This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement Nº 101137423

D2.2 – Stakeholder Requirements and legal framework

Deliverable No.	D2.2	**Due Date**	31/08/2025
Description	Outlines the legal requirement and needs of stakeholders for the research project. It provides a comprehensive overview of the project's stakeholders' needs and expectations, alongside an analysis of relevant legal and regulatory frameworks.		
Type	Report	**Dissemination Level**	PU
Work Package No.	WP2	**Work Package Title**	Codesign and multi-stakeholders' requirements
Version	1	**Status**	Final

Authors

Name and surname	Partner name	e-mail
Adrian Quesada Rodriguez	UDGA	aquesada@udgalliance.org
Renata Radocz	UDGA	rradocz@udgalliance.org
Iida Lehto	UDGA	ilehto@udgalliance.org
Vasiliki Tsiompanidou	UDGA	vtsiompanidou@udgalliance.org
Ana Maria Pacheco	UDGA	admin@udgalliance.org

Document History

Version	Date	Changes	Authors
V0.1	01.01.2025	Initial TOC	Adrian Quesada Rodriguez
V0.5	01.03.2025	Initial draft	Adrian Quesada Rodriguez
V0.9	20.08.2025	Ready for peer review	Adrian Quesada Rodriguez
V1.1	22.09.2025	Final version	Adrian Quesada Rodriguez

Key data

Keywords	Legal, Ethics, Contractual, Compliance, Requirements, Stakeholders, Self-assessment, Certification
Lead Editor	Adrian Quesada Rodriguez
Internal Reviewer(s)	UTW, UGR

Abstract

This deliverable, D2.2, outlines the definitive legal and ethical framework for the PROTECT-CHILD project.

This document, D2.2, outlines the legal and ethical framework for the PROTECT-CHILD project. It provides an overview of digital and data laws in the European Union, including the Digital Services Act (DSA), the General Data Protection Regulation (GDPR), the European Health Data Space (EHDS) Regulation, the Data Governance Act (DGA), the Data Act, and the Artificial Intelligence (AI) Act. It also covers important cybersecurity requirements from the NIS2 Directive and the Cyber Resilience Act (CRA). A review of national laws and regulations in all partner countries, including Spain, Italy, Greece, the Netherlands, Germany, and Belgium, as well as non-EU partners in Serbia, the US State of Georgia, and Switzerland, is an essential part of this document.

The deliverable lays down foundational ethical principles, which were derived from key international instruments such as the Declaration of Helsinki, the Oviedo Convention, and the UN Convention on the Rights of the Child, are integrated into actionable project requirements. These principles are synthesised with obligations arising from the Grant Agreement and stakeholder needs identified through the project's co-design process.

This document is a key compliance guide for all consortium partners. It translates complex legal and ethical obligations into a clear, actionable plan. This plan focuses on developing the federated Data Space, conducting clinical research responsibly, and managing sensitive paediatric health and genomic data securely.

Statement of originality

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

TABLE OF CONTENTS

LIST OF TABLES

1 About this deliverable

Deliverable D2.2 outlines the legal requirement and needs of stakeholders for the research project. It provides a comprehensive overview of the project's stakeholders' needs and expectations, alongside an analysis of relevant legal and regulatory frameworks. It outlines the specific requirements, preferences, and constraints of stakeholders such as researchers, clinicians, patients, regulatory bodies, and industry partners. Additionally, the deliverable delves into the legal landscape, encompassing data protection laws, medical ethics regulations, and clinical trial guidelines, ensuring the project's compliance with all pertinent legal and ethical standards. Detailed provisions for data governance, privacy protection, and ethical considerations are provided to safeguard participant rights and welfare. Furthermore, the document assesses potential risks and proposes mitigation strategies to address legal, regulatory, and stakeholder-related challenges, ensuring the project's smooth execution and adherence to ethical principles throughout its lifecycle. Ultimately, Deliverable D2.2 serves as a guiding document for navigating the complex interplay of stakeholder requirements and legal considerations in the PROTECT-CHILD project, thereby facilitating its responsible conduct and successful outcomes in child health research and protection.

1.1 Deliverable context

Table 1 Deliverable context

PROJECT ITEM IN THE DoA	RELATIONSHIP
Project Objectives	D2.2 directly supports all project goals. To improve treatment for paediatric transplant patients, we need to process sensitive health data in a lawful and ethical way. Our aim to support the European Health Data Space (EHDS) depends on fully following the framework outlined here, especially the EHDS Regulation. Building a compliant and trustworthy data-sharing system is essential for reaching all scientific and clinical objectives.
Exploitable Results	An essential part of the project's main outcome, the "PROTECT-CHILD Data Space," is the legal and ethical framework outlined in D2.2. This framework makes the platform a reliable resource for future research. It also allows for possible integration with larger projects like the EHDS and the Beyond 1 Million Genomes (B1MG) initiative, ensuring its legal and ethical viability.
Workplan	D2.2 is the main result of Task 2.2 ("Legal framework definition to build PROTECT-CHILD Data Space"). It outlines the key legal and ethical guidelines that will direct the work of all technical development Work Packages (WP3, WP4, WP5, WP6), the clinical research Work Package (WP8), and the ethics and governance Work Packages (WP11, WP12). It turns abstract legal principles into specific requirements for system design, data management, and research protocols.

Milestones	This deliverable directly addresses the project milestone for creating the ethical and legal framework (M1-M24). Completing it means the project has a strong, documented foundation for moving forward with data collection and processing activities in a compliant way.
Deliverables	Upcoming deliverables by WP11 are to be based on the results of D2.2.
Risks	D2.2 is the main tool for reducing several key project risks. These include legal non-compliance with the complex and changing EU laws, data protection violations, loss of participant trust, and not meeting the ethical standards needed for research with minors. The thorough examination of national laws and international data transfer methods targets the risks linked to a multi-jurisdictional consortium.

2 Project Overview

The overarching clinical objective of the project is to enhance treatment and long-term care for children who have undergone organ transplants. This encompasses the improvement of targeted therapies and of follow-ups, the prevention and avoidance of treatment toxicities and side effects, and overall assurance of better quality of life. To achieve these goals, the data from ERN TransplantChild's will be exploited and integrated with existing and newly generated genome and methylome study data from a cohort of 200 paediatric liver and kidney transplant patients across four European hospitals. The participants in this study will be children between the ages of 3 and 18 who have undergone a kidney or liver transplant and whose participation is based on consent provided either by themselves, where applicable, or by their parental/legal guardians.[1]

The PROJECT-CHILD intends to contribute to the creation of the European Health Data Space by enabling the integration and cross-border sharing of previously mentioned data. Additionally, the project will implement federated algorithms that provide functionalities such as cohort selection, data cleaning, imputation, statistical analysis, and machine learning. These algorithms are designed to operate in a distributed environment under strict privacy and security requirements, ensuring that sensitive data remain at their source. They will also generate standardized analysis templates for automated and reproducible use across participating sites.[2]

The project's primary objective is to perform thorough genomic and methylome analyses to better understand and treat paediatric liver and kidney transplant patients. This includes finding biomarkers linked to adverse drug reactions and long-term complications from immunosuppressive therapy, and identifying novel genes, genomic regions, and methylation patterns associated with transplant outcomes. As part of the secondary objective, the project aims to incorporate the generated genomic and epigenomic data into the Beyond 1 Million Genomes (B1MG) initiative.[3]

[1] European Health and Digital Executive Agency. (2024). Page 177. *Grant Agreement: PROTECT-CHILD* (Grant Agreement No. 101137423). Brussels, Belgium

[2] Ibid, p 82

[3] Ibid, p 175 and 176

3 Introduction

The following definition is provided for the legal framework: the establishment of the PROTECT-CHILD DataSpace (M1-M24) [UDGA]. The objective of the task is to encourage collaboration and co-creation between healthcare professionals, health policymakers, legal and ethical experts, with a view to establishing an ethical and legal framework. The proposed framework is to comprise guidelines for data controllership, data processing, and ethical approval agreement templates. The objective is to enable the effective use of Electronic Health Data (EHD) within the framework of EHDS, thereby fostering confidence in the dissemination and reuse of health data for both research and healthcare purposes. The task at hand is to establish the fundamental principles underpinning the development of Secure Processing Environments (SPEs), which are defined as secure and reliable systems for the handling of sensitive information. The following principles will be defined and validated to ensure their effectiveness in governing and processing data securely.

