proportionality test concerning the purpose of data processing. Controllers must ensure they only process personal data that are suitable and reasonable for accomplishing the specified purposes according to the purpose limitation principle. In other words, controllers should assess whether these purposes could be achieved with less data or with properly anonymized datasets. This also implies tailoring the amount of data collected and their retention period to the identified purposes, necessitating adequate technical and organizational measures, such as pseudonymization.

In practice, performing the minimisation assessment can be more complex in the context of research activities because minimisation is linked to the purposes of the processing and cannot be evaluated in the abstract. The GDPR acknowledges this difficulty, as it is often not possible to fully identify the purpose of personal data processing for scientific research at the time of data collection (Recital 33).

For example, collecting data other than payment details and postal addresses for an online delivery would likely be seen as excessive concerning the purpose of product delivery.

4.3.1.11 Accountability

One important aspect to consider is the accountability measures introduced by the GDPR and their relevance to HEREDITARY. Accountability in the GDPR context means that an organization must demonstrate compliance by adopting internal policies and documentation to ensure adherence to applicable provisions. Examples of such policies and documents include:

- Data protection policy
- Privacy notice
- Staff training policy
- Information security policy
- Data protection impact assessment procedure
- Retention of records procedures
- Procedures to comply with data subjects’ rights
- International data transfer procedure
- Data portability procedures
- Complaints procedure

HEREDITARY partners are committed to applying the highest standards of data protection throughout the project. Therefore, each partner should assess which policies need to be developed or updated to ensure GDPR compliance.

4.3.1.12 Data Protection Impact Assessment

Previously, Directive 95/46/EC (the Data Protection Directive) mandated a general obligation to notify the supervisory authority(ies) about the processing of personal data. The GDPR abolished these notification requirements to tailor data protection obligations based on the risk severity to individuals' rights and freedoms (Recital 89 GDPR). When 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) according to Article 35 GDPR.

a) When is a DPIA Required?

A DPIA is required in three categories of situations:

- Explicit Requirement by the GDPR:
  - A systematic and extensive evaluation of personal aspects relating to natural persons based on automated processing, including profiling, which significantly affects the individual.
  - Processing on a large scale of "special categories of data" or personal data relating to criminal convictions and offenses.
  - Systematic monitoring of a publicly accessible area on a large scale.
- The controller envisages data processing activities identified on the list published by the national supervisory authority
- The controller otherwise envisages that processing of personal data is likely to result in a high risk to the rights and freedoms of natural persons, taking into account the nature, scope, context and purposes of the processing. This is especially so if “new technologies” are used, but the GDPR does not exhaustively list these cases to remain future-proof.

A DPIA is not required if processing operations are based on a legal obligation or the performance of a public task, provided the law regulates the specific processing operation and a DPIA has already been conducted as part of the general impact assessment.

b) When Should the DPIA be Conducted?

A DPIA should be conducted prior to the envisaged data processing. It may address a set of similar processing operations presenting similar high risks or a single operation. Existing processing operations (started before GDPR) require a DPIA if the risks change, considering the nature, scope, context, and purposes of processing.

Both the DPIA and the processing operations it assesses should be periodically reviewed, especially when risks change due to new technologies, broadened processing scope, or environmental changes. The DPIA is an iterative process, not a one-time obligation, and it is a starting point for applying privacy by design to the technology.

c) What is a DPIA and What is it For?

A DPIA is “a process for building and demonstrating compliance” (WP29), focusing on managing risks to data subjects' rights, unlike other risk management fields. The GDPR does not mandate a specific form or methodology, allowing controllers to choose a format that complies with GDPR requirements. A DPIA must include:

- A systematic description of the envisaged processing operations and purposes, including legitimate interests pursued by the controller.
- An assessment of the necessity and proportionality of the processing operations.
- An assessment of the risks to the rights and freedoms of data subjects, considering the origin, nature, and severity of the risks.
- Measures to address risks, including safeguards, security measures, and mechanisms to ensure data protection and GDPR compliance. Compliance with approved codes of conduct and other standards (e.g., certification, seals, and marks) should be considered to demonstrate that adequate measures are in place.

d) Involvement of Interested Parties

To protect the interests of involved parties, the data controller must seek advice from the data protection officer when conducting the DPIA and consider the views of data subjects or their representatives if appropriate. Consultation is inappropriate if it compromises commercial or public interests or security.

The controller must notify the supervisory authority if the DPIA indicates that processing would result in a high risk without mitigating measures. The supervisory authority may provide written advice or act according to Article 58 GDPR, which grants investigative, corrective, authorization, and advisory powers.

4.3.1.13 Rights of the Data Subject

The GDPR grants several rights to data subjects, and data controllers have an obligation to facilitate the exercise of these rights. Under the transparency principle, controllers must communicate appropriately with data subjects regarding their rights. Articles 12, 13, and 14 outline the information that controllers must provide to data subjects, ensuring they can effectively exercise their rights under the GDPR. These provisions also aim to ensure that personal data processing is conducted fairly and transparently.

The rights of data subjects, as detailed in Articles 15 to 22, include the right to: *access; rectification; erasure; restriction of processing; data portability; object; and not to be subject to a decision based solely on automated processing*.

These rights are fundamental to ensuring that data subjects have control over their personal data and that processing activities are conducted with respect to their privacy and autonomy.

