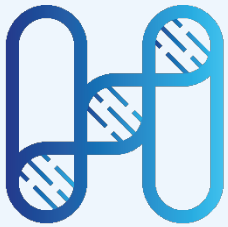

HEREDITARY

HetERogeneous sEmantic Data integratIon for the guT-bRain interplaY

Deliverable 7.1

LEGAL, ETHICAL, AND REGULATORY INVENTORY

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

The HEREDITARY project represents an ambitious and multi-faceted approach to address the integration of complex medical data to enhance disease prevention, diagnosis, and treatment. In an era where digitalisation and machine learning promise transformative advances in healthcare, substantial legal, ethical and societal challenges persist, also due to the inherently complex, multimodal nature of health data and the regulatory frameworks governing it. HEREDITARY tackles these challenges by aiming to build a secure, interoperable infrastructure to link diverse health data sources across disease domains, centring on diseases involving the gut-brain axis – neurological diseases and gut microbiome-related disorders.

The main barriers to health data integration include technical and legal complexities that limit the potential of these data sources. These variations challenge interoperability and data consistency, obstructing the development of seamless, large-scale data analysis systems. Furthermore, legal frameworks such as the EU's GDPR introduce essential but challenging requirements, adding complexity to cross-border and multicentre collaborations.

The deliverable analysis shows that the development of HEREDITARY must be guided by legal and ethical standards. The most relevant are the GDPR, cybersecurity legislation, EHDS proposal, NIS 2 Directive, and the evolving AI regulatory landscape, including the AI Act. Each of these legislation mandates robust data protection, security, and privacy measures, as well as guidelines for ethical AI deployment. HEREDITARY's legal framework shall ensure that personal data use aligns with these requirements, fostering trusted, transparent, and ethical use of health data in clinical and research contexts. Next to these requirements, the ethical framework can help in finding the most suitable interpretative solutions in those areas where the law is imprecise, vague, or simply non-existent. Four main principles of biomedical ethics and the principles for the development of trustworthy AI systems are crucial for the HEREDITARY project.

Both the legal and ethical frameworks mentioned above and further detailed in this deliverable lay the ground for the research in forthcoming deliverables of WP7 'Legal, Ethical and Regulatory Frameworks'.

DOCUMENT INFORMATION

Deliverable ID	D7.1
Deliverable Title	Legal, ethical, and regulatory inventory
Work Package	WP7
Lead Partner	KU Leuven
Due date	31.12.2024
Date of submission	18.12.2024
Type of deliverable	R
Dissemination level	PU

AUTHORS

Name	Organisation
Erik Kamenjasevic	KU Leuven
Elisabetta Biasin	KU Leuven
Daniele Dell'Aglio (Reviewer)	AAU
Anna Romanovych (Contributor)	UNIPD

REVISION HISTORY

Version	Date	Author	Document history/approvals
V0.1	24.11.2024	KU Leuven	First draft for internal review submission.
V0.2	02.12.2024	AAU	Partner's review.
V0.3	04.12.2024	KU Leuven	Feedback implementation.
V0.4	12.12.2024	AAU	Final reviewer feedback on minor improvements of the document.
V0.5	12.12.2024	KU Leuven	Feedback implementation and finalisation of the document.
V1.0	12.12.2024	UNIPD	Final formatting edition.
V1.1	18.12.2024	UNIPD	Double check and some final fixes.

Contents

LIST OF ACRONYMS

Acronym	Full word
AD	Alzheimer's Disease
ADHD	Attention Deficit Hyperactivity Disorder
AI	Artificial Intelligence
AML	Amyotrophic Lateral Sclerosis
DGA	Data Governance Act
EDIB	European Data Innovation Board
EEG	Electroencephalogram
EHDS	European Health Data Space
EHRs	Electronic Health Records
EMG	Electromyography
EU	European Union
FD	Frontotemporal Dementia
GA	Grant Agreement
GDPR	General Data Protection Regulation
HLEG	High-Level Expert Group on Artificial Intelligence
MS	Multiple Sclerosis
PD	Parkinson's Disease
NIS 2 Directive	Network Information Security 2 Directive
OCT	Optical Coherence Tomography
SME	Small-Medium Enterprises

1 INTRODUCTION

1.1 Project description

HEREDITARY aims to significantly transform the way we approach disease detection, prepare treatment response, and explore medical knowledge by building a robust, interoperable, trustworthy and secure framework that integrates multimodal health data (including genetic data) while ensuring compliance with cross-national privacy-preserving policies.

The HEREDITARY framework comprises five interconnected layers, from federated data processing and semantic data integration to visual interaction. By utilising advanced federated analytics and learning workflows, we aim to identify new risk factors and treatment responses focusing, as exploratory use cases, on **neurodegenerative** and **gut microbiome-related disorders**.

HEREDITARY is harmonising and linking various sources of **clinical, genomic, and environmental data on a large scale**. This enables clinicians, researchers, and policymakers to understand these diseases better and develop more effective treatment strategies. HEREDITARY adheres to the citizen science paradigm to ensure that patients and the public have a primary role in guiding scientific and medical research while maintaining full control of their data. Our goal is to change the way we approach healthcare by unlocking insights that were previously impossible to obtain.

1.2 Objectives of Deliverable 7.1

WP 7 aims to identify, analyse and evaluate the ethical and legal requirements related to the project with a focus on inter alia the EU data protection and privacy (e.g., the GDPR), access to data, interoperability, data quality and data sharing in the health sector (e.g., EHDS proposal), data governance, (cyber)security, and regulations applicable to AI systems. It will assist the consortium in aligning its activities with the proposed EHDS and the legal and ethical aspects of the 1+MG initiative by explaining the legal and ethical standards for cross-border access to health data (e.g., genomic data) for research purposes.

Deliverable 7.1, "*Legal, ethical, and regulatory inventory*", stems from WP 7's Task 7.1. The aim of that task is to provide a preliminary overview of the legal and ethical requirements applicable to the HEREDITARY project. T7.1 also aims to identify relevant legal and ethical frameworks and give **an overview of the key principles and rules that should be considered in the general setting of the project**, such as those on personal data processing, secondary use of health data, access to data, interoperability and infrastructure provisions of the proposed EHDS, and other legal and ethical frameworks.