D2.2 provides a comprehensive overview of the legal obligations and requirements of stakeholders in relation to the research project, along with a detailed analysis of their needs. The document provides a comprehensive overview of relevant legal and regulatory frameworks. It also delineates the specific requirements and constraints of stakeholders such as researchers, clinicians, patients, regulatory bodies, and industry partners. Furthermore, the deliverable explores the legal framework, incorporating data protection laws, medical ethics regulations, and clinical trial guidelines, thereby ensuring the project's adherence to all relevant legal and ethical standards. A comprehensive set of detailed provisions for data governance, privacy protection and ethical considerations is provided with the aim of safeguarding the rights and welfare of participants. Moreover, the document assesses potential risks and proposes mitigation strategies to address legal, regulatory, and stakeholder-related challenges, ensuring the project's execution is both efficient and ethical throughout its lifecycle. In essence, the function of Deliverable D2.2 is to serve as a foundational document that facilitates the navigation of the intricate dynamics inherent in the complex interplay of stakeholders.

4 Regulatory Framework

This section provides a comprehensive overview and further assessment of the legislation applicable for the PROTECT-CHILD project. This assessment provides a detailed analysis of legislation relevant to the fields of data protection and data governance, cybersecurity, and Artificial Intelligence (AI), which has been identified the 1.2.7 and 1.2.8 of the Grant Agreement.[4] Firstly, this section dissects the relevant laws and highlights their applicability and relevance to the case, drawing attention to further obligations that project beneficiaries need to be aware of. Secondly, it provides an overview of the national implementations of EU laws of the involved beneficiaries' countries, together with any additional relevant national laws.

4.1 Data Protection and Data Governance

4.1.1 General Data Protection Regulation

The General Data Protection Regulation (GDPR) lays down rules on processing of personal data of individuals within the European Union,[5] no matter of the location of the data controller or processor, provided that the processing is related to the provision of goods or services to, or the monitoring of behaviour of, individuals within the EU.[6] The regulatory instrument does not apply to processing carried out for personal or household activities, for law enforcement purposes, by EU institutions and bodies, or in areas outside the scope of EU law such as national security.[7]

The data necessary for the conducting of the project PROTECT-CHILD are personal medical data collected from minors, which from the perspective of the GDPR presents various challenges. Any medical information can be considered personal data if it relates to an identifiable natural person, i.e. data subjects[8]. The data subjects in this case are the children selected for the PROJECT-CHILD study. Personal data related to the physical or mental health of a natural person, including the data related to provision of health care services, which can reveal information one's health status fall explicitly within the scope of this Regulation.[9] This data is considered special category of data under Article 9 GDPR, and its processing is by default prohibited. Its processing is only permitted if one of the exceptions to the general prohibition on data processing in Article 9.1 applies[10]. Data which are not considered as a special category of personal data can be processed if the controller or processor applies one of the bases listed in Article 6.

[4] Ibid, p 150

[5] European Parliament & Council of the European Union. (2016, April 27). Article 1. *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). Official Journal of the European Union*, L 119, 1–88.

[6] Ibid, Art 3

[7] Ibid, Art 2

[8] In order to determine whether a person is identifiable account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly (Rec. 26 GDPR)

[9] Ibid, Art 4 (15)

[10] It should also be noted that in order to process any category of personal data, one or more of the legal bases provided for in Article 6 must apply, and that this also applies to special categories of data. Therefore, in order to process special categories of data, one or more bases for legitimacy must be selected, together with one or more exceptions to the prohibition in Article 9.1 GDPR.

The legal basis relevant to this project are:

- Article 6(1)(a): the data subject has given consent,
- Article 6(1)(b): necessary for performance of a contract,
- Article 6(1)(c): compliance with legal obligation (such as compliance with EHDS),
- Article 6(1)(f): necessary for legitimate purposes (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child),
- Article 9(2)(a): the data subject has given explicit consent,
- Article 9(2)(i): necessary for reasons of public interest in the area of public health,
- Article 9(2)(j): necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State.

However, under the GDPR consent must be freely given, specific, informed, explicit, and unambiguous.[11] It must be a clear, affirmative action taken by the data subject, who has the right to withdraw their consent at any time (could result in issues during research projects).[12] This project involves minors and if one of the only grounds for data processing would be Article 6(1)(a) or Article 9(2)(a) the beneficiaries could face certain challenges. Firstly, GDPR refers to a consent of minor only in relation to information society services[13] Secondly, it must be said that consent for medical research purposes and consent under the GDPR are two different concepts. Therefore, it is advised to not rely on the two previously mentioned Articles (i.e., Article 6 and Article 9) as a sole basis for data processing, even though the beneficiaries obtained the consent from the legal/parental guardians of the data subjects.

Article 9(2)(j), "necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1)", should therefore serve as the main basis for data processing activities. Article 89 lays down safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. As previously noted, this Article is transposed by the Member States and therefore its phrasing can differ throughout the Union. The article states:

- Processing for archiving, scientific or historical research, or statistical purposes must include appropriate safeguards under the GDPR to protect data subjects' rights and freedoms. These safeguards must ensure technical and organisational measures, particularly to uphold data minimisation, such as pseudonymisation where suitable. If the purposes can be achieved without identifying individuals, they must be pursued in that way.

[11] Ibid, Recital (11)

[12] Ibid, Art 7(3)

[13] Ibid, Art 8.

- For archiving in the public interest, similar derogations may be allowed from Articles 15, 16, 18, 19, 20, and 21, under the same conditions.[14]

For further information, the following publication of the European Data Protection Board can be consulted:

1. Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak,[15]
2. EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research,[16]
3. Study on the appropriate safeguards under Article 89(1) GDPR for the processing of personal data for scientific research (Final report – commissioned by the EDPB - 2019),[17]

Furthermore, when processing data, the following principles should be met:

- **Principle of lawfulness, fairness and transparency:** data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.
- **Principle of data minimisation**: 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.
- **Principle of accuracy:** data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- **Principle of storage limitation**: data must be accurate and, where necessary, kept up to date.
- **Principle of integrity:** must be processed in a manner that ensures appropriate security of the personal data.
- **Principle of accountability**: the controller must be able to demonstrate compliance with the above-mentioned principles.[18]

According to Article 25 GDPR, data protection should be implemented by design and default.

---

[14] Ibid, Art 89

[15] European Data Protection Board. (2021, March 2). *Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak.* Retrieved from https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032020-processing-data-concerning-health-purpose_en

[16] European Data Protection Board. (2020, January 8). *Reply to the European Commission questionnaire on processing of personal data for scientific research.* Retrieved from https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_replyec_questionnaireresearch_final.pdf

[17] European Data Protection Board. (2022, February 4). *Legal study on appropriate safeguards under Article 89(1) GDPR for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes*. Retrieved from https://www.edpb.europa.eu/our-work-tools/our-documents/legal-study-appropriate-safeguards-under-article-891-gdpr-processing_en

[18] European Parliament & Council of the European Union. (2016, April 27). Article 5. *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). Official Journal of the European Union*, L 119, 1–88.

Moreover, under Article 32 GDPR, appropriate technical and organisational measures should be adopted to ensure a level of security appropriate to the possible risk. These measures should include:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.[19]

For further details, please consult the Guidelines 4/2019 on Article 25 Data Protection by Design and by Default.[20] The federated model that has been proposed for the PROTECT-CHILD project enhances data protection by design, as it ensures sensitive data remains within the secure perimeter of the source clinical institution. Nevertheless, other protective measures have to be implemented.

In case of a data breach, the GDPR imposes reporting obligations on the controllers to notify the competent authorities and the data subjects in accordance with Article 33 GDPR. Additionally, as the project involves new technologies such as data spaces and AI, and requires processing of large amount of sensitive data, where applicable, beneficiaries should conduct a data protection impact assessment in accordance with Article 35 GDPR. Furthermore, considering that the processing is carried out by public authorities and sensitive data is being processed, a data protection officer should be appointed by the relevant beneficiaries.[21] Lastly, as a few of the beneficiaries do not reside in the EU, special attention should be paid to any data transfers out of EU, in accordance with Chapter V GDPR.

4.1.1.1 Regulatory considerations

Data Protection Impact Assessment (Article 35)

1. The DPIA should be carried out before the processing activity begins.[22]
2. The controller should seek advice of a DPO[23]
3. It should be particularly triggered in the following cases:
    - Automated decision-making or profiling that significantly affects individuals,
    - Large-scale processing of sensitive data,
    - Systematic large-scale monitoring of publicly accessible areas[24]

[19] Ibid, Art 32 (1)

[20] European Data Protection Board. (2020, October 20). *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, version 2.0*. Retrieved from https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

[21] European Parliament & Council of the European Union. (2016, April 27). Article 37. *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). Official Journal of the European Union*, L 119, 1–88.