4.3.1.14 Security, Integrity, and Managing Data Breaches

For the scope of this report, it is important to highlight the security measures introduced by the GDPR regarding personal data. Article 5(f) states:

"[personal data shall be] *processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures*."

Article 5(f) establishes the principles of integrity and confidentiality of personal data. Adhering to information security standards for the technical aspects of HEREDITARY is desirable, as it enhances personal data security. Article 32 provides further details on the security of personal data, including both technical and organizational measures such as:

- Pseudonymization, anonymization, and encryption of personal data
- Measures to ensure the reliability of services and systems
- Safeguards against cyber and physical incidents
- Policies for testing these measures

The principles of security and integrity follow a risk-based approach, meaning that the implementation of mitigation strategies must consider costs, state-of-the-art technology, and the nature and scope of data processing operations.

Another crucial aspect of the GDPR is the procedures for managing data breaches. Articles 33 and 34 outline the duty of processors to inform the supervisory authority and data subjects, respectively, in the event of a data breach. Data processors must notify the authority within 72 hours of discovering the breach. The notification must include:

- Nature of the breach, estimated number of data subjects and personal data records affected
- Contact details of the DPO
- Likely consequences of the data breach

- Measures adopted to address the breach

Notification to data subjects is required if the breach is likely to result in a high risk to their rights and freedoms. This communication, which should be in clear and plain language, is not required in three cases:

- Appropriate measures have been taken, and security has been restored
- The high risk is no longer present
- A disproportionate effort is required

In the last case, controllers should replace individual notifications with effective public communication.

4.3.1.15 International Transfers of Personal Data

The GDPR outlines the conditions for the legitimate international transfer of personal data. As previously discussed, Conventions 108 and 108+ established the necessity for adequate safeguards in the jurisdiction to which personal data are transferred. The GDPR provides more detailed conditions under which such transfers can occur to a third country or international organization.

There are two primary scenarios in which the transfer of personal data is allowed:

- Transfers on the Basis of an Adequacy Decision. Article 45 stipulates that personal data transfers are permitted if the European Commission has issued an adequacy decision, confirming that the recipient jurisdiction ensures an adequate level of protection.
- Instruments Providing Appropriate Safeguards. In the absence of an adequacy decision, several instruments can provide the necessary safeguards for international data transfers. These include:
    - A legally binding and enforceable instrument between public authorities or bodies
    - Binding corporate rules
    - Standard data protection clauses adopted by the European Commission
    - Standard data protection clauses adopted by an authority and approved by the European Commission
    - An approved code of conduct
    - An approved certification mechanism

  These instruments allow for data transfers without prior authorization from the competent data protection authority. However, there are cases where cross-border transfers may require authorization from the competent supervisory authority, specifically:
    - Contractual clauses between the data controller and the data processor
    - Provisions in administrative agreements between public bodies or authorities

These conditions ensure that international data transfers are conducted with appropriate safeguards to protect the rights and freedoms of data subjects.

The EU-US Data Privacy Framework

The European Commission adopted an adequacy decision for the new EU-U.S. Data Privacy Framework (DPF) on July 10, 2023. The DPF allows organizations that have self-certified with the DPF to transfer data from the EU to the U.S. without the need for additional transfer mechanisms.

U.S. organizations can use the new DPF to ensure an adequate level of personal data protection that is comparable to the standard under the GDPR. On that basis, the adequacy decision concludes that the United States ensures an adequate level of protection for personal data transferred from the EU to companies participating in the

EU-U.S. Data Privacy Framework. With the adoption of the adequacy decision, European entities are able to transfer personal data to participating companies in the United States, without having to put in place additional data protection safeguards.

The Framework provides EU individuals whose data would be transferred to participating companies in the US with several new rights (e.g. to obtain access to their data, or obtain correction or deletion of incorrect or unlawfully handled data). In addition, it offers different redress avenues in case their data is wrongly handled, including before free of charge independent dispute resolution mechanisms and an arbitration panel. To join the DPF, U.S. organizations must commit to comply with a detailed set of privacy obligations available in detail on the DPF site[15]. It is worth noting that the DPF may not be the final word. Furthermore, the DPF does not affect data residency requirements that may be in place in other countries and does not affect the requirements for Data Protection Impact Assessments or Privacy by Design requirements under the GDPR.

EU adequacy decision regarding Switzerland

The European Commission has classified Swiss data protection as equivalent to the EU General Data Protection Regulation (GDPR), as it was concluded that personal data transferred from the EU to Switzerland is subject to appropriate data protection guarantees.

4.4 The AI Act

4.4.1 Introduction

With the AI Act, approved by the European Parliament on 13 March 2024, the EU addresses the risks of AI and establishes a comprehensive legal framework for fostering trustworthy AI in Europe and beyond by ensuring that AI systems respect fundamental rights, safety, and ethical principles and by addressing risks of very powerful and impactful AI models.

The AI Act categorizes AI based on risk levels:

- AI systems deemed as posing an unacceptable risk, like social scoring systems and manipulative AI, are banned.
- High-risk AI systems are subject to regulation.
- Limited-risk AI systems have lighter transparency requirements; developers and deployers must inform end-users that they are interacting with AI, such as in the case of chatbots and deepfakes.
- Minimal risk AI applications, such as AI-enabled video games and spam filters (as of 2021), are largely unregulated, although this is evolving with the rise of generative AI.