1.3 Structure of Deliverable 7.1

To achieve the objectives delineated in Section 1.2, this deliverable is structured as follows. Section 2 contains the inventory of the legal, ethical and regulatory pieces of legislation relevant to the HEREDITARY project. Section 2.1 sets the scene and explains

the relevance of different laws and regulations in light of the project objectives. Six main elements are identified as most relevant: data protection legislation (Section 2.3), the forthcoming European Health Data Space proposal (Section 2.4), the Data Governance Act (Section 2.6) and the cybersecurity legal framework (Section 2.7). Further to the legal requirements, the report outlines the ethics framework, which is primarily grounded in AI Ethics (Section 3.1) and the principles of biomedical ethics (Section 3.2). As some stakeholders might have difficulties in discerning ethics from law, Sections 3.3.is dedicated to such important conceptual differentiation. Section 4 recapitulates and concludes.

2 LEGAL, ETHICAL, AND REGULATORY INVENTORY

2.1 Setting the scene within the EU legal framework

The integration of medical data to enhance disease prevention, diagnosis, and treatment remains challenging despite advancements in digitalisation and machine learning. This difficulty arises primarily from the complex, multimodal nature of medical data, which spans genomics, bio-images, bio-signals, and varied forms of text. Technical and legal obstacles also hinder the large-scale integration of health data from multiple sources, limiting their potential impact.

A significant barrier is the acquisition and management of both structured and unstructured data, such as bio-images and signals, which often differ widely due to diverse devices and protocols. Similarly, medical text data, or electronic health records (EHRs), present interoperability issues due to variations in terminology and language, complicating cross-disciplinary use. Patient information, though valuable for clinical decision-making, suffers from limitations due to data heterogeneity, quality, and accessibility issues.

The complexity of medical data makes it challenging to identify connections across data types, which could reveal insights like comorbidity patterns or effects of pre-existing conditions. Discovering such connections relies on effectively aggregating and analysing diverse data types across diseases.

The HEREDITARY project aims to meet three main objectives, as specified within the Grant Agreement (hereinafter: GA)[1]. These objectives are:

- Objective 1: Secure distributed system for multimodal health data linkage;
- Objective 2: Semantics-aware learning methods integrating multimodal and genomics data for improving health outcomes and
- Objective 3: Interactive data-driven solutions to empower decision-making prevention and strengthen citizen‘s trust.

All the objectives are equally relevant and will be supported throughout the project by legal, ethical, and regulatory analysis. However, in order to start outlining the preliminary principles of law and ethics that must be considered from the early start of the project.

HEREDITARY aims to develop a federated, scalable, secure, and privacy-preserving system for the linkage of health data, enabling querying of multimodal data across sources and disease groups. Currently, the collaboration of multiple medical centres and data modalities for joint data analysis is impeded by sparse data islands using diverse models and languages. Centralised solutions face challenges due to inefficiency, lack of cross-border infrastructure, security concerns, and divergent implementation of the GDPR among Member States and other health sector-specific national laws. However,

[1] Grant Agreement 101137074, HEREDITARY, HORIZON-HLTH-2023-TOOL-05.

once this objective is met, the multicentre and multimodal health data will be analysed seamlessly while fully considering the regulatory and policy developments facilitating health data sharing and interoperability, such as the EHDS, in compliance with relevant legal and ethical requirements, primarily with a European focus.

HEREDITARY focuses on diseases involving the complex gut-brain interplay to develop advanced analytics and learning workflows to identify new risk factors and treatment responses and to increase public awareness with the involvement of patient organisations and other stakeholders following an effective path of citizen science.

HEREDITARY includes two cross-domain groups of diseases studied in five exemplary clinical use cases – neurological diseases and gut microbiome-related disorders.

The first group concerns *neurological diseases*, including Amyotrophic Lateral Sclerosis (ALS), Multiple Sclerosis (MS), Parkinson's (PD), Alzheimer's (AD), Frontotemporal Dementia (FD), and stroke, which are major healthcare challenges. HEREDITARY integrates **multimodal and genomic data** to inform the phenotypic characterisation of neurological disorders, thus paving the way **for novel drug discovery and precision medicine**.

The second group of *gut microbiome-related disorders* includes some of the most critical diseases for society, including diabetes, obesity and psychiatric disorders, such as depression or ADHD. It is considered that the gut microbiome can impact brain function, including behaviour, cognition, and emotional states. The gut microbiome comprises the collective **genome** of roughly 100 trillion microorganisms residing in the gastrointestinal tract.

In order to meet the abovementioned objectives, HEREDITARY relies on numerous data sources and types. Namely, those data include **electronic health records**, **genomic data**, **medical imaging** (OCT, (f)MRI, [18F] FDG-PET, and histopathological Whole Slide Images), **laboratory and diagnostic tests, pathogen data, public health registries, and GWAS/WGS data**.

Genetic data are particularly important in studying neurological diseases and the gut microbiome because genetic factors can contribute to the susceptibility and progression of these diseases and can help identify potential therapeutic targets. In addition, genetic data can be used to identify biomarkers associated with these diseases, develop more accurate diagnostic tools, and improve treatment options and prevention strategies.

Various types of data will be used throughout the project's duration, including bioimages such as OCT, (f)MRI, and [18F]FDG-PET scans, biosignals such as EEG and EMG, and those collected by patient evaluations through clinical scales targeting cognitive, behavioural, functional or specific pathology features, multilingual texts covering diagnosis, therapies, and literature, as well as environmental and sensor data encompassing CO2 emissions, and PM2.5 air pollution.

As indicated, personal data and special categories of personal data, within the meaning of the **EU General Data Protection Regulation** (hereinafter: GDPR)[2], will be collected and processed within the project in order to meet the three main objectives. The accessibility and interoperability of data can be facilitated by secure and trusted infrastructures built in compliance with the legal requirements set out inter alia in the GDPR and the **Network and Information Systems Directive 2** (hereinafter: NIS 2 Directive)[3]. Hence, data access and sharing features of the system are to consider the requirements under the GDPR and the **European Health Data Space Regulation proposal** (hereinafter: EHDS proposal)[4] to facilitate patients' rights and to offer data-driven patient-focused health interventions. These considerations will also assist in aligning project activities, particularly the design of the "Federated Networking Infrastructure" layer with the EHDS infrastructure efforts on the secondary use of health data (e.g., cross-border access to data and cross-border infrastructures).