[22] Ibid, Art 35(1)

[23] Ibid, (2)

[24] Ibid, (3)

4. The DPIA should include the following information:
    - A systematic description of the envisaged processing operations and their purposes.
    - An assessment of the necessity and proportionality of the processing operations in relation to the purposes.
    - An assessment of the risks to the rights and freedoms of data subjects.
    - The measures used to address the risks, including safeguards, security measures, and mechanisms to ensure the protection of personal data.[25]
5. Compliance with a code of conduct has to be taken into account when assessing the impact of a data processing operation. This can be useful to demonstrate that adequate measures have been chosen or put in place, provided that the code of conduct is appropriate to the processing operation.[26]
6. Publishing of the DPIA is not mandatory but is highly encouraged by the EDPB.[27]

For more details, please consult the Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.[28]

Notification of obligation of a Data Breach

Notification of the supervisory authority (Article 33 GDPR):

1. Controller must notify the supervisory authority of a data breach latest in 72 hours after becoming aware of the data breach, unless the breach does not present high risk to the rights and freedoms of natural persons
2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.
3. The notification should include the following information:
    - Nature of the breach, including categories and approximate number of affected data subjects and records
    - Contact details of the data protection officer or other relevant contact point
    - Likely consequences of the breach
    - Measures taken or planned to address the breach and mitigate its impact
4. The data breaches should be documented by the controller.[29]

[25] Ibid, (7)

[26] European Commission. (2017, October 13). Page 16. *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (wp248rev.01). Retrieved from https://ec.europa.eu/newsroom/article29/items/611236

[27] European Commission. (2017, October 13). Page 18. *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (wp248rev.01). Retrieved from https://ec.europa.eu/newsroom/article29/items/611236

[28] European Commission. (2017, October 13). Page 19. *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (wp248rev.01). Retrieved from https://ec.europa.eu/newsroom/article29/items/611236

[29] European Parliament & Council of the European Union. (2016, April 27). Article 33. *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). Official Journal of the European Union*, L 119, 1–88.

Communication of personal data breach to the data subject (Article 34 GDPR)

1. Communication is mandatory to the data subjects by the controller when:
    - A data breach is likely to result in a high risk to the rights and freedoms of natural persons[30]
    - Communication must be in clear and plain language so it is understandable for the data subject and must include the details of the DPO, information about the consequences of the breach, and lastly, the measures taken or proposed to be taken by the controller to address the personal data breach.[31]
2. Communication is not necessary if the following conditions are met:
    - Application of appropriate technical and organisational measures (e.g., encryption) that render the data unintelligible to unauthorised persons.
    - Subsequent measures were taken to ensure the high risk to data subjects is no longer likely to materialise.
    - Disproportionate effort is required for individual communication; an alternative equally effective public notice is used instead.[32]

Third-Country Transfers

Transfers of data to non-EU countries or to international organisations (IO) are regulated by Chapter V GDPR, which lays down very strict rules for the controllers and the processors, so that the protection of the Regulation for data subjects is not undermined outside the EU.

Transfers could be based on adequacy decisions: when the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the IO in question ensures an adequate level of protection, it grants to that state, territory, or international organization and adequacy agreement. When the adequacy decision is in place, there is no need for a specific authorisation of a data transfer.[33]

Transfers in the absence of an adequacy decision: in case there is no adequacy decision in place, the processor or the controller must put in place appropriate safeguards to be able to conduct the data transfer to a third country or to an IO. These safeguards include:

- "a legally binding and enforceable instrument between public authorities or bodies;
- binding corporate rules in accordance with Article 47;
- standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);
- standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);
- an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights;

[30] Ibid, Art 34(1)

[31] Ibid, Art 34(2)

[32] Ibid, Art 34(3)

[33] Ibid, Art 45(1)

- an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights."[34]

4.1.2 European Health Data Space Regulation

The European Health Data Space Regulation (EHDS) is a Regulation which provides common rules, standards, and infrastructures and a governance framework, with a view to facilitating access to electronic health data for the purposes of primary use of electronic health data and secondary use of those data as well as establishing the European Health Data Space.[35]

Electronic health data encompasses both personal and non-personal data processed in electronic form.[36] Personal electronic health data refers to health and genetic data linked to an identifiable natural person.[37] On the other hand, non-personal electronic health data includes anonymised[38] health data or data that never can be tied back or are not related to a data subject.[39] This data can, according to the Regulation, be processed for two main uses:

1) The primary use refers to processing of electronic health data for the provision of healthcare (i.e., for assessment, maintenance or restoration of one's health).[40]
2) Secondary use refers to processing for purposes other than the initial purposes for which they were collected or produced, provided that the conditions under Chapter IV are met.[41]

The beneficiaries of the PROTECT-CHILD project shall comply with obligations related to secondary use when processing data collected from registries and repositories, where the data was originally stored for purposes other than the research in question.

[34] Ibid, Article 46(2).

[35] European Parliament & Council of the European Union. (2025, February 11). Art 1(1). *Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847*. *Official Journal of the European Union*, L 2025/327, 1–120

[36] Ibid, Art 2(2)(c)

[37] Ibid, Art 2(2)(a)

[38] On this point, partners are kindly reminded of the ongoing discussions surrounding Anonymization and Pseudonymization, particularly the points made on the limits of pseudonymized data's equivalence to personal data and the cases when pseudonymised data functions legally as anonymised data when there is no reasonable likelihood of re-identification.

Namely, it is understood that pseudonymisation requires a context assessment in each circumstance, but it provides flexibility in data processing when technical and organisational measures are in place to prevent re-identification. In short, the fact that data is pseudonymised does not automatically qualify it as personal data (opinion of the EDPS/EDPB) or as non-personal data; rather, it will depend on whether or not it would be a disproportionate effort for each potential data controller to re-identify the person to whom the data refers. This doctrine has been upheld by the ECJ with regard to both the GDPR and Regulation (EU) 2018/1725. For more information on this point, see ECJ, 4/09/2025 (C-413/23 P), SEPD/EDPB v. SRB/EC (Recitals 71-81). ECJ (General Court), 26/04/2023 (T-557/20); ECJ, 9/11/2023 (C-319/22) (Particularly, Rec. 45); ECJ, 7/03/2024 (C-341/22), and ECJ (6th Chamber), 7/03/2024.

[39] Ibid, Art 2(2)(b)

[40] Ibid, Art 2(2)(d)

[41] Ibid, Art 2(2)(e)

However, the beneficiaries will have different obligations under the Regulation as it distinguishes between two main actors - data holders and data users. A health data holder is any natural or legal person, public authority, agency, or other body operating in the healthcare or care sectors.[42] This includes, for example, hospitals, research institutions, companies developing medical technologies or wellness applications, reimbursement bodies, and EU institutions. To qualify as a health data holder, an entity must meet at least one of the following conditions:

- It has the legal right or obligation, under EU or national law, and acts as a controller or joint controller to process personal electronic health data. The purposes may include healthcare provision, public health, research, innovation, reimbursement, policymaking, official statistics, patient safety, or regulatory compliance.
- It has the ability to make available non-personal electronic health data, by controlling the technical design of a product or related services. This includes managing access to data, registering, providing, restricting, or exchanging such data.[43]

Therefore, the beneficiaries such as SERMAS, UKE, and ISMETT are to be considered as data holders.

Contrary, data users are defined as any natural or legal persons who have been granted lawful access to electronic health data for secondary use pursuant to a data permit, a health data request approval or an access approval by an authorised participant in HealthData@EU. These permits will be granted by health data access bodies, which are competent authorities established under national law.[44] An example of a data users within the PROTECT-CHILD project would be researchers accessing the data for analysis from the data space.

The categories of electronic health data that shall be shared by the data holders for secondary purposes are listed in Article 51 EHDS. The list includes electronic health data from Electronic Health Records,[45] data from medical registries and mortality registries,[46] human genetic, epigenomic and genomic data[47] etc. The purpose for secondary processing of health data applicable to this project can be found in Article 53(1)(e) EHDS:

> *"(e) scientific research related to health or care sectors that contributes to public health or health technology assessments, or ensures high levels of quality and safety of healthcare, of medicinal products or of medical devices, with the aim of benefiting end-users, such as patients, health professionals and health administrators, including:*
>
> *(i) development and innovation activities for products or services;*

[42] Ibid, Art 2(2)(t)

[43] Ibid, Art 2(2)(t)

[44] Ibid, (v)

[45] Ibid, Art 51(1)(a)

[46] Ibid, 2(2)(l)

[47] Ibid, (f)

(ii) training, testing and evaluation of algorithms, including in medical devices, in vitro diagnostic medical devices, AI systems and digital health applications."[48]

All the processing activities for secondary use should be consulted with Articles 53 and 54 EHDS. Other relevant provisions include:

- Article 60, which describes the duties of health data holders, which are as follows:
  - Provision of data upon request
  - Provision of data within a reasonable time, no later than 3 months after the receipt of the access
  - Provision of dataset description in accordance with Article 77 and (at minimum) annual checks of the accuracy of the dataset
  - Provision of access to quality/utility label documentation
  - Provision of access to non-personal data through trusted open public databases with robust, transparent, and sustainable governance and a transparent model of user access
- Article 61, which describes the duties of health data users, which are:
  - Access and processing of data only with a data permit, approved request, or authorised participant approval.
  - Not to make data accessible to third parties without a permit during the processing of the data
  - Making public the results or output of secondary use, including information relevant for the provision of healthcare, within 18 months of the completion of the processing of the electronic health data. These results must contain only anonymous data, so no re-identification is possible.
  - Informing the health data access body of any significant finding related to the health of the natural person whose data are included in the dataset
- Article 66 on data minimisation and purpose limitation
  - Similarly to the GDPR, EHDS ensures that the data processed is adequate, relevant and limited to what is necessary for clearly defined secondary purposes
- Article 71, which encompasses the right to opt out of secondary use for individuals
  - This opt-out mechanism should be accessible and easily understandable for the data subjects
- Article 73 on the use of a secure processing environment
  - Through which the data can be accessed
  - These environments should be protected by the measures listed in paragraph 1 of the Article
  - The PROTECT-CHILD project must comply with this Article as the EHDS capsules were designed as secure processing environments
- Section 4, which lays out the cross-border infrastructure enabling secondary use of health data across the EU
- Section 5, which addresses health data quality and utility standards for secondary use.