The bulk of the responsibilities falls on the providers (developers) of high-risk AI systems, whether they are based within the EU or outside of it, as long as the AI system's output is used within the EU. Users, defined as individuals or entities deploying AI systems professionally, have fewer obligations than providers but still bear some responsibilities. This applies to users within the EU and those outside the EU whose AI system outputs are used in the EU.

[15] https://www.dataprivacyframework.gov/

4.4.2 Prohibited AI systems

The AI Act prohibits the following types of AI systems (Chapter II, Art. 5):

- AI systems using subliminal, manipulative, or deceptive techniques to distort behavior and hinder informed decision-making, resulting in significant harm.
- AI systems exploiting vulnerabilities related to age, disability, or socio-economic status to distort behavior, causing significant harm.
- Biometric categorization systems inferring sensitive attributes (such as race, political opinions, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation), except when used for labeling or filtering lawfully acquired biometric datasets or when law enforcement categorizes biometric data.
- Social scoring systems that evaluate or classify individuals or groups based on social behavior or personal traits, leading to detrimental or unfavorable treatment.
- Systems that assess the risk of an individual committing criminal offenses based solely on profiling or personality traits, except when they support human assessments based on objective, verifiable facts directly linked to criminal activity.
- Compiling facial recognition databases through untargeted scraping of facial images from the internet or CCTV footage.
- Inferring emotions in workplaces or educational institutions, except for medical or safety reasons.
- "Real-time" remote biometric identification (RBI) in publicly accessible spaces for law enforcement, except in cases of:
- Searching for missing persons, abduction victims, and individuals who have been human trafficked or sexually exploited.
- Preventing substantial and imminent threats to life or foreseeable terrorist attacks.
- Identifying suspects in serious crimes, such as murder, rape, armed robbery, narcotics and illegal weapons trafficking, organized crime, and environmental crime.

4.4.3 High-Risk AI Systems

Certain AI systems are classified as "high-risk" under the AI Act (Chapter III), subjecting their providers to additional requirements.

Classification Rules for High-Risk AI Systems (Art. 6)

AI systems are considered high-risk if they:

- Serve as a safety component of a product covered by EU laws listed in Annex I and must undergo a third-party conformity assessment under those laws; or
- Fall under the use cases listed in Annex III, unless:
- The AI system performs a narrow procedural task.
- It improves the outcome of a previously completed human activity.
- It detects decision-making patterns or deviations but is not intended to replace or influence prior human assessments without proper human review.
- It performs a preparatory task relevant to the use cases in Annex III.

AI systems are always considered high-risk if they profile individuals by automatically processing personal data to assess aspects of a person's life, such as work performance, economic situation, health, preferences, interests, reliability, behavior, location, or movement.

Requirements for Providers of High-Risk AI Systems (Art. 8–17)

Providers of high-risk AI systems must:

- Implement a risk management system throughout the AI system's lifecycle.
- Ensure data governance by making training, validation, and testing datasets relevant, sufficiently representative, as error-free as possible, and complete according to the intended purpose.
- Prepare technical documentation to demonstrate compliance and provide information for authorities to assess that compliance.
- Design their AI system for record-keeping to automatically log events relevant for identifying national-level risks and significant modifications throughout its lifecycle.
- Provide usage instructions to downstream deployers to ensure their compliance.
- Design the AI system to enable human oversight by deployers.
- Ensure the AI system achieves appropriate levels of accuracy, robustness, and cybersecurity.
- Establish a quality management system to ensure compliance.

5 RESEARCH ETHICS AS APPLIED IN HEREDITARY

5.1 Ethical Issues Management

5.1.1 Legal and ethics manager

To ensure ethical compliance throughout the HEREDITARY project, a Legal and Ethics Manager and a Scientific and Ethics Advisory Board will be appointed. They are responsible for:

- Ensuring the proper management of all ethics procedures.
- Reviewing all HEREDITARY materials and outputs for ethical compliance.
- Providing advice and assistance on ethics to all consortium partners.

5.1.2 Procedure in Case of Scientific Misconduct

HEREDITARY consortium members are fully aware of the ethical issues they may encounter during their work and condemn all forms of scientific misconduct. They are committed to following the fundamental principles of research integrity outlined in the revised version of the European Code of Conduct for Research Integrity as described above, regardless of the country in which the research is carried out:

- Reliability: Ensuring the quality of research, reflected in the design, methodology, analysis, and use of resources.
- Honesty: Conducting, reviewing, reporting, and communicating research in a transparent, fair, full, and unbiased manner.
- Respect: Showing respect for colleagues, research participants, society,

ecosystems, cultural heritage, and the environment.
- Accountability: Taking responsibility for the research from idea to publication, including management, organization, training, supervision, mentoring, and its wider impacts.

Violations of research integrity should be avoided at all costs. Research misconduct can include fabrication of results, falsification of data or records, plagiarism, failing to acknowledge authorship, misleading reporting of study results, and sabotaging the work of other scientists. If misconduct related to HEREDITARY activities occurs, it will be handled locally according to local regulations, following the principle of subsidiarity. Consortium partners will inform the Ethics Manager, the Scientific and Ethics Advisory Board and the coordinator about any misconduct and regularly update them on the local process.