In the HEREDITARY project, ensuring **the accuracy of personal data is crucial**. To meet an appropriate level of accuracy, legal and ethical requirements stemming from the **AI Act**[5] and the **GDPR**[6] will be outlined, as well as **principles of ethics concerning trustworthy AI systems**[7].

The components of the architecture of the HEREDITARY project that are crucial for the analysis from the perspective of this deliverable concern **the federated networking infrastructure** and **the multimodal semantic integration platform**.
The former is designed for collaborative training of machine learning models and analytics while ensuring strict data privacy and security. This component allows for data-

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016.
[3] Regulation (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148.
[4] Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, COM/2022/197 final.
[5] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), PE/24/2024/REV/1, OJ L, 2024/1689, 12.7.2024.
[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016.
[7] European Commission, Independent High-Level Expert Group. (2019). Ethics Guidelines for Trustworthy AI.

and model-centric federated analytics and learning by decoupling access to data and sharing query or learning results, ensuring that no sensitive data crosses organisation boundaries.

The latter realises a polystore system, which harmonises access to public and private data, making medical data islands interoperable and integrated, and executes training and query plans from higher layers while maintaining security and privacy. By enabling secure and efficient access to medical data for analysis and model development, the layer ensures the seamless functioning of the HEREDITARY framework.

On the basis of the information provided above as well as in the GA, the following sections analyse relevant and applicable pieces of EU legislation, including GDPR, EHDS proposal, NISD 2, and AI Act. This is followed by an analysis of the appropriate ethics framework for AI systems, including the trustworthy AI guidelines and the four principles of biomedical ethics.

2.2 Data protection and the GDPR

The GDPR is a data protection law that governs how personal data are collected, stored, and processed. It aims to protect individuals' fundamental right to data protection and gives individuals control over their personal information. The aim of this section is to provide a high-level overview of the main aspects of the GDPR that concern data concerning health, genomic data and genetic data.

Under the GDPR, health data are classified as "special category" data, meaning it requires an additional layer of protection due to its sensitive nature. **Data concerning health**[8] includes any information related to the physical or mental health of a natural person. The GDPR defines **genetic data**[9] as personal data relating to inherited or acquired genetic characteristics. This includes DNA, RNA, or other data obtained from analysis that provides insights into an individual's physiology or health. **Genomic data** are a subset of genetic data, referring specifically to data about an individual's entire genome or large portions of it. This kind of data is highly unique and may predict not only health conditions but also traits, predispositions, and lineage.

Processing of data concerning health, genetic data and genomic data might require explicit, informed consent from the individual, emphasising their understanding of what data is collected, why, and who will have access[10]. Whether consent will be the most appropriate legal basis depends on the data controller.
Nonetheless, other legal bases are established under the GDPR. For example, in specific cases, data concerning health, genetic data and genomic data can be processed without consent, particularly if it serves substantial public interests or if necessary for medical diagnosis, health management, or vital interests (for example, life-saving

[8] GDPR, Article 4(15).
[9] GDPR, Article 4(13).
[10] GDPR, Article 9(2)(a).

treatments)[11]. Moreover, the GDPR allows flexibility for scientific research involving special categories of personal data, with conditions such as anonymisation or pseudonymisation, to minimise privacy risks[12].

When processing personal data as well as special categories of personal data, the following principles of processing have to be respected at all times.:

- Lawfulness, fairness, and transparency: data controllers must process personal data following a specific legal basis, in a way that individuals reasonably expect. It should be transparent to people to understand how and to what extent data are used.[13].
- Data minimisation: only the minimum necessary personal data should be collected and processed[14].
- Purpose limitation: personal data can only be used for specified, legitimate purposes and not beyond that scope without additional consent or another lawful basis[15].
- Accuracy: personal data must be accurate and kept up to date[16].
- Storage limitation: personal data should only be kept no longer than necessary for the purposes they were collected[17].
- Integrity and confidentiality: personal data must be protected by strong security measures to prevent unauthorised access or breaches[18].

Those whose personal data are processed (data subjects) have the following rights concerning their personal data:

- Right to access: data subjects can request access to their personal data held by a data controller and processor(s)[19].
- Right to rectification: individuals can request corrections to inaccurate personal data[20].
- Right to erasure (“right to be forgotten“): data subjects may request deletion of their personal data in certain cases, such as when it’s no longer needed for its original purpose[21].
- Right to restriction of processing: under specific conditions listed in Article 18 GDPR, data subjects have the right to restrict the processing of their personal data[22].

[11] See Article 9 GDPR.
[12] Ibid.
[13] GDPR, Article 5(1)(a).
[14] Ibid, Article 5(1)(b).
[15] Ibid, Article 5(1)(c).
[16] Ibid, Article 5(1)(d).
[17] Ibid, Article 5(1)(e).
[18] Ibid, Article 5(1)(f).
[19] Ibid, Article 15.
[20] Ibid, Article 16.
[21] Ibid, Article 17.
[22] Ibid, Article 18.

- Right to data portability: individuals can request that their personal data are transferred to another provider[23].
- Right to object: individuals can object to the processing of their personal data in circumstances such as profiling, especially if it is used for direct marketing[24].

Furthermore, data controllers handling personal data and special categories of personal data (such as health data and genetic data) must implement strong security measures, including encryption and access controls, to protect this sensitive information[25]. In case of a data breach, organisations must notify the competent data protection authorities within 72 hours if there is a risk to individuals' privacy and inform affected individuals promptly if their personal data are compromised[26].

Data controllers[27] are required to conduct data protection impact assessments before engaging in high-risk processing activities involving sensitive personal data to assess and mitigate potential privacy risks[28].

The GDPR allows some flexibility for processing health data and other types of personal and sensitive data for scientific research or public health purposes, provided certain safeguards (such as pseudonymisation or anonymisation) are in place. However, the processing must still align with EU or member-state law.

In summary, the GDPR imposes stringent requirements on the processing of health data to ensure its confidentiality, integrity, and availability. As it is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose[29].