[48] Ibid, Art 53(1)(e)

4.1.3 Data Governance Act

The Data Governance Act (DGA) is a Regulation laying down rules on conditions of re-use of certain data held by public sector bodies, a notification and supervisory framework for the provision of data intermediation services, and registration of bodies pursuing data altruism.[49]

Federated nodes are local, decentralized data infrastructures, which are hosted locally, in this case, in university research centres or at hospitals. They enable data to remain at the source (such as in a hospital) and be accessed or queried remotely rather than moving all the data to a central repository. Since raw personal data never leaves the institution, this model is frequently used in health data projects to preserve data sovereignty and enhance privacy protection.[50] The act of uploading, organisation, and preparation of data for nodes does constitute a "processing activity" under Article 4 GDPR. The question remains whether the previously mentioned exception for data processing of sensitive data for (archival) research purposes does apply.[51] The exception is further developed in Article 89 GDPR, the form of transposition of which is left up to the Member States. This ambiguity could be covered by the Data Governance Act as it permits the "conditions for the re-use, within the Union, of certain categories of data held by public sector bodies".[52] Re-use of data is defined as "the use by natural or legal persons of data held by public sector bodies, for commercial or non-commercial purposes other than the initial purpose within the public task for which the data were produced."[53] Therefore, if the act of processing data for the data nodes by the public institutions, such as hospitals, was not covered by the GDPR, it would most likely be regulated under the DGA.

Chapter II of the Regulation concerns re-use of certain categories of protected data held by public sector bodies. It applies to the following categories of data:

- commercial confidentiality, including business, professional and company secrets;
- statistical confidentiality;
- the protection of intellectual property rights of third parties; or
- the protection of personal data, insofar as such data fall outside the scope of Directive (EU) 2019/1024.[54]

[49] European Parliament & Council of the European Union. (2022, May 30). Article 1(1). *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)*. *Official Journal of the European Union*, L 152, 1-44

[50] Zhan, S., Huang, L., Luo, G., Zheng, S., Gao, Z., & Chao, H.-C. (2025). A review on federated learning architectures for privacy-preserving AI: Lightweight and secure cloud–edge–end collaboration. *Electronics*, *14*(13), 2512. https://www.mdpi.com/2079-9292/14/13/2512

[51] European Parliament & Council of the European Union. (2016, April 27). Article 9(2)(j). *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)*. *Official Journal of the European Union*, L 119, 1–88.

[52] European Parliament & Council of the European Union. (2022, May 30). Article 1(1). *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)*. *Official Journal of the European Union*, L 152, 1-44

[53] Ibid, Art 2(2)

[54] Ibid, Art 3 (1)

The Chapter also lays down rules on the prohibition of exclusive arrangements,[55] conditions for re-use of data,[56] and fees for their re-use.[57] Under the Article 5 of the DGA the re-use conditions must:

- be published by the public sector body,
- be fair (i.e. non-discriminatory, transparent, proportionate, and objectively justified),
- preserve data protection and confidentiality, under the safeguards of anonymisation, etc
- establish security controls over the data processing, and establish confidentiality and re-identification bans,
- follow rules for third-country transfers,
- provide special protection for highly sensitive data. [58]

4.1.4 Data Act

The Data Act (DA) establishes harmonised rules for data access and sharing across the EU. It covers the availability of product and service data to users, data sharing between data holders and recipients, facilitates switching between data processing services, introduces safeguards against unlawful access to non-personal data, and promotes interoperability through common standards for data access, transfer, and use.[59]

The DA serves as a complementary instrument to the GDPR. Nevertheless, unlike the GDPR, it also covers non-personal data. The Regulation is significant for PROTECT-CHILD as it applies to "data holders, irrespective of their place of establishment, that make data available to data recipients in the Union."[60] Data holders are defined as natural or legal persons who have the legal right or duty to use and share data they have obtained or generated, including product or service data.[61] Consequently, the beneficiaries providing the data for this project, such as the hospitals, will most likely be considered "data holders." Moreover, the Regulation applies to "data recipients in the Union to whom data are made available."[62] Data recipients are defined as a natural or legal persons (not the user) to whom the data holder makes data available, either at the user's request or due to a legal obligation.[63] In this project, which could include researchers, public authorities, or partner institutions accessing data through PROTECT-CHILD under predefined rules. Lastly, it also applies to "participants in data spaces and vendors of applications using smart contracts and persons whose trade, business or profession involves the deployment of smart contracts for others in the context of executing an agreement."[64] This application case illustrates the interaction between the EHDS and the Data Act, with the EHDS functioning as *lex specialis* for health-related data spaces.

[55] Ibid, Art 4

[56] Ibid, Art 5

[57] Ibid, Art 6

[58] Ibid, Art 5

[59] European Parliament & Council of the European Union. (2023, December 13). Article 1(1). *Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act)*. *Official Journal of the European Union*, L 2023, 1–64.

[60] Ibid, Art 1(3)(c)

[61] Ibid, Art 1 (13)

[62] Ibid, Art 1(3)(d)

[63] Ibid, Art 1 (14)

[64] Ibid, Art 1(3)(g)

The most relevant Article is in this case Article 33 DA, which lays down rules on the interoperability of data spaces. It therefore obliges anyone offering a data or data services in data spaces in scientific research to ensure their systems and datasets are interoperable. This can be achieved through ensuring:

- Clear documentation of the content, quality, licensing and collection method of the datasets,
- Consistent structuring of the data formats, vocabularies, and taxonomies,
- Technical accessibility of the data through defined interfaces, accompanied with information on how to use them,
- The interoperability of smart contracts or data-sharing tools if they are utilised.[65]

4.2 Artificial Intelligence Act and Digital Services Act

4.2.1 Artificial Intelligence Act

The Artificial Intelligence Act (AI Act) is the European Union's first legislative framework that addresses artificial intelligence systems deployed and sold on the internal market. Its primary objective is to promote human-centric and trustworthy artificial intelligence (AI) by ensuring strong protection of health, safety, and fundamental rights as set out in the Charter, while guarding against the harmful effects of AI systems within the Union and fostering innovation.[66]

As previously mentioned, the federated algorithms will provide functionalities such as cohort selection, data cleaning, imputation, statistical analysis, and machine learning. These algorithms are designed to operate in a distributed environment under strict privacy and security requirements, ensuring that sensitive data remains at their source. They will also generate standardized analysis templates for automated and reproducible use across participating sites

From an initial evaluation of the AI system and its tasks, it should not classify as general-purpose AI model, nor prohibited, high-risk, or limited risk AI systems. Therefore, the technology should be classified as minimal risk, which means that it is not subject to specific mandatory obligations laid down in this Act. The Ethical Self-Assessment of the project included in the Grant Agreement states that the “use of AI in this project does not raise any ethical concerns related to human rights and values.”[67]

The fact that the AI system is exempt for the obligations laid down by the AI does however, not exempt the algorithms from complying with privacy and data protection requirements under the GDPR and relevant cybersecurity legislation, as they process sensitive health data.

[65] Ibid, Art 33(1)

[66] European Parliament and of the Council. (2024, June 13) Art 1(1). Regulation (EU) 2024/1684 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence 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), OJ L 22024/1689, 12.7.2024

[67] European Health and Digital Executive Agency. (2024). Page 170. *Grant Agreement: PROTECT-CHILD* (Grant Agreement No. 101137423). Brussels, Belgium

4.2.2 Digital Services Act

As for the DSA, there are some potential interplays between the instrument and EHDs, though most of them remain theoretical at this stage. It should be noted, that, in order to decide about its applicability, the development of the project must be overseen. For example, the DSA may become relevant depending on the final deployment of the PROTECT-CHILD platform. It could apply indirectly, particularly in relation to algorithmic transparency obligations, if the platform is deployed and accessible to public.