5.1.3 Ethical Clearance

Full ethical clearance is being sought for the HEREDITARY project. Therefore, protocols for HEREDITARY activities will be submitted by clinical consortium partners to the Ethics Committee of their institution.

5.2 Ethical Guidelines and Procedures

The following internal ethical guidelines are intended to assist all HEREDITARY consortium members throughout the project, promoting a shared understanding of the importance of high research standards, integrity, and adherence to ethical conduct in research. These guidelines complement the rules for participation and dissemination outlined in the HEREDITARY consortium agreement.

5.2.1 Data Collection

HEREDITARY is committed to maintaining the highest scientific standards in data collection. All research conducted within the project will be approached with a critical and open mind, ensuring respect and dignity for all human participants. The Use Cases implemented in HEREDITARY primarily utilize data that has already been collected by partners. However, the collection of new data may be necessary for certain Use Cases. In such cases, clear and detailed data collection procedures and protocols must be provided.

Data collection and handling will comply with national laws and the General Data Protection Regulation (EU) 2016/679, ensuring the following rights and principles:

- Data Subject Rights: right of access, right to be informed, right to erasure
- Data Protection Principles, as detailed in section 6.2.4:

5.2.1.1 Identification and Recruitment of Participants

Participation in HEREDITARY activities will always be voluntary. New data will mainly be collected from the clinical partners represented in the HEREDITARY consortium. The following guidelines must be respected during recruitment and data collection:

- Researchers must provide a clear description of the data needed for each specific study.
- All individuals must be explicitly informed that participation is voluntary and that withdrawal will not have negative consequences; no pressure can be applied to candidates to participate.
- Explicit consent must be obtained from data subjects for one or more specific purposes, or if processing is necessary for scientific research purposes, in accordance with Article 9 of the GDPR regarding the collection of special

categories of data.

Procedures and Criteria to Identify/Recruit Research Participants

Participant Selection and Recruitment: If the partners involved in the Use Cases will require the collection of new data, they will inform the other partners and the Scientific and Ethic Commette. The partner should specify why new data collection is needed and the number of subjects that will be purposively recruited. Efforts will be made to ensure that the sample is adequate to the research purposes and as diverse as possible to maximize the generalizability and richness of the findings.

Eligibility Criteria: The eligibility criteria will be determined by involved partners according to the research necessity of the consortium. Eligibility screening will be performed by a study researcher.

Ethics Approvals for Research with Humans: Ethics approval will be sought from the Research Ethics Committee of the involved clinical partners once the design of the protocol for clinical data collection and eligibility criteria has been completed.

5.2.2 Data Management

HEREDITARY will adhere to good scientific practices in preserving primary data, managing data correctly, storing and documenting all relevant data, and processing data adequately. All consortium partners must comply with the Data Management Plan (D1.1), which details specific procedures. Individual consortium partners should develop appropriate mechanisms to ensure compliance with these procedures.

5.2.3 Informed Consent on Participation and Data Processing

If new data collection and new subject recruitment are necessary for specific Use Cases, data subjects must provide written informed consent. Prior to their actual participation in a HEREDITARY study, all human participants should be extensively briefed, either orally by a member of the research staff or through an information letter. Participants should be informed, prior to agreeing to participate, about the following (as per Chapter III of the GDPR):

- The identity and contact details of the researcher responsible for the study.
- The contact details of the appointed Data Protection Officer.
- The purpose of the study.
- The study procedures.
- The recipients of the personal data.
- The period for which the personal data will be stored.
- Their rights:
    - The right to request access to and rectification or erasure of personal data.
    - The right to withdraw consent at any time, without negative consequences.
    - The right to lodge a complaint with a supervisory authority.

All this information should be conveyed clearly and unambiguously. If subjects have additional questions, they should be answered by HEREDITARY team members present. Prior to participation, the participant should have read and, if they agree to participate, signed the Consent Form (template in Annex I).

Informed Consent Procedures

Informed Consent Process: Participation in the study will be entirely voluntary, with written consent obtained before the experiments begin. The informed consent process will be carefully designed to suit participants, supported by clear and simple information sheets.

Consent Meeting: A study researcher will communicate the information in a clear and simple manner and make sure that participants fully understand the project. During the meeting, the researcher will provide a participant information form and invite the candidate to read it or have it read aloud. This form will describe the study's nature and purpose, eligibility criteria, procedures, voluntary participation, data handling, benefits, risks, and contact information. Subjects will be given time to consider the information. Those choosing to participate without further consultation will read and sign the informed consent form, which will summarize key points from the information form.

Written and Verbal Consent: Written consent will be sought where possible. If not, verbal consent will be obtained in the presence of a literate witness who will countersign the consent document. The witness, who cannot be another researcher or study team member, must sign and date the consent form, attesting that the requirements for informed consent have been satisfied and that consent is voluntary. If allowed by national legislation, verbal consent could also be video-recorded.

Templates of Informed Consent Forms and Information Sheets: Included with this document are a template of the informed consent forms and information sheets, noting that these are incomplete and will be finalized upon design completion and approval of the Scientific and Ethics Committee.

Involvement of Children and/or Adults Unable to Give Informed Consent: This study will not involve children or adults unable to give informed consent. Regarding patients with neurodegenerative diseases, only adults who pass the minimum acceptable performance at disease-specific cognitive assessment scales will be eligible for participation.