2.3 European Health Data Space Regulation proposal

2.3.1 Introduction

The EHDS proposal[30] establishes the European health data space with the aim of strengthening the rights of natural persons concerning the availability of their electronic health data. Furthermore, it creates rules for the placing on the market of electronic

[23] Ibid, Article 20.
[24] Ibid, Articles 21 and 22.
[25] See Article 32 GDPR.
[26] Ibid, Article 33.
[27] Ibid, Articles 24-27.
[28] Ibid, Article 35.
[29] Recital 33 GDPR. See also Article 89 GDPR.
[30] Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space COM/2022/197.

health records systems (hereinafter: EHR systems) and wellness applications in the EU and establishes rules for the secondary use of electronic health data[31].

Among others, the EHDS applies to manufacturers and suppliers of EHR systems placed on the EU market and their users, controllers and processors established in the EU who are processing electronic health data of the EU citizens and third-country nationals residing in the EU[32].

The EHDS proposal defines personal electronic health data as data concerning health, as defined by the GDPR, that is processed in an electronic form[33].

Electronic health record is defined as a collection of electronic health data relating to a natural person and collected in the health system, processed for purposes of the provision of healthcare[34].

An EHR system is defined as any system where the appliance or software allows for storing, intermediating, importing, exporting, converting, editing or viewing personal electronic health data that belongs to the priority categories of personal electronic health data and is intended by the manufacturer to be used by healthcare providers in providing patient care or by a patient to access to their health data[35].

A wellness application is defined as any appliance or software intended by the manufacturer to be used by a natural person for processing electronic health data specifically for providing information on the health of individuals or the delivery of care for other purposes than the provision of healthcare[36].

The main goals of the EHDS proposals are (1) the empowerment of patients (i.e., to enable individuals to access, manage, and share their health data across borders in Europe. This interoperability aims to improve patient care and facilitate a smoother patient experience within the EU), (2) the promotion of research and innovation (i.e., to facilitate secondary use of health data for research, innovation, public health, and policymaking while safeguarding privacy and data security), and (3) the standardised and secure handling of health data (i.e., to establish standardised, secure, and lawful ways of handling health data, reducing fragmentation and improving data quality across EU Member States).

2.3.2 Primary use *versus* secondary use of health data

The primary use of electronic health data is defined as the processing of personal electronic health data for the provision of healthcare to assess, maintain or restore the

[31] Article 1(2) of the EHDS proposal.
[32] Ibid, Article 1(3).
[33] Ibid, Article 2(2)(a).
[34] Ibid, Article 2(2)(m).
[35] Ibid, Article 2(2)(n).
[36] Ibid, Article 2(2)(o).

state of health of the natural person to whom that data relates, including the prescription, dispensation and provision of medicinal products and medical devices, as well as for relevant social, administrative or reimbursement services[37].

The secondary use of electronic health data is defined as the processing of electronic health data for purposes such as scientific research, development and innovation for products contributing to public health, safety and quality of medicinal products or medical devices, providing personalised healthcare consisting in assessing, maintaining or restoring the state of health of natural persons, based on the health data of other natural persons[38].

The EHDS framework for the secondary use of electronic health data involves data access bodies. Namely, the EHDS proposal aims at setting up data access bodies in each EU Member State, responsible for overseeing, managing, and granting permission for secondary health data use requests. These bodies would ensure data are handled securely and in line with EU norms. Only entities that meet criteria for data handling, privacy, and ethical standards will be permitted access to electronic health data for secondary use. Individuals will be informed of how their data are being used and, in some cases, may be able to opt out of specific secondary uses. The EHDS proposal aims to ensure a balance between patient rights and societal benefits. Furthermore, the harmonisation of health data standards across the EU will allow approved entities to access and share data across Member States more efficiently, which is especially valuable for international research projects and large-scale clinical trials.

2.3.3 Data quality and utility label

Data quality and utility label[39] mean a graphic diagram, including a scale, describing the data quality and conditions of use of a dataset. The label serves to standardise and ensure the reliability of data made available through data access bodies. This labelling system aims to improve data usability and trustworthiness in electronic health records across the EU. Health datasets supported by EU or national public funding must have a quality and utility label detailing data attributes for transparency and usability. The label must include several elements:

- Data documentation: metadata, support documentation, data models, standards, and data provenance,
- Technical quality: measures such as data completeness, accuracy, timeliness, consistency, and validity,
- Data quality management: maturity of quality control processes, review and audit details, and examination for biases,
- Coverage: information on dataset representativeness, population sampling, and average timespan of individual records,
- Access and provision: timeline for data inclusion post-collection and time taken to provide access once approved,

[37] Ibid, Article 2(2)(d).
[38] Ibid, Articles 2(2)(e) and 34(1).
[39] See Article 56 of the EHDS proposal for the specific requirements.

- Data enrichment: information on data merging and integration with other datasets.

2.4 Data Governance Act

The Data Governance Act (hereinafter: DGA)[40] seeks to address the barriers to data sharing created due to trust issues, legal obstacles, and technical challenges by regulating data sharing and encouraging the reuse of public sector data while ensuring safeguards to maintain trust. It aims to create a more open, secure, and efficient data-sharing ecosystem, unlocking its full potential for societal and economic benefits while ensuring trust, privacy, and protection. The DGA promotes data sharing through several key mechanisms.

Public sector data reuse[41]: the DGA facilitates the reuse of publicly held but protected data (such as personal or commercially confidential data, such as trade secrets) under strict safeguards like anonymisation or secure processing environments. The DGA recognises that the public sector holds vast amounts of data, including personal and confidential information, which could be reused under specific conditions without compromising privacy or security. For example, data about health, mobility, or the environment could be invaluable for research and innovation. Public sector bodies must assist in data access, help obtain consent, and limit exclusive reuse agreements to cases of public interest. To avoid monopolising public data, the DGA limits the use of exclusive data-sharing agreements to cases with a clear public interest. Public sector bodies are encouraged to reduce fees for data reuse for research purposes or by SMEs and start-ups, promoting innovation without overburdening smaller players. Public sector bodies must decide on data reuse requests within two months, providing clarity and timeliness for data users. To help users find relevant data, Member States must set up a centralised information system with a European register to make public data more accessible to access across borders.