4.3 Cybersecurity

4.3.1 Cyber Resilience Act

The Cyber Resilience Act (CRA) is a regulation laying down rules regarding the cybersecurity of products with digital elements deployed on the internal market.[68] It very likely that a component within the data space of the project could be considered as a product with digital element under the CRA, which is defined as a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately.[69] The act differentiates between important products with digital elements (listed in Annex III)[70] and critical products with digital elements (listed in Annex 4).[71]

The Act divides the obligations into pre- and post-market. Therefore, different beneficiaries could be subject to different obligations. Pre-market obligations apply mainly to manufacturers, nevertheless, they hold continual responsibility. Consequently, the obligations of the beneficiaries depend on their role of a manufacturer,[72] importer,[73] or distributor.[74]

Table 2. Obligations for Different Actors

Obligations	Manufacturer	Importer	Distributor
Product design and risk analysis	Yes	No	No
Conformity assessment	Yes	No	No
Technical documentation	Yes	No	No
CE marking	Yes	No	No

[68] European Parliament & Council of the European Union. (2024, October 23). Article 1. *Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act). Official Journal of the European Union*, L 2847, 1–52

[69] Ibid, Art 3(1).

[70] Ibid, Art 7

[71] Ibid, Art 8

[72] Ibid, Art 3(12)

[73] Ibid, (16)

[74] Ibid, (17)

Security monitoring and updates	Yes	Yes, if they are aware	Yes, if they are aware
Incident/vulnerability reporting	Yes	Yes, if they are aware	Yes, if they are aware
Market surveillance / Cooperation	Yes	Yes	Yes

Annex I of the Act lists all the essential cybersecurity requirements and vulnerability handling requirements. Moreover, Annex V provides the information necessary for EU declaration of conformity. Furthermore, Annex VII lays down all the information that need to be included in the technical documentation for products with digital element. Lastly, Annex VIII describes the conformity assessment procedure.

4.3.2 NIS2 Directive

The NIS2 Directive (NIS2) lays down measures that aim to achieve a high common level of cybersecurity across the Union, with a view to improving the functioning of the internal market.[75] The scope of the NIS2 Directive is laid down in Article 2 and Annex I and II. Research organisations[76] can fall within if they are providing its services in the EU and classify as medium-sized enterprises or bigger entities, or if their description falls within one of the categories listed in Article 2(2) NIS2. Furthermore, according to paragraph 5(b) of the Article, Member States can decide to apply the Directive to education institutions, in particular where they carry out critical research activities. Consequently, universities who act as beneficiaries in this project, residing in the Member States, should verify what the national implementation of the NIS2 Directive states. In case the beneficiaries identify themselves as subjects to the NIS2, they should implement appropriate and proportionate technical, operational, and organisational cybersecurity risk-management measures, listed in Article 21 NIS2. The measures should help manage the risks posed to the security of network and information systems which the entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services.[77] Lastly, entities who are subject to the Directive have reporting obligations under Article 23 NIS2. Therefore, in case of a security incident that has a significant impact on the provision of their services, entities must notify its CSIRT or its competent authority without undue delay.[78] If the incident would impact the users of the services, they also have to be notified.[79]

4.3.2.1 Regulatory considerations

Cybersecurity measures:

[75] European Parliament & Council of the European Union. (2022, December 14). *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). Official Journal of the European Union*, L 333, 80–152.

[76] Ibid, Annex II (7.)

[77] Ibid, Art 21(1)

[78] Ibid, Art 23 (1)

[79] Ibid

NIS2 set the following measures as minimum level of protection:

- policies on risk analysis and information system security;
- incident handling;
- business continuity, such as backup management and disaster recovery, and crisis management;
- supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
- security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
- policies and procedures to assess the effectiveness of cybersecurity risk-management measures;
- basic cyber hygiene practices and cybersecurity training;
- policies and procedures regarding the use of cryptography and, where appropriate, encryption;
- human resources security, access control policies and asset management;
- the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.[80]

The Directive also refers to international and European standards as a source of examples of cybersecurity measures. Standards such as ISO, NIST or ENISA guidelines can be consulted. More specifically, ENISA has drafted the NIS2 Technical implementation guidance, which provides entities with details about putting Article 21-23 in practice.[81]

Reporting Cybersecurity Incident

1. Identify whether the incident was significant.
    - An incident is considered significant, if:
        i. it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;
        ii. it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.[82]
2. Cross-border/ cross-sector coordination
    - In the case of a cross-border or cross-sectoral significant incident, Member States shall ensure that their single points of contact are provided in due time with relevant information. [83]
3. Early warning: Notification of CSIRT or competent authority within 24 hours after becoming aware
    - Without undue delay, and in any event within 24 hours of becoming aware of the significant incident, an early warning shall be issued. Where applicable, this

[80] Ibid, Art 21(2)

[81] European Union Agency for Cybersecurity. (2023). *NIS 2 technical implementation guidance*. Retrieved from https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance

[82] European Parliament & Council of the European Union. (2022, December 14). Article 23(3). *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). Official Journal of the European Union*, L 333, 80–152. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555

[83] Ibid, Art 23 (1) and (5)

warning shall indicate whether the significant incident is suspected to have been caused by unlawful or malicious acts, or whether it could have a cross-border impact.[84]

4. Notification of affected users or service recipients
    - Users and service recipients need to be informed about any measures or remedies which they can apply themselves to remediate the threat. Where appropriate, the entities shall also inform those recipients of the significant cyber threat itself.[85]
5. Incident notification within 72 hours
    - Without undue delay, and in any event within 72 hours of becoming aware of the significant incident, an incident notification shall be provided. Where applicable, this notification shall update the information provided in the early warning and indicate an initial assessment of the significant incident. This assessment shall include an indication of the incident's severity and impact, as well as the indicators of compromise, where available.[86]
6. (Optional) Intermediate Report
    - Must be provided after a request from the CSIRT or a competent authority.[87]
7. Final Report within 1 month after the submission of the early warning
    - Must include:
        - a detailed description of the incident, including its severity and impact;
        - the type of threat or root cause that is likely to have triggered the incident;
        - applied and ongoing mitigation measures;
        - where applicable, the cross-border impact of the incident.[88]

4.4 Legislation applicable to EU Beneficiaries

4.4.1 EU Member States Legislation

4.4.1.1 Spain

<table>
<tr><th>European Legislation</th><th colspan="3">National Implementation</th></tr>
<tr><td rowspan="4">GDPR</td><td colspan="3">Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)</td></tr>
<tr><td>Age of Consent</td><td colspan="2">14</td></tr>
<tr><td>Research exception:</td><td colspan="2">Disposición adicional decimoséptima of the LOPDGDD</td></tr>
<tr><td>DPA</td><td>AEPD[89]</td><td>○ Guidelines on Generation of</td></tr>
</table>

[84] Ibid, Art (4)(a)

[85] Ibid, Art 23(1)-(2).

[86] Ibid, Art 23(4)(b)

[87] Ibid, 23(4)(c)

[88] Ibid, (4)(d)

[89] Agencia Española de Protección de Datos. *Informes y resoluciones: Informes jurídicos*. Retrieved from https://www.aepd.es/informes-y-resoluciones/informes-juridicos?f%5B0%5D=conceptos%3A1418

European Legislation	National Implementation		
			Synthetic Data (Spanish)[90] ○ Guidelines on Approaching data spaces from the perspective of the GDPR (Spanish) [91] ○ Guidelines on Compliance with GDPR of treatments that incorporate Artificial Intelligence (Spanish) [92] ○ Guidelines on The adoption of pseudonymization techniques: The case of the healthcare sector (Spanish)[93] ○ Guidelines on LOPD: New obligations for the Public Sector (Spanish)[94] ○ Guidelines on LOPD: News for the Private Sector (Spanish)[95] ○ Infographic: information on consent to process personal data of minors[96] ○ Legal report on access to the medical history of minors (Spanish)[97]
AI Act	Draft approved, under review[98]		

[90] Agencia Española de Protección de Datos. (2024). *Guía sobre generación de datos sintéticos*. Retrieved from https://www.aepd.es/guias/guia-sobre-generacion-datos-sinteticos.pdf

[91] Agencia Española de Protección de Datos. (2024). *Aproximación a los espacios de datos y el RGPD*. Retrieved from https://www.aepd.es/guias/aproximacion-espacios-datos-rgpd.pdf

[92] Agencia Española de Protección de Datos. (2024). *Adecuación del RGPD a la inteligencia artificial*. Retrieved from https://www.aepd.es/guias/adecuacion-rgpd-ia.pdf

[93] Agencia Española de Protección de Datos & European Union Agency for Cybersecurity. (2024). *Técnicas de seudonimización en el sector sanitario*. Retrieved from https://www.aepd.es/documento/tecnicas-seudonimizacion-sector-sanitario-enisa.pdf