Reporting Concerns: While research data will be treated confidentially and anonymously, any significant concerns about participants' well-being or legal breaches will be reported to appropriate authorities.

Maintaining Usual Care: Efforts will be made to ensure that the study does not impact participants' usual care. Staff will be requested not to change their usual practices for the collection of data in HEREDITARY, and participants will be explained that participation of the lack of participation will not affect their care.

Ethical Review: Data collection procedures will be thoroughly reviewed by the Research Ethics Committee of the involved clinical partner Institution. We will integrate all useful feedback to further reduce the likelihood of harm.

5.2.4 Data protection

In accordance with Article 5 of Regulation (EU) 2016/679 (General Data Protection Regulation), personal data shall be processed according to the following principles:

- *Lawfulness, Fairness, and Transparency*: Personal data shall be processed lawfully, fairly, and in a transparent manner in relation to the data subject.
- *Purpose Limitation*: Personal data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible

with those purposes.
- *Data Minimization*: Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
- *Accuracy*: Personal data shall be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- *Storage Limitation*: Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- *Integrity and Confidentiality*: Personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.

HEREDITARY has implemented necessary technical measures by design to ensure data security. To maintain privacy and regulatory compliance across nations, the project utilizes a federated network infrastructure that avoids centralizing health data and employs privacy-preserving querying methods. HEREDITARY's federated learning approach involves using secure supercomputer environments provided by a consortium partner, SURF. These environments offer a secure and isolated platform for combining public and private data from various sources. By leveraging these environments, clients can process their data locally while the supercomputer environment provides the computational resources needed for executing large-scale machine-learning tasks on anonymized data. To focus on the privacy and confidentiality aspects of federated learning, HEREDITARY ensures a protected communication channel between clients and the central server. Additionally, these environments guarantee that only authorized personnel have access to the data, preventing any leaks or compromises during the training process.

All data in HEREDITARY will be anonymized whenever possible or pseudonymized. Potentially identifiable data, such as Brain Magnetic Resonance Imaging (MRI) data, will undergo additional and specific de-identification methods to protect the confidentiality consented to by participants.

A protocol will be established in the event of a data breach likely to result in a risk to participants' rights and freedoms, as detailed in section 5.3.1.14.

5.2.5 Data Processing Limitations and Data Transfer Agreement

Within the HEREDITARY project, the right to process study data is strictly limited to the research organizations participating in HEREDITARY. To formalize this arrangement, a 'Data Sharing Agreement' will be established (Annex II), detailing each partner's responsibilities and duties. This agreement is essential as all scientific partners will be involved in analyzing data collected from human participants. The document will outline and agree upon the shared responsibilities in terms of data protection among all academic partners. It emphasizes the joint liability of all partners regarding the protection of the study data and ensures that all scientific partners adhere to the same high standards for data protection within HEREDITARY.

5.3 Privacy and Data Protection in Federated Learning

Federated learning is a distributed machine learning approach that enables training on a large corpus of decentralized data. It has emerged as a prominent solution to some of

the data protection challenges raised by AI. This technique facilitates the training of machine learning models without centralized data aggregation. Here, we briefly examine whether federated learning aligns with the GDPR and identify the potential benefits and challenges it presents.

GDPR Compliance Benefits

Federated learning offers several potential benefits for GDPR compliance:

- **Data Minimization**: By avoiding the transfer and centralization of raw training data, federated learning reduces the risk of unnecessary data duplication.
- **Purpose Limitation**: Federated learning helps comply with the principle of purpose limitation, which mandates that personal data be collected for specified, explicit, and legitimate purposes and not processed further in ways incompatible with those purposes.
- **Reduced Vulnerability to Attacks**: Federated learning models are less susceptible to attacks, improving the overall security of the data.
- **Data Localization**: Federated learning processes data locally, ensuring compliance with the GDPR. This is particularly crucial in the healthcare setting.
- **Encryption and Differential Privacy**: Federated learning often employs encryption techniques and differential privacy during the model update aggregation process. Differential privacy introduces "noise" to data or model updates, ensuring that the contributions of individual devices cannot be distinguished in the aggregated data, providing a mathematical guarantee of privacy.

The privacy-preservation advantage of FL compared to the traditional centralised ML approaches is undeniable. FL enables the training of an ML model whilst retaining personal training data on end-user devices. Only locally trained model parameters, which contain the essential amount of information required to update the global model, are shared with a coordination server. Nevertheless, such model parameters still enclose some sensitive features that can be exploited to reconstruct or to infer related personal information because some features of the training data samples are inherently encoded into such models. Therefore, all involved partners will take responsibility for complying with the principles and implementing appropriate measures to demonstrate compliance:

- Lawfulness, either Consent or Legitimate Interest)
- Fairness and Transparency, encouraging the design a new type of ML models with associated algorithms that are inherently interpretable
- Purpose limitation, which is fully satisfied because locally trained ML models from clients are aggregated only for the global model updates and cannot be individually extracted and exploited for other purposes
- Data Minimization, which is satisfied as FL assures that the global model itself contains no individual sensitive features that can be exploited
- Accuracy
- Storage limitations
- Integrity and confidentiality, where security and privacy should be implemented not only at a coordination server but also at end-users' devices as the FL system itself does not guarantee security and privacy.