Data intermediation services[42]: data intermediaries, such as data marketplaces, are regulated to ensure transparency and neutrality, with strict safeguards against misuse or conflicts of interest. Data intermediaries will function as neutral platforms to help connect data providers and users. They cannot profit from the data directly (e.g., by reselling or using it to develop their own products), ensuring they remain unbiased. These intermediaries help companies and individuals share data securely while retaining control over its use. They must also notify authorities and comply with specific measures to maintain their neutrality and prevent conflicts of interest. They must be legally separated from any other services they offer, and commercial terms cannot depend on the use of other services they provide.

[40] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) PE/85/2021/REV/1, OJ L 152, 3.6.2022.
[41] Ibid, Articles 3-9.
[42] Ibid, see Chapter 3.

Data altruism principle[43]: the DGA encourages voluntary, non-rewarded sharing of data for public good, particularly in fields like health and the environment. Trusted organisations can register as data altruism bodies, ensuring transparency, protection of rights, and standardised consent forms to facilitate cross-border data sharing. Entities that facilitate data altruism must meet transparency and security standards, ensuring that data shared for societal benefits is handled responsibly. These organisations will be not-for-profit and comply with a "rulebook" developed by the European Commission to standardise practices across the EU. A unified consent form for data altruism will be used across the EU, ensuring a consistent and legal approach to obtaining data donations. This will make it easier for individuals to donate data while giving them control over how it is used.

European Data Innovation Board (EDIB): the EDIB fosters best practices in data intermediation, altruism, and public data use, helping to ensure cross-sector interoperability and protection of data across the EU[44].

International access and data flows: the DGA also supports international data transfers by setting safeguards to ensure EU-level data protection is maintained, especially for non-personal data, and allows the Commission to adopt adequacy decisions and model contracts for transfers to third countries[45].

2.5 AI Act

The AI Act[46] applies to providers, deployers, and other stakeholders listed in Article 2 who are placing on the EU market or putting into service AI systems[47].

An AI system is defined as **a machine-based system** designed to operate with **varying levels of autonomy** that may exhibit **adaptiveness** after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as **predictions, content, recommendations, or decisions that can influence physical or virtual environments**[48].

The AI Act distinguishes between prohibited AI systems and high-risk AI systems. The former are regulated through Article 5, which, among others, prohibits AI systems that deploy subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of, materially

[43] Ibid, see Chapter 4.
[44] Ibid, Article 29.
[45] Ibid, Article 31.
[46] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828. PE/24/2024/REV/1, OJ L, 2024/1689, 12.07.2024.
[47] Ibid, Article 2.
[48] Ibid, Article 3(1).

distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing a person to take a decision that that person would not have otherwise taken in a manner that causes or is likely to cause that person, another person or group of persons significant harm.

Furthermore, high-risk AI systems are regulated under Article 6(1) AI Act, which provides rules for their classification. An AI system is considered high-risk if it is **intended for use as a safety component of a product or is itself a product covered by the EU harmonisation legislation** listed in Annex I, and such a product must undergo **a third-party conformity assessment** to be placed on the market or put into service according to the EU harmonisation legislation listed in Annex I AI Act.

Section 2 of the AI Act outlines the requirements for high-risk AI systems. To avoid duplication and ensure consistency, providers of AI systems that fall within the scope of the legislation listed in Annex I can choose whether they want to submit the required documentation and comply with the processes established under that legislation or the AI Act.

As the basis for ensuring and demonstrating compliance with the AI Act, Article 9 establishes **a risk management system** for high-risk AI systems. Providers of AI systems have to ensure **regular systematic reviews and updating of risk management**[49]. This should include the identification and analysis of the known and reasonably foreseeable risks to health, safety of fundamental rights when the AI system is used according to its intended purpose, the estimation and evaluation of the risks that may emerge when a high-risk AI system is used in accordance with its intended purpose, the evaluation of the possible risks based on post-market monitoring data, and the adoption of appropriate and targeted measures designed to address the known and the reasonably foreseeable risks. Further to this, providers have to draft technical documentation.

Moreover, high-risk AI systems have to allow for record-keeping, should be designed, must operate transparently[50], and must include an appropriate human-machine interface for oversight[51]. High-risk AI systems must achieve an appropriate level of accuracy, robustness and cybersecurity[52].

Section 3 of the AI Act focuses on the regulation and management of high-risk AI systems. The AI Act establishes the obligations of companies and organisations that develop, deploy, or manage high-risk AI systems to ensure these systems operate safely, ethically, and transparently.

[49] Article 9(2) of the AI Act.
[50] Ibid, Article 12.
[51] Ibid, Article 14.
[52] Ibid, Article 15.

High-risk AI systems must meet specific technical and operational requirements before they are placed on the market or put into service. Requirements include data quality and governance, ensuring that training data is unbiased, complete, and representative to minimise risks of bias or discriminatory outcomes. Risk management systems must be implemented to identify, analyse, and mitigate risks throughout the AI system's lifecycle. Documentation and logging are mandatory to ensure traceability and facilitate oversight. Detailed records of the AI system's functioning, decisions, and impact are essential for accountability.

Human oversight must be built into high-risk AI systems, allowing humans to intervene or override automated decisions in critical situations. To meet this obligation , transparency measures require informing users and affected parties about the AI's purpose, how decisions are made, and any limitations or risks. This is intended to foster trust and enable users to make informed choices.

Developers and users of high-risk AI systems must establish continuous monitoring mechanisms. This includes post-market monitoring to detect, assess, and address any emerging risks after the system is deployed. Moreover, AI systems must undergo regular evaluations to ensure they maintain compliance with the regulatory standards over time.

The AI Act mandates a protocol for reporting incidents related to high-risk AI systems. Any system failures, malfunctions, or incidents that could lead to harm or legal violations must be reported to regulatory authorities. Affected users or entities must be informed about incidents that could impact their safety or rights.

Section 3 of the AI Act also outlines penalties for non-compliance with high-risk AI standards, ranging from warnings and fines to severe restrictions or prohibitions on market access. Penalties vary depending on the severity of non-compliance, and they aim to incentivise adherence to safety and ethical standards.