[94] Agencia Española de Protección de Datos. *Novedades LOPD sector público*. Retrieved from https://www.aepd.es/guias/novedades-lopd-sector-publico.pdf

[95] Agencia Española de Protección de Datos. *Novedades LOPD sector privado*. Retrieved from https://www.aepd.es/guias/novedades-lopd-sector-privado.pdf

[96] Agencia Española de Protección de Datos. *Infografía: Consentimiento de menores*. Retrieved from https://www.aepd.es/infografias/infografia-consentimiento-menores.pdf

[97] Ibid

[98] DLA Piper. (2025, February 28). *Spanish government approves draft law for ethical, inclusive and beneficial use of artificial intelligence*. Retrieved from https://knowledge.dlapiper.com/dlapiperknowledge/globalemploymentlatestdevelopments/2025/spanish-government-approved-draft-law-for-ethical-inclusive-and-beneficial-use-of-artificial-intelligence

European Legislation	National Implementation
EHDS Regulation	Reglamento (UE) 2025/327 del Parlamento Europeo y del Consejo, de 11 de febrero de 2025, relativo al Espacio Europeo de Datos de Salud, y por el que se modifican la Directiva 2011/24/UE y el Reglamento (UE) 2024/2847, in BOE 327[99]
DSA	Not applicable (Directive)
DGA	Applicable, amendments to the Law 37/2007, of 16 November 2007, on the re-use of public sector information.
DA	Not applicable (Directive)
NIS2 Directive	Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2)[100] + Reglamento de Ejecución (UE) 2024/2690 de la Comisión[101]
CRA	Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) nº 168/2013 y el Reglamento (UE) 2019/1020 y la Directiva (UE) 2020/1828 (Reglamento de Ciberresiliencia)[102]
National Legislation – Sector	**Name**

[99] Spain. (2025, February 20). *Reglamento (UE) 2025/327 del Parlamento Europeo y del Consejo, de 11 de febrero de 2025, relativo al Espacio Europeo de Datos de Salud, y por el que se modifican la Directiva 2011/24/UE y el Reglamento (UE) 2024/2847*. Retrieved from https://www.boe.es/buscar/doc.php?id=DOUE-L-2025-80382

[100] Spain. (2022, December 27) *Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2)*. Retrieved from https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81963

[101] Spain. (2025, March 5). *Reglamento de Ejecución (UE) 2024/2690 de la Comisión, de 17 de octubre de 2024, por el que se establecen las disposiciones de aplicación de la Directiva (UE) 2022/2555 en lo que respecta a los requisitos técnicos y metodológicos de las medidas para la gestión de riesgos de ciberseguridad y en el que se detallan los casos en que un incidente se considera significativo con respecto a los proveedores de servicios de DNS, los registros de nombres de dominio de primer nivel, los proveedores de servicios de computación en nube, los proveedores de servicios de centro de datos, los proveedores de redes de distribución de contenidos, los proveedores de servicios gestionados, los proveedores de servicios de seguridad gestionados, los proveedores de mercados en línea, motores de búsqueda en línea y plataformas de servicios de redes sociales, y los proveedores de servicios de confianza*. Retrieved from https://www.boe.es/buscar/doc.php?id=DOUE-L-2024-81540

[102] European Union. (2024, November 20). *Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Regulation)* (OJ L 2847, 20.11.2024, pp. 1–81). Retrieved from https://www.boe.es/buscar/doc.php?id=DOUE-L-2024-81720

European Legislation	National Implementation
Medical Sector	Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica (Art 3, 8(4), 16)[103]
Open Data	Law 37/2007 of 16 November on the reuse of public sector information[104]
	Law 18/2015, of 9 July, amending Law 37/2007, of 16 November, on the reuse of public sector information[105]

4.4.1.2 Italy

European Legislation	National Implementation		
GDPR	Codice in materia di protezione dei dati personali		
	Age of Consent:	14	
	Research exception:	Article 105 of the Code	
	DPA:	Garante per la protezione dei dati personali[106]	○ Handbook: Right to be forgotten in oncology (Italian)[107] ○ Guidelines on cookies (english)[108] ○ Guidelines on the Electronic Health Record and the Health File - 16 July 2009 [1672821] (English)[109]

[103] Spain. (2002, November 14). *Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica*. (BOE No. 274, 15.11.2002). Retrieved from https://www.boe.es/buscar/act.php?id=BOE-A-2002-22188

[104] Spain. (2007, November 16). *Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público*. (BOE No. 276, 17.11.2007). Retrieved from https://boe.es/buscar/act.php?id=BOE-A-2007-19814

[105] Spain. (2011, October 24). *Real Decreto 1495/2011, de 24 de octubre, por el que se desarrolla la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, para el ámbito del sector público estatal*. (BOE No. 269, 08.11.2011). Retrieved from https://boe.es/buscar/act.php?id=BOE-A-2011-17560

[106] Garante per la protezione dei dati personali. *Oblio oncologico (Oncology "Right to Be Forgotten")*. Retrieved from https://www.garanteprivacy.it/temi/sanita-e-ricerca-scientifica/oblio-oncologico

[107] Garante per la protezione dei dati personali. *Main decisions*. Retrieved from https://www.garanteprivacy.it/web/garante-privacy-en/main-decisions

[108] Garante per la protezione dei dati personali. (2021, July 10). *Linee guida in materia di cookie e altri strumenti di tracciamento* (Doc. web n. 9677876). Retrieved from https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9677876

[109] Garante per la protezione dei dati personali. (2009, August 3). *Linee guida in tema di fascicolo sanitario elettronico (FSE)* (Doc. web n. 1672821). Retrieved from https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1672821

European Legislation	National Implementation		
			○ Guidelines on Online Examination Records (English)[110] ○ Guidelines on Cookies and Other Tracking Tools - June 10, 2021 [9677876] (English)[111]
AI Act	Atto Senato n. 1146-B[112]		
EHDS Regulation	implemented in Gazzete Ufficiale Anno 166-No 53[113]		
DSA	implemented, (transl.) LEGISLATIVE DECREE No. 50 of March 25, 2024. Supplementary and corrective provisions of Legislative Decree No. 208 of November 8, 2021, containing the consolidated text of audiovisual media services, taking into account the evolution of market realities implementing Directive (EU) , 2018/1808 amending Directive 2010/13/EU, in Gazzete Ufficiale Anno 165-No 90[114]		
DGA	implemented, (transl.) LEGISLATIVE DECREE No. 144 of October 7, 2024. Rules for adapting national legislation to the provisions of 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, in Gazzete Ufficiale Anno 165-No 238[115]		
DA	Not implemented		
NIS2 Directive	Transposition of Directive (EU) 2022/2555 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, in Gazzete Ufficiale Anno 165 – Numero 230[116]		

[110] Garante per la protezione dei dati personali. (2009, November 19). *Linee guida in tema di referti on-line* (Doc. web n. 1683328). Retrieved from https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1683328

[111] Presidenza del Consiglio dei Ministri – Dipartimento della Protezione Civile. (2024, February 26). *Decreto 26 febbraio 2024: Approvazione del Piano straordinario di analisi della vulnerabilità delle zone …* (GU Serie Generale n. 90, 17-04-2024). Retrieved from https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9677876

[112] Ministero dell'Economia e delle Finanze. (2025, February 27). *Decreto 27 febbraio 2025: Riapertura delle operazioni di sottoscrizione dei certificati di credito del Tesoro indicizzati al tasso Euribor a sei mesi ("CCTeu"), godimento 15 ottobre 2024, scadenza 15 aprile 2033, quinta e sesta tranche* (Gazzetta Ufficiale, Serie Generale, No. 53 del 05-03-2025). Retrieved from https://www.senato.it/leggi-e-documenti/disegni-di-legge/scheda-ddl?tab=datiGenerali&did=59313

[113] Repubblica Italiana. (2024, March 25). *Decreto Legislativo 25 marzo 2024, n. 50: Disposizioni integrative e correttive …* (GU Serie Generale n. 90, 17-04-2024). Retrieved from https://www.gazzettaufficiale.it/eli/gu/2024/04/17/90/sg/pdf

[114] Ministero della Salute. (2024, December 31). *Decreto 31 dicembre 2024: Istituzione dell'Ecosistema dati sanitari* (GU Serie Generale n. 53, 05-03-2025). Retrieved from https://www.gazzettaufficiale.it/eli/gu/2025/03/05/53/sg/pdf

[115] Repubblica Italiana. (2024, October 7). *Decreto Legislativo 7 ottobre 2024, n. 144: Norme di adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2022/868 (Data Governance Act)* (Gazzetta Ufficiale, Serie Generale, n. 238). Retrieved from https://www.gazzettaufficiale.it/eli/id/2024/10/10/24G00167/SG