Other Ethical Advantages

Federated Learning provides additional benefits, which underlie its potential to make AI accessible and democratic:

- Reduced Bandwidth Requirements: Federated learning's efficiency in data transmission reduces bandwidth requirements, which is beneficial in scenarios with limited network connectivity or where data transmission costs are a concern.
- Decentralized Learning: The decentralized nature of federated learning contributes to privacy and efficiency and democratizes AI by enabling broader participation in the model training process.

GDPR Compliance Challenges

Despite its clear benefits over traditional machine learning methods in preserving data privacy, federated learning also raises several compliance challenges under the GDPR:

- **Responsibility for Compliance**: Assigning responsibility for GDPR compliance is challenging due to the decentralized nature of federated learning. The binary controller-processor distinction in the GDPR does not easily apply to complex ecosystems involving numerous participants.
- **Ensuring Accurate Predictions:** Federated learning's decentralized approach can make it vulnerable to poisoning attacks, potentially leading to inaccurate model predictions. If the final model infers new personal data inaccurately, it may violate the principle of accuracy (Article 5(1)(d) GDPR), which requires personal data to be accurate and kept up to date.

Other Security Aspects of Federated Learning

Significant research has focused on improving the security of federated learning algorithms against poisoning attacks. These attacks aim to undermine the learning process by manipulating the data provided by participants (data poisoning) or corrupting the information exchanged between participants and the central node (model poisoning). While data poisoning can occur in both centralized and federated learning, model poisoning is unique to federated learning and can significantly impact the final model's performance if standard aggregation schemes are used. Compared to centralized models, federated learning models are generally less vulnerable to membership inference attacks, which attempt to determine if a specific data point was used in training the model. Federated learning leverages a larger dataset, making it more challenging for adversaries to gather all the necessary data for a successful attack. However, federated learning models are particularly susceptible to property inference attacks, where malicious participants infer broader properties (such as gender or race) from the data updates exchanged during training. Although these attacks are theoretically possible, their practical occurrence remains limited.

HEREDITARY is committed to carefully considering and implementing security measures and compliance protocols, such as robust anomaly detection mechanisms, secure aggregation protocols, and trustworthiness assessments

5.3.1 Data Controller in Hereditary

As described in section 5, according to the GDPR (Article 4), 'controller' "means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data". The controller is the person or entity that leads the personal data processing operation by determining the purposes and means for the processing.

In HEREDITARY, processing operations are handled by different partners. Therefore, each partner is responsible for the supervision over the determination of purposes and means for which the specific data will be used and how such operations will be performed. Should participants have any query regarding the way personal data is processed, principal investigator of each involved partner will serve as the contact point.

5.3.2 Data Protection Officers

Each host institution in HEREDITARY whose core activities as data controller or processor involve processing operations requiring regular and systematic monitoring of data subjects on a large scale or large-scale processing of special categories of data will appoint a Data Protection Officer (DPO) for the entire duration of the project.

5.3.3 Compliance with the AI act

Although HEREDITARY will not necessarily be categorized as high-risk under the AI Act, we recognize the importance of safeguarding personal health data in the context of AI, and are therefore committed to implementing comprehensive measures to ensure its security and reliability:

- A Risk Management Committee that oversee all aspects of risk management, including those related to A, has already been established.
- Detailed risk management procedures and plans will be documented in Deliverable 1.4, ensuring systematic identification, assessment, and mitigation of risks throughout the AI system's lifecycle.
- Use Cases partners are responsible for providing the consortium with datasets that are relevant, sufficiently representative, as error-free as possible, and complete according to the intended purpose.
- Technical documentation will be prepared to demonstrate compliance with applicable standards and regulations. This documentation will also provide necessary information for authorities to assess our compliance effectively.
- Tansparency and traceability will be ensured to record-keeping, capable of automatically logging events relevant to identifying risks and significant modifications throughout its lifecycle.
- At the end of the project, detailed usage instructions to downstream deployers will be provided
- All AI in Hereditary will be designed to allow deployers to implement human oversight,
- Appropriate levels of accuracy, robustness, and cybersecurity will be ensured, safeguarding the integrity and security of personal health data.
- Quality management system will be established to ensure ongoing compliance with all relevant standards and regulations. This system will support continuous improvement and adherence to best practices (see Deliverable 1.3).

5.4 Addressing AI Overuse and Misuse in the Healthcare Setting

While AI techniques employed in HEREDITARY Use Cases are designed to tackle complex analytical and prediction problems involving nonlinear or high-dimensional data relationships, it is important to recognize that many medical prediction problems are inherently linear and well-served by traditional statistical methods. In such cases, machine learning (ML) methods may not provide substantial improvements. To avoid the overuse of AI, the following guidelines will be adhered to throughout HEREDITARY:

- **Evaluation Against Traditional Methods:**

    - *Comparison and Validation*: Techniques developed in HEREDITARY will be rigorously evaluated against traditional statistical methodologies before deployment. Algorithms will be compared to predefined regression techniques to ensure they offer real improvements.
    - *Pre-specified Metrics*: Analytical methods and performance metrics will be pre-specified, covering aspects beyond overall performance, such as discrimination, calibration, and over-fitting. Continuous discussions between clinical and other partners will ensure that statistically significant improvements translate into clinically significant outcomes.
- **Rationalizing AI Usage:**
    - *Appropriate Application*: AI methods will be applied where they provide clear benefits. For example, unsupervised clustering analyses are suitable for discovering hidden patterns, while traditional statistical models may suffice for developing prognostic models or inferring causal treatment effects.
    - *Objective Assessment*: Researchers will assess the advantages of AI, ML, or conventional statistical techniques for each specific clinical use case, ensuring the chosen method is justified.
    -

In contrast to overuse, 'misuse' refers to more egregious uses of AI, ranging from problematic methodologies that produce spurious inferences or predictions, to attempts to replace the role of physicians in situations that still require human input. This includes indiscriminately accepting an AI algorithm purely based on its performance without scrutinizing its internal workings.