2.6 Cybersecurity

In the EU, data protection and cybersecurity rules **intersect closely**, as both aim to protect individual's personal data and maintain digital security. However, while they share common goals, they are distinct in scope and application. While GDPR[53] focuses on safeguarding individuals' data protection rights, EU cybersecurity laws like the NIS 2 Directive[54] aim to protect critical infrastructures and systems against cyber threats. **Both frameworks complement each other by promoting security and accountability,**

[53] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016.
[54] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), OJ L 333 27.12.2022.

encouraging a secure digital ecosystem, and ensuring that personal data and critical services are well-protected.

The GDPR is primarily focused on protecting individuals' personal data and ensuring privacy rights. It sets standards for how organisations collect, process, store, and transfer personal data, emphasising individuals' rights over their own information. The obligations stemming from the GDPR have been analysed in the section above.

The EU cybersecurity legislation, such as the NIS 2 Directive and the Cybersecurity Act[55], focuses on strengthening the digital infrastructure and resilience of critical sectors against cyber threats. These laws prioritise the security of networks and information systems to prevent unauthorised access, data breaches, and other cyber incidents.

Both data protection and cybersecurity frameworks aim to secure personal data, especially given the prevalence of cyber attacks that can lead to data breaches. Under Article 32 of GDPR, organisations must implement **appropriate technical and organisational measures** to safeguard personal data against unauthorised access or accidental loss. Similarly, cybersecurity laws mandate **securing networks and systems**, especially in essential services, to prevent cyber incidents. For instance, the NIS 2 Directive mandates that organisations in sectors like energy, **health**, and transport adopt stringent security measures. This aligns with GDPR's security requirements, as a cyber breach often results in a data breach.

Both frameworks require organisations to implement "appropriate" security measures. However, GDPR leaves this open-ended, allowing for a risk-based approach tailored to the data sensitivity. Cybersecurity laws, in contrast, may prescribe more specific standards, especially for critical infrastructure.

The GDPR and the NIS 2 Directive both require notifying relevant authorities in case of a security breach. Under GDPR, data breaches involving personal data must be reported within 72 hours to the relevant Data Protection Authority (DPA) and, in some cases, to the affected individuals. Under the NIS 2 Directive, entities experiencing a significant incident must notify the designated national cybersecurity authority, with requirements varying based on incident severity. Since a cyber incident often results in both cybersecurity and data protection concerns, organisations may have to report the same incident to both authorities.

As organisations become more data-driven, the boundaries between personal data protection and overall cybersecurity are blurring. For example, a healthcare provider might store sensitive health data, subject to GDPR protection, and use it in critical digital infrastructure, making it subject to the NIS 2 Directive as well. This interplay creates

[55] Regulation (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148.

compliance challenges, where organisations must address both GDPR's privacy-focused requirements and NIS 2 Directive's infrastructure security requirements, often involving overlapping and stringent reporting and security protocols.

The EU has been increasingly emphasising a cohesive approach to digital security. The EU Cybersecurity Strategy[56] calls for closer alignment between data protection and cybersecurity policies, recognising that data protection without cybersecurity is ineffective.

[56] European Commission, Joint Communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade, 2020, JOIN(2020) 18 final.

3 The ethics framework

3.1 AI Guidelines for trustworthy AI systems

The High-Level Expert Group on Artificial Intelligence (HLEG) AI Guidelines[57] is a set of recommendations developed by the European Commission to establish ethical and trustworthy practices in the development and deployment of AI systems within the EU. Launched in 2018, the HLEG AI was composed of experts from academia, civil society, and industry who were tasked with advising on policy development and fostering a human-centric approach to AI.

The Guidelines represent a foundational step toward responsible AI development, reflecting the EU's commitment to fostering technology that respects human rights and societal values. By promoting ethical principles alongside practical requirements, the guidelines aim to create an AI ecosystem that is trustworthy, transparent, and aligned with European values. These guidelines have not only shaped European policy but have also contributed significantly to the global discourse on AI ethics and regulation. The Guidelines serve as a voluntary framework for organisations and developers seeking to create responsible and ethical AI systems. While the guidelines are not legally binding, they have influenced the development of the AI Act. The Guidelines have been praised for setting a high standard for ethical AI, yet they also face criticism. One major challenge is the implementation gap, as enforcing and operationalising these principles across varied sectors can be difficult without more specific regulatory frameworks. There is also concern about balancing innovation with regulation.

The Guidelines emphasise transparency, accountability, and respect for human rights, providing a framework that has influenced both EU and global approaches to AI governance.

The Guidelines centre around a concept of **trustworthy AI systems**, which are characterised by three components: lawfulness, ethics, and technical robustness. These components ensure that AI systems are developed in ways that uphold human rights, are transparent, and can be relied upon to function safely and securely.

AI systems must adhere to applicable laws and regulations, such as those that protect human rights and privacy. Ethical considerations focus on respect for human autonomy, prevention of harm, fairness, and explicability. These guidelines outline ethical principles that ensure AI development aligns with values intrinsic to European society, including human dignity, individual freedom, and democracy. The guidelines emphasise that AI systems must be technically robust, resilient to attacks, and secure to prevent unexpected outcomes or harm. This includes regular testing, verification processes, and implementing redundancy to minimise risks in case of failure.

[57] European Commission, Independent High-Level Expert Group. (2019). Ethics Guidelines for Trustworthy AI.

The Guidelines delineate **four primary ethical principles** for AI systems:

- **Respect for human autonomy**: AI systems should not override human agency or manipulate users in harmful ways. Users should retain control over AI-assisted decisions, and the systems should enhance, rather than replace, human capabilities.
- **Prevention of harm**: AI systems should prioritise the well-being of individuals and society as a whole, minimising risks of harm or discriminatory impacts. Developers and operators are encouraged to conduct risk assessments and implement protocols to mitigate potential harm.
- **Fairness**: AI systems should be unbiased and promote equality. The guidelines stress that AI systems must avoid discrimination based on age, gender, race, or other protected attributes. This involves carefully curating datasets to ensure they do not reinforce existing biases or create new ones.
- **Explicability**: This principle requires that AI systems should be transparent and understandable. Stakeholders should be able to understand how an AI system makes decisions. This also supports accountability, allowing for assessment and verification of the AI's fairness, reliability, and compliance.

To translate the high-level principles into actionable steps, the Guidelines set forth seven key requirements for Trustworthy AI.