[116] Repubblica Italiana. (2024, October 1). *Decreto-Legge 1 ottobre 2024, n. 137: Misure urgenti per contrastare i fenomeni di violenza nei confronti dei professionisti sanitari…* (Gazzetta Ufficiale, Serie Generale, n. 230). Retrieved from https://www.gazzettaufficiale.it/eli/gu/2024/10/01/230/sg/pdf

European Legislation	National Implementation
CRA	Not implemented

4.4.1.3 Greece

European Legislation	National Implementation	
GDPR	Law 4624/2019 which also contains provisions for the implementation of Directive (EU) 2016/680 and Data Protection Act 2019	
	Age of Consent	15
	Research Exception	Article 30 of the Data Protection Act 2019
	DPA	HDPA
AI Act	Not implemented	
EHDS Regulation	Not implemented	
DSA	Law 5099/2024 on adoption of measures for the implementation of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on the single market for digital services[117]	
DGA	Law 5188/2025 on measures implementing EU Regulation 2022/868 (Data Governance Act – DGA) was published in the Official Government Gazette of the Hellenic Republic[118]	
DA	Not implemented	
NIS2 Directive	Law 5160/2024[119]	
CRA	Not implemented	
National Legislation – Sector	**Name**	
Technologies	Law 4961/2022 regulates emerging technologies like AI, IoT, and 3D printing to ensure their safe, lawful use. It aims to modernize public	

[117] Baker McKenzie Resource Hub. *Key Data & Cybersecurity Laws—Greece*. Retrieved from https://resourcehub.bakermckenzie.com/en/resources/global-data-and-cyber-handbook/emea/greece/topics/key-data-and-cybersecurity-laws

[118] Law No. 5188: Measures for the implementation of Regulation (EU) 2022/868 (Data Governance Act) – Designation of competent authority for Regulation (EU) 2024/903 (Interoperable Europe Regulation). Retrieved from https://search.et.gr/el/fek/?fekId=779379

[119] Zeya. (2025, May 12). *Greece adopts national cybersecurity requirements framework*. Retrieved from https://www.zeya.com/newsletters/greece-adopts-national-cybersecurity-requirements-framework

	services, enhance digital governance, and promote Greece's digital transformation[120]

4.4.1.4 The Netherlands

European Legislation	National Implementation		
GDPR	Uitvoeringswet Algemene verordening gegevensbescherming (UAVG)		
	Age of Consent	16, except for consent for other support and advisory services offered directly and for free to a minor = no limit	
	Research exception	Art 44 UAVG and Articles 15, 16, 18 GDPR	
	DPA	AP	○ Investigation into handling data breaches in youth care (English)[121] ○ Test Act on Strengthening Legal Protection in Youth Protection (Dutch)[122] ○ Other documents accessible in the Archive[123]
AI Act	Not implemented		
EHDS Regulation	Not implemented		
DSA	Uitvoering van verordening (EU) 2022/2065 van het Europees Parlement en de Raad van 19 oktober 2022 betreffende een eengemaakte markt voor digitale diensten en tot wijziging van Richtlijn 2000/31/EG (Uitvoeringswet digitaledienstenverordening[124]		

[120] OECD AI Policy Observatory. (2025, Month Day). *Law 4961/2022: Emerging information and communication technologies and societies—enhancing digital governance and other provisions*. Retrieved from https://oecd.ai/en/dashboards/policy-initiatives/law-n-49612022-emerging-information-and-communication-technologies-and-societies-enhancing-digital-governance-and-other-provisions-3368

[121] Autoriteit Persoonsgegevens. (2025, March 27). *Investigation into handling data breaches in youth care*. Dutch Data Protection Authority. Retrieved from https://www.autoriteitpersoonsgegevens.nl/en/documents/investigation-into-handling-data-breaches-in-youth-care

[122] Autoriteit Persoonsgegevens. (2025, March 19). *Toets Wet versterking rechtsbescherming in de jeugdbescherming*. Retrieved from https://www.autoriteitpersoonsgegevens.nl/documenten/toets-wet-versterking-rechtsbescherming-in-de-jeugdbescherming

[123] Autoriteit Persoonsgegevens – Archief. *Archive overview*. Retrieved from https://autoriteitpersoonsgegevens.archiefweb.eu/#archive

[124] Parliament of the Netherlands. (2024). *Kamerstuk KST-36531-5*. Retrieved from https://zoek.officielebekendmakingen.nl/kst-36531-5.html

European Legislation	National Implementation
DGA	Not implemented yet, preliminary registration of data intermediation service[125]
DA	Publication of the proposal
NIS2 Directive	Drafting in progress, Council of State advice issued, for updated information please check the footnote[126]
CRA	Wet tot uitvoering van Verordening (EU) 2024/2847 van het Europees Parlement en de Raad van 23 oktober 2024 betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordeningen (EU) nr. 168/2013 en (EU) 2019/1020 en Richtlijn (EU) 2020/1828 (Uitvoeringswet verordening cyberweerbaarheid) VOORSTEL VAN WET[127] The consultation period has closed, the Bill is still a draft.

4.4.1.5 Germany

European Legislation	National Implementation	
GDPR	Bundesdatenschutzgesetz (BDSG)	
	Age of Consent	16[128]
	DPA	BfDI
AI Act	Not implemented	
EHDS Regulation	Not implemented	
DSA	German Digital Services Act (DDG)[129]	

[125] Netherlands Enterprise Agency. *Mandatory registration of data intermediation service (DGA)*. Retrieved from https://business.gov.nl/regulation/mandatory-registration-data-intermediation-service-dga

[126] Government of the Netherlands. *Regeling WGK014627*. Retrieved from https://wetgevingskalender.overheid.nl/Regeling/WGK014627

[127] Wet tot uitvoering van Verordening (EU) 2024/2847 van het Europees Parlement en de Raad van 23 oktober 2024 betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordeningen (EU) nr. 168/2013 en (EU) 2019/1020 en Richtlijn (EU) 2020/1828 (Uitvoeringswet verordening cyberweerbaarheid) VOORSTEL VAN WET). Retrieved from: https://www.rijksoverheid.nl/actueel/nieuws/2025/03/10/internetconsultatie-uitvoeringswet-verordening-cyberweerbaarheid-van-start .

[128] Linklaters. *Data Protected – Germany*. Retrieved from https://www.linklaters.com/insights/data-protected/data-protected---germany#:~:text=Are%20there%20any%20special%20rules,the%20field%20of%20employment%20law

[129] Taylor Wessing. (2024, May 14). *DDG lays the foundation for enforcing the EU Digital Services Act in Germany*. Retrieved from https://www.taylorwessing.com/en/insights-and-events/insights/2024/05/ddg#:~:text=Proclaimed%20on%20May%2013%2C%202024

European Legislation	National Implementation
DGA	Draft[130]
DA	Not implemented
NIS2 Directive	Not implemented
CRA	Not implemented
National Guidelines - Sector	**Name**
Data Protection	Guidelines on the Protection of Health Data (in German)[131]

4.4.1.6 Belgium

European Legislation	National Implementation		
GDPR	Data Protection Act (2019)		
	Age of Consent	13	
	DPA	APD/GBA (L'Autorité de protection des données – Gegevensbeschermingsautoritei)[132]	○ Opinion No 52/2024 of May 17 2024 Preliminary draft royal decree on access to health data (Dutch)[133] ○ Opinion No. 83/2023 of 27 April 2023 Request for advice on a preliminary draft ordinance amending the ordinance of 4 April 2019 concerning the electronic exchange platform for health data (Dutch)[134] ○ Opinion No 110/2018 of October 17 2018 Draft

[130] CMS. (2025, April 28). *Capgemini and CMS: German Data Act Implementation Act – German Federal Network Agency to become enforcement authority*. Retrieved from https://cms-lawnow.com/en/ealerts/2025/04/capgemini-and-cms-german-data-act-implementation-act-german-federal-network-agency-to-become-enforcement-authority

[131] Federal Ministry for Economic Affairs and Climate Action.*Guidelines on the protection of health data*. Retrieved from https://www.bundeswirtschaftsministerium.de/Redaktion/EN/Dossier/guidelines-on-the-protection-of-health-data.html

[132] Linklaters. (2024, March). *Data Protected – Belgium*. Retrieved from https://www.linklaters.com/en/insights/data-protected/data-protected---belgium

[133] Gegevensbeschermingsautoriteit. (2024, May 17). *Advies nr. 52/2024 van 17 mei 2024: Voorontwerp van koninklijk besluit over de toegang tot gezondheidsgegevens* (Advies nr. 52/2024). Retrieved from https://www.gegevensbeschermingsautoriteit.be/publications/advies-nr.-52-2024.pdf

[134] Gegevensbeschermingsautoriteit. (2023, April 27). *Advies nr. 83/2023 van 27 april 2023: Voorontwerp van ordonnantie betreffende het elektronisch uitwisselingsplatform voor gezondheidsgegevens* (Advies nr. 83/2023). Retrieved from https://www.gegevensbeschermingsautoriteit.be/publications/advies-nr.-83-2023.pdf