HEREDITARY partners commit to developing interpretable and explainable AI. The following points serve as guidelines for the HEREDITARY consortium:

- **Interpretability and Explanation**
    - *Interpretable Models*: AI models should be interpretable, and their reasoning transparent to human experts. De-identified scripts will be shared for external replication and validation.
    - *Visualization Techniques*: Use novel visual analytics approaches to reveal relevant relationships and insights across multimodal datasets, making data mining methods transparent and allowing clinicians, researchers, and interested members of the public to better understand and interact with the data.
- **Ensuring Diverse and Representative Data:**
    - *Inclusivity*: AI development must utilize diverse and representative data to better recognize, diagnose, and treat a wide range of conditions, reducing disparities and promoting equity in healthcare outcomes. This includes, but is not limited to, incorporating data from various patient populations, age and gender groups, and disease stages.
- **Establishing Liability and Accountability Frameworks:**
    - *Clear Guidelines*: Define the roles and responsibilities of physicians, AI developers, and healthcare institutions to address potential errors and biases in AI predictions. Encourage continuous feedback and improvement of AI algorithms while maintaining transparency and providing guidance on the intended use and limitations of AI solutions.
    - *Accountability*: Establish clear guidelines for responsibility and accountability in healthcare AI to manage potential errors, harmful outcomes, and biases. This includes determining the roles and responsibilities of various stakeholders, such as physicians and AI developers.
- **Collaboration Among Stakeholders:**

    - *Interdisciplinary Collaboration*: Foster collaboration among physicians, AI researchers, and developers to share expertise and develop strategies to mitigate biases and improve algorithm fairness.
- **Patient and Advocacy Group Participation:**
    - Involve patients and advocacy groups in the design, implementation, and evaluation of AI solutions. Their insights ensure AI addresses the specific challenges faced by diverse patient populations. This involvement helps build trust in AI-driven healthcare solutions and ensures that individual preferences, values, and circumstances are considered in AI development.
- **Education and Awareness of AI Biases:**
    - Educate clinicians and patients on the biases inherent in AI through workshops, conferences, and interdisciplinary collaborations. This promotes a shared understanding and encourages critical evaluation of AI recommendations, enabling healthcare professionals and patients to make informed decisions.

5.5 Ethics checks required in the Ethics Summary report

Limit risks of misuse with open-source code

Open-source algorithms carry the risk the information will be accessed by organizations or individuals who will misappropriate or perform another violation within the field for which the license has been granted. To mitigate these risks, we will implement measures such as purpose-limitation to prevent the code from being used for unintended purposes. We will also provide clear information on the responsibilities associated with algorithm implementation and consider indemnification for third-party infringement claims. Further measures to prevent misuse of AI in the healthcare setting are outlined in the previous section.

Ethics approval and authorizations by competent supervisory authorities for new personal data collection

Ethics approval will be sought from the Research Ethics Committee of the involved clinical partners once the design of the protocol for clinical data collection and eligibility criteria has been completed, as outlined in section 6.2.1.1.

Processing of data from non-EU partners

US-based partners in HEREDITARY will not process data of EU individuals or collect data from individuals within the EU. Similarly, under the federated learning framework, no personal data will be imported from non-EU countries. However, data from the US will be processed (Use Cases 3). Therefore, data will be shared between US and EU partners under a data sharing agreement (see section 6.2.5). The involved partners and the data controller will ensure that the federated learning architecture and pseudonymisation/ anonymisation techniques will be compliant with national laws.

Compliance with Technology Readiness Level Definition.

HEREDITARY will actively engage with project stakeholders and disseminate the project's activities, resources, and results to the relevant target groups, including clinicians and the scientific communities. Therefore, compliance with validation and demonstration at levels of Technology Readiness Levels (TRL) 5/6 will be maintained throughout the project.

Technology Readiness Levels (TRL) are a type of measurement system used to assess the maturity level of a particular technology. In other terms, this scale defines in terms of technology how robust is the solution or the product as it works/operates closer to their actual working conditions.