- **Human agency and oversight**: AI systems should support human autonomy and empower users by providing meaningful control and oversight mechanisms. This ensures that humans remain in control and can intervene if necessary.
- **Technical robustness and safety**: The technical structure of AI systems must be resilient to failures and attacks, ensuring they perform consistently across different scenarios.
- **Privacy and data governance**: AI systems should protect privacy, ensuring that users have control over their data. The Guidelines promote data governance mechanisms that include data quality controls and consent management, aligning with GDPR standards.
- **Transparency**: Transparency involves making AI systems understandable to stakeholders by documenting the processes and decisions they make. This includes disclosure of AI systems' capabilities and limitations.
- **Diversity, non-discrimination, and fairness**: AI systems should be inclusive, fair, and accessible to all. This requirement calls for active efforts to identify and mitigate biases in data and algorithms and to ensure equitable access to the benefits of AI.
- **Societal and environmental well-being**: AI systems should contribute positively to society and the environment, which includes minimising its carbon footprint and prioritising sustainability. Developers are encouraged to consider the broader impact of AI on society and the environment.
- **Accountability**: Mechanisms must be in place to ensure accountability and liability for AI systems. This involves clearly defined roles and responsibilities, audits, and continuous monitoring to address unforeseen issues.

3.2 Principles of biomedical ethics

The principles of biomedical ethics[58] are essential guidelines that help healthcare professionals and researchers navigate ethical issues in medicine, healthcare and biomedical research.

These principles serve as a foundation for ethical decision-making, balancing patient rights, the well-being of individuals and societies, and the responsibilities of healthcare providers and researchers.

Four main principles have been widely accepted as the cornerstone of biomedical ethics: respect for autonomy, nonmaleficence, beneficence, and justice. Together, they provide a framework that supports ethical practices in clinical settings, research environments, and public health.

These principles should be used throughout the project's development in order to find the most suitable solutions for interpreting the applicable legislation, as well as to propose feasible interpretations of those aspects where the relevant law is left ambiguous or unclear.

The principle of respect for autonomy emphasises the right of individuals to make their own choices, particularly regarding their health and medical treatments. In the context of biomedical ethics, autonomy is respected when patients are given enough information to make informed decisions and their decisions are respected by healthcare providers. **Informed consent** is a core aspect of respecting autonomy, ensuring that patients understand the risks, benefits, and alternatives of a treatment or procedure. Respecting autonomy also involves understanding and respecting the cultural, social, and personal values of patients. It means that healthcare professionals and researchers should refrain from making decisions for patients unless it is absolutely necessary, such as in cases where patients lack the capacity to make informed decisions or are in a life-threatening situation. However, the principle of autonomy is not absolute; it may be limited when a person's choices may cause harm to themselves or others. Ethical dilemmas often arise in situations where patient autonomy conflicts with medical advice or public health measures, challenging healthcare professionals to balance individual rights with collective welfare.

Nonmaleficence is the principle of "do no harm". This principle requires healthcare providers and researchers to avoid causing harm to patients. Nonmaleficence implies that medical professionals must carefully consider the potential risks and harms of any intervention and take steps to minimise them. It is also the basis for refraining from providing treatments that may be ineffective or harmful. In practice, nonmaleficence can sometimes conflict with other principles, particularly beneficence, as some treatments may carry risks or side effects that can harm the patient. In such cases, healthcare

[58] Beauchamp, T., & Childress, J. (2009). Principles of biomedical ethics. Oxford University Press.

providers must weigh the potential harm against the potential benefit and make decisions that prioritise the patient's overall well-being. Nonmaleficence also extends beyond physical harm to include psychological harm, where healthcare providers are encouraged to avoid causing unnecessary emotional distress to patients.

The principle of beneficence emphasises actively promoting the welfare of the patient. Beneficence requires healthcare providers and researchers to act in ways that benefit patients, whether by relieving pain, improving health, or enhancing quality of life. It calls for a proactive approach to healthcare, where professionals seek the best possible outcomes for their patients. The principle of beneficence often involves making judgments about what is in the best interest of the patient, which can be complicated by differing values, cultures, and beliefs. This principle is fundamental to patient-centred care and requires healthcare providers to consider not only the physical health of patients but also their well-being. Like other principles, beneficence must be balanced with autonomy, as promoting well-being should not override the patient's right to make their own decisions. This balance becomes particularly challenging in cases where a patient's decision conflicts with what the healthcare provider believes is in their best interest.

The principle of justice refers to the fair and equitable distribution of healthcare resources, benefits, and burdens. This principle requires that all individuals are treated fairly and that disparities in access to healthcare are addressed. This principle is particularly relevant in public health, where limited resources must be allocated in a way that maximises benefit while ensuring that vulnerable or marginalised populations are not disadvantaged. Justice also encompasses procedural fairness, ensuring that decisions are made transparently and that patients have access to fair processes for resolving grievances or ethical concerns. Healthcare providers are called to be mindful of social and economic factors that may affect patients' ability to access care, including insurance coverage, geographical location, and cultural barriers. In biomedical research, justice is also relevant to the treatment of research participants, ensuring that no group is unduly burdened or disproportionately subjected to risk and that the benefits of research are distributed fairly across society.

3.3 The link between ethics and law

Ethics can be defined as a normative system co-existing alongside the legal system[59]. Ethics, as a system, also contains high-level principles and norms, just as a legal system does, that can be applied to resolve specific moral doubts and propose better suitable alternatives or result in more just solutions to various kinds of daily issues. However, the ethics system often lacks an agreement among those with the democratic power that would provide for the formalisation of its institutional enforcement, such as the one that established hard laws enjoy. This can be referred to as 'ethics as theory'[60].

[59] This section is based on Kamenjasevic, E. (2025). Mood Enhancement Technology: Ethical and Legal Challenges. Doctoral thesis, forthcoming.
[60] Vedder, A., et al. (2025). Ethics First? On the EU Approach to AI Governance. Forthcoming in: Raposo, V. L., The European Artificial Intelligence Act, Springer.

Ethics can also be used as a notion to describe the practice of ethical reasoning, decisions, and communications. This is referred to as 'ethics as practice'[61]. An example of ethics in practice can be found in non-binding expert guidelines adopted prior to the adoption of the EU AI Act dealing with the development and deployment of trustworthy AI systems in the EU[62] (analysed above). Therein, several principles of ethics that were considered to be of utmost importance for the future development and use of AI systems within the EU have been proposed and are now considered to be the basis of the new Regulation dealing with AI systems – the AI Act[63].

Ethical principles in the mentioned guidelines have provided for the initial direction and have pointed toward the best suitable solution for those matters where the hard law has not yet been developed[64]. As such, ethics has been used first, prior to any sector-specific legislation, as a governance model by the institutions with the role of a co-legislator.

Another way in which ethical principles can be used is to apply them in parallel with the existing laws in order to find the most suitable or just solution for the issue at stake for which the law exists, but it is either not specific enough or leaves ambiguous its effects in a given situation, thus creating legal uncertainties.

A third example of how ethical principles can be used refers to those cases where the specific law applies, but the result of such application is not satisfactory because, for instance, it does not consider those in vulnerable positions, provokes discrimination, or another unacceptable outcome. This way, referral to ethics and principles is done in order to criticise the law. An example of this way of applying ethics may be found in the currently discussed ethical guidelines and recommendations dealing with neurotechnology by UNESCO Member States[65].

Throughout this research project, ethics will be applied in parallel with the applicable legislation, whenever this is necessary and appropriate in order to find the most fit solution.

[61] Ibid.
[62] European Commission, Independent High-Level Expert Group. (2019). Ethics Guidelines for Trustworthy AI.
[63] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828, PE/24/2024/REV/1, OJ L, 2024/1689, 12.7.2024.
[64] See Lessig, L. (1999). Code and Other Laws of Cyberspace. Basic Books; Lessig, L. (2006). Code: Version 2.0. Basic Books.
[65] UNESCO, Ad hoc Expert Group. (2024). Outcome document of the first meeting of the AHEG. First draft of a recommendation on the ethics of neurotechnology (first version), SHS/BIO/AHEG-Neuro/2024/1.REV.

4 Conclusion

The aim of this deliverable D7.1 was to provide a preliminary overview of the legal and ethical requirements applicable to the HEREDITARY project. Based on the early description of the project goals, this deliverable looked at the relevant EU legislation and principles of ethics in order to provide guidance and set the basis for further research in the upcoming deliverables.

As described, both personal data and special categories of personal data—defined according to the EU General Data Protection Regulation (GDPR)—will be collected and processed throughout the project to achieve its three core objectives.

Ensuring accessibility and interoperability of data is central to the project and will be supported by secure, trusted infrastructures designed in compliance with key legal frameworks, including the GDPR and the NIS 2 Directive. These infrastructures will be constructed to prioritize data access and sharing in line with GDPR requirements and the proposed European Health Data Space Regulation. This alignment aims to uphold patient rights and enable data-driven, patient-centered healthcare interventions.

The project's design, especially the creation of the "Federated Networking Infrastructure" layer, will consider EHDS provisions for the secondary use of health data, facilitating cross-border data access and interoperable infrastructures. Integrating these norms should be followed to ensure a seamless, secure exchange of health data across borders, enhancing the system's utility for both patients and healthcare providers.

In the HEREDITARY project, maintaining the accuracy of personal data is a priority. This commitment involves rigorous adherence to data quality standards, put in place the all the relevant and feasible measures to make sure that data contained in datasets are accurate and suitable for generating reliable insights and downstream applications. To achieve this, a robust framework concerning legal and ethical requirements of the AI Act and the GDPR was examined while also following ethical principles designed to ensure trustworthy AI systems. These guidelines, although voluntary, laid the groundwork for the AI Act by emphasizing transparency, accountability, and human rights. They focus on three pillars of trustworthiness: lawfulness, ethics, and technical robustness, mandating that AI systems comply with laws, respect human autonomy, prevent harm, and uphold fairness and explicability. Next to this, biomedical ethics centres around four core principles essential for ethical medical practices: autonomy, nonmaleficence, beneficence, and justice. These principles serve to guide healthcare professionals in balancing patient rights with their responsibilities, among others.

Based on this preliminary analysis, it can be concluded that ethics, as a system of high-level norms, complements the legal system, especially where laws may be ambiguous or insufficient. Unlike enforceable laws, ethics offers "theory" and "practice" models, serving as a guideline for situations not adequately addressed by existing legislation.

In the following deliverables, an in-depth analysis of the relevant legislation supported by principles of ethics will be performed in order to ensure the development of HEREDITARY that is in line with the values and principles of the EU.

REFERENCES

The bibliographic entries are arranged in lexicographical order based on the key, following the APA style. This enables us to place the entries and citations in the table and text in any sequence, allowing for later sorting while ensuring consistency.

Key	Reference
Beauchamp, Childress	Beauchamp, T., & Childress, J. (2009). Principles of biomedical ethics. Oxford University Press.
NIS 2 Directive	Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), OJ L 333 27.12.2022.
AI Guidelines	European Commission, Independent High-Level Expert Group. (2019). Ethics Guidelines for Trustworthy AI.
EU Cybersecurity Strategy	European Commission, Joint Communication to the European Parliament and the Council. (2020). The EU's Cybersecurity Strategy for the Digital Decade, JOIN(2020) 18 final.
GA	Grant Agreement 101137074, HEREDITARY, HORIZON-HLTH-2023-TOOL-05.
Kamenjasevic	Kamenjasevic, E. (2025). Mood Enhancement Technology: Ethical and Legal Challenges. Doctoral thesis, forthcoming.
Lessig 1999	Lessig, L. (1999). Code and Other Laws of Cyberspace. Basic Books.
Lessig 2006	Lessig, L. (2006). Code: Version 2.0. Basic Books.
EHDS proposal	Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, COM/2022/197 final.
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016.
DGA	Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) PE/85/2021/REV/1, OJ L 152, 3.6.2022.
AI Act	Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), PE/24/2024/REV/1, OJ L, 2024/1689, 12.7.2024.
UNESCO 2024	UNESCO, Ad hoc Expert Group. (2024). Outcome document of the first meeting of the AHEG. First draft of a recommendation on the

Key	Reference
	ethics of neurotechnology (first version), SHS/BIO/AHEG-Neuro/2024/1.REV.
Vedder	Vedder, A., et al. (2025). Ethics First? On the EU Approach to AI Governance. Forthcoming in: Raposo, V. L., The European Artificial Intelligence Act, Springer.