Table 1 Description of Technology Readiness Levels

TRL	Definition	Description	Supporting Information
1	Basic principles observed and reported.	Lowest level of software technology readiness. A new software domain is being investigated by the basic research community. This level extends to the development of basic use, basic properties of software architecture, mathematical formulations, and general algorithms.	Basic research activities, research articles, peer-reviewed white papers, point papers, early lab model of basic concept may be useful for substantiating the TRL.
2	Technology concept and/or application formulated.	Once basic principles are observed, practical applications can be invented. Applications are speculative, and there may be no proof or detailed analysis to support the assumptions. Examples are limited to analytic studies using synthetic data.	Applied research activities, analytic studies, small code units, and papers comparing competing technologies.
3	Analytical and experimental critical function and/or characteristic proof of concept.	Active R&D is initiated. The level at which scientific feasibility is demonstrated through analytical and laboratory studies. This level extends to the development of limited functionality environments to validate critical properties including cybersecurity and analytical predictions using non- integrated software components and partially representative data.	Algorithms run on a surrogate processor in a laboratory environment, instrumented components operating in a laboratory environment, laboratory results showing validation of critical properties.
4	Module and/or subsystem validation in a laboratory environment (i.e., software prototype development environment).	Basic software components are integrated to establish that they will work together. They are relatively primitive with regard to efficiency and robustness compared with the eventual system. Architecture development initiated to include interoperability, reliability, maintainability, extensibility, scalability, and security issues. Emulation with current/legacy elements as appropriate. Prototypes developed to demonstrate different aspects of eventual system.	Advanced technology development, stand-alone prototype solving a synthetic full-scale problem, or stand-alone prototype processing fully representative data sets.
5	Module and/or subsystem	Level at which software technology is ready to start integration with	System architecture diagram around technology

TRL	Definition	Description	Supporting Information
	validation in a relevant environment.	existing systems. The prototype implementations conform to target environment/interfaces. Experiments with realistic problems. Simulated interfaces to existing systems. System software architecture established. Algorithms run on a processor(s) with characteristics expected in the operational environment.	element with critical performance requirements defined. Processor selection analysis, Simulation/Stimulation (Sim/Stim) Laboratory buildup plan. Software placed under configuration management. Commercial-of-the- shelf/ government-off-the-shelf (COTS/GOTS) components in the system software architecture are identified.
6	Module and/or subsystem validation in a relevant end-to-end environment.	Level at which the engineering feasibility of a software technology is demonstrated. This level extends to laboratory prototype implementations on full-scale realistic problems in which the software technology is partially integrated with existing hardware/software systems. Cybersecurity verification should be included in the testing.	Results from laboratory testing of a prototype package that is near the desired configuration in terms of performance, including physical, logical, data, and security interfaces. Comparisons between tested environment and operational environment analytically understood. Analysis and test measurements quantifying contribution to system- wide requirements such as throughput, scalability, and reliability. Analysis of human-computer (user environment) begun.
7	System prototype demonstration in an operational, high- fidelity environment.	Level at which the program feasibility of a software technology is demonstrated. This level extends to operational environment prototype implementations, where critical technical risk functionality is available for demonstration and a test in which the software technology is well integrated with operational hardware/software systems.	Critical technological properties, including cybersecurity, are measured against requirements in an operational environment.
8	Actual system completed and mission qualified through test and demonstration in	Level at which a software technology is fully integrated with operational hardware and software systems. Software development documentation is complete. All	Published documentation and product technology refresh build schedule. Software resource reserve measured and tracked. All severity 1 and severity 2

TRL	Definition	Description	Supporting Information
	an operational environment.	functionality and cybersecurity measures tested in simulated and operational scenarios.	defects are resolved/confirmed, and a reasonably low level of severity 3 defects remain open.
9	Actual system proven through successful mission- proven operational capabilities.	Level at which a software technology is readily repeatable and reusable. The software based on the technology is fully integrated with operational hardware/software systems. All software documentation verified. Successful operational experience. Sustaining software engineering support in place. Actual system.	Production configuration management reports. Defect resolution system and process is in place for deployed software to address defects discovered in production.

6 CONCLUSIONS

Research ethics govern the standards of conduct for scientific researchers. Adhering to these principles is crucial for protecting the dignity, rights, and welfare of research participants, ensuring quality research outcomes.

Ethics holds a special place in Horizon projects. Responsible research and innovation (RRI) anticipates and assesses potential implications and societal expectations regarding research and innovation. Its goal is to foster inclusive and sustainable research. The European Code of Conduct for Research Integrity offers guiding principles for the self-regulation of the research community. HEREDITARY should comply with the following four ethical principles:

- Reliability: Ensure the quality of research through robust design, methodology, analysis, and resource use.
- Honesty: Conduct research transparently, fairly, fully, and without bias.
- Respect: Honor the rights and dignity of colleagues, research participants, society, ecosystems, cultural heritage, and the environment.
- Accountability: Be accountable for the entire research process, from idea to publication, including management, organization, training, supervision, mentoring, and broader impacts.

EU data protection laws aim to facilitate the free flow of data within the EU under common standards for lawful processing while safeguarding individual rights. The GDPR outlines six principles for data processing: lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, and integrity, confidentiality, and accountability.

Under the GDPR, research is recognized as a means to improve the quality of life and the efficiency of social services. The GDPR assumes a broad definition of “research” and provides a special regime for scientific research, allowing certain derogations from controller obligations.

In the context of AI, privacy and data protection require AI systems to be designed to guarantee user privacy and data protection. AI developers should employ techniques such as data anonymization and ensure data quality. While AI offers many benefits, it also raises ethical concerns, particularly regarding human rights and fundamental freedoms. The ethical guidelines recommended by the AI HLEG and OECD and the AI act emphasize these issues. As the legislative framework around AI evolves, a more in-depth analysis of the AI ethical and legal framework in the context of HEREDITARY will be necessary.

It is essential to underscore that compliance with ethical and legal requirements is a continuous effort that partners must maintain throughout the HEREDITARY project.