European Legislation	National Implementation		
			Ordinance (GGC) on the electronic exchange platform for health data (Dutch)[135] ○ Opinion No 117/2018 of November 7 2018 request for advice on a draft legal basis for access to health data via an electronic platform (Dutch)[136] ○ Opinion No. 1/2005 of 10 January 2005 Draft Royal Decree concerning the organisation of cancer registration (Dutch)[137] ○ Opinion No. 36/2020 of 29 April 2020 establishing a database at Sciensano in the context of the fight against the spread of the coronavirus COVID-19[138]
AI Act	Not implemented		
EHDS Regulation	Not implemented		
DSA	Document parlementaire 55K3799, 31 janvier 2024: Projet de loi mettant en oeuvre le règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE, portant modifications du livre XII et du livre XV du Code de droit économique et portant modifications de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges.		
DGA	Adopted but no access to the legislation[139]		
DA	Not implemented		

[135] *Advies nr. 110–2018. (2018)*. Gegevensbeschermingsautoriteit. Retrieved from https://www.gegevensbeschermingsautoriteit.be/publications/advies-nr.-110-2018.pdf

[136] *Advies nr. 117–2018.* (2018). Gegevensbeschermingsautoriteit. Retrieved from https://www.gegevensbeschermingsautoriteit.be/publications/advies-nr.-117-2018.pdf

[137] *Advies nr. 1–2005.* (2005). Gegevensbeschermingsautoriteit. Retrieved from https://www.gegevensbeschermingsautoriteit.be/publications/advies-nr.-1-2005.pdf

[138] *Advies nr. 36–2020.* (2020). Gegevensbeschermingsautoriteit. Retrieved from https://www.gegevensbeschermingsautoriteit.be/publications/advies-nr.-36-2020.pdf

[139] Brussels-Capital Region. (2023, October 31). *The challenges of the Data Governance Act*. Retrieved from https://be.brussels/en/about-region/challenges-data-governance-act

European Legislation	National Implementation
NIS2 Directive	Law of 26 April 2024 establishing a framework for the cybersecurity of networks and information systems of general interest for public security[140]
CRA	Not implemented

4.4.2 Legislation applicable to Non-EU States Beneficiaries

4.4.2.1 Serbia

Sector Legislation	Law
Data Protection	Serbian Data Protection Act (ZZPL = Zakon o zaštiti podataka o ličnosti), Official Gazette of RS no. 87/2018[141]
Medical	Clinical research in Serbia requires to appoint a DPO and a data representative[142] (Law on Personal Data Protection ("Official Gazette of RS" No. 97/08, 104/09 - other law, 68/12 – decision of the CC and 107/12))
AI	In the process of adopting a law + Belgrade Ministerial Declaration on Artificial Intelligence Adopted[143]

4.4.2.2 United States: the State of Georgia

Sector Specific Laws	Federal Law
Privacy	Children's Online Privacy Protection Act and regulations (COPPA)
Medical Privacy	HIPPA
	Federal standards protecting sensitive health information from disclosure without patient's consent

[140] Service public fédéral Chancellerie du Premier Ministre. (2024, April 26**).** *Loi établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique* (Moniteur belge, Numac 2024202344). Belgique: Auteur. Retrieved from https://www.ejustice.just.fgov.be/cgi/article.pl?language=fr&sum_date=2024-05-17&lg_txt=f&caller=sum&s_editie=1&2024202344=4&numac_search=2024202344&view_numac=2024202344f

[141] Ruzicic, I. (2024, July 5). *Data Protection Laws and Regulations in Serbia*. CEE Legal Matters. Retrieved from https://ceelegalmatters.com/data-protection-2024/serbia-data-protection-2024

[142] Đukanović, J., & Spasojević, D. (2025, February 20). *If you are doing clinical research in Serbia, you must appoint a Data Representative and/or a DPO*. Zunic Law. Retrieved from https://zuniclaw.com/en/clinical-research-in-serbia-data-representative-dpo/

[143] Government of Serbia. (2024, December 27). *Belgrade Ministerial Declaration on Artificial Intelligence adopted*. Retrieved from https://www.ai.gov.rs/vest/en/1419/belgrade-ministerial-declaration-on-artificial-intelligence-adopted.php

	Permitted uses and disclosure of medical information	Public interest and benefit activities: Health and oversight activities, public health activities, research under certain conditions, to prevent or lessen a serious threat to health or safety
Sector Specific Laws	**National Law**	
Data Protection	Law of Georgia on Personal Data Protection	

4.4.2.3 Switzerland

Sector Legislation	Law
Data Protection	Federal Act on Data Protection (FADP)
AI	The Swiss Federal Council decided that it does not support the implementation of broad, horizontal AI regulation in Switzerland.[144] Switzerland signed the Council of Europe's Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law and is now awaiting its ratification (awaiting ratification).[145]

[144] Dal Molin, L., Bühler, G., Wesiak-Schmidt, K., & Al Abiad, T. (2025, February 13). *Swiss AI regulation: Tailored rules instead of a Swiss AI Act*. Homburger AG. Retrieved from https://www.homburger.ch/en/insights/swiss-ai-regulation-tailored-rules-instead-of-a-swiss-ai-act

[145] Reuters. (2024, September 5). *US, Britain, EU to sign first international AI treaty* [News article]. Retrieved from https://www.coe.int/en/web/artificial-intelligence/-/switzerland-signs-the-council-of-europe-s-global-treaty-on-ai

5 Ethical Standards and their Application

5.1 Foundational Obligations from the Grant Agreement

The relevant Articles of the Grant Agreement for this part of the project are Articles 13 to 18 which are further elaborated on in Annex 5 of the Grant Agreement.

- Article 13 lays down rules regarding confidentiality and security for sensitive and EU classified information. [146]
- Article 14 mandates beneficiaries to comply with the relevant ethical principles and applicable EU and international law (listed in the Sections below). It highlights the necessity of paying attention to the principle of proportionality, the right to privacy, the right to the protection of personal data, the right to the physical and mental integrity of persons, the right to non-discrimination, the need to ensure protection of the environment and high levels of human health protection. Furthermore, it lists prohibited research activities.[147]
- Article 16 applies to intellectual property rights, access rights and rights to use.[148] This Article explains the rules on ownership and protection results, exploitation obligations, transfer and licensing, access rights and open science obligations.
- Article 17 covers dissemination and communication of the open science results and promotes the open science and open access principles.
- Lastly, Article 18 covers multiple topics, such as strategic restrictions, researchers' recruitment and working conditions, access to research infrastructure etc.

5.1.1 FAIR Principles

The FAIR principles should serve as guidelines to improvement the findability, accessibility, interoperability, and reuse of digital assets. The principles emphasize machine actionability. This means that computational systems should be able to find, access, work with, and reuse data with little or no human help. Humans are relying more on computers to manage data because the amount, complexity, and speed of data creation are growing.[149] These principles apply to data, metadata, and infrastructure.[150] The four concepts can be explained as follows:

1. Findable: first step is to find data which could be (re)used. Both computers and humans should be able to easily locate data and metadata. This is a crucial step in the FAIRification process since machine-readable metadata is necessary for the automatic discovery of datasets and services.

[146] European Health and Digital Executive Agency. (2024). Page 206. *Grant Agreement: PROTECT-CHILD* (Grant Agreement No. 101137423). Brussels, Belgium

[147] Ibid, Page 207

[148] Ibid, Page 208.

[149] GO FAIR. *FAIR Principles*. Retrieved from https://www.go-fair.org/fair-principles/ (go-fair.org)

[150] Ibid

2. Accessible: After locating the necessary information, the user must understand how to access it, possibly including authorization and authentication.
3. Interoperability: Data must be interoperable, which means that the data must be integrated with other data. The data must also work with workflows or applications for processing, storing and analysing.
4. Reusability: FAIR's ultimate objective is to maximize data reuse. This is accomplished by having well-described metadata and data that can be combined and/or replicated in various contexts.[151]

5.1.2 Open Access and Open Science Practices

The practice of Open Access requires unrestricted, online access to scientific information that is free of charge and reusable to the user, including peer-review publications, data underlying publications and publication of data sets.[152] On the other hand, Open Science is an approach to research that emphasises the sharing of knowledge, results and tools as early and widely as possible, based on open, cooperative work.[153] These practices have to be mandatorily applied in the Horizon Europe projects. Consequently, the beneficiaries must comply with the following obligations:

- Open Access to Publications:
  - Deposit peer-reviewed publications in a trusted, open repository at the latest at the time of publication.
  - Ensure immediate open access to the deposited publication via the repository, under CC BY license or license with equivalent rights.
  - Provide supporting information via the repository about any research output or any other tools and instruments needed to validate the conclusions of the scientific publication.
  - Retain sufficient IP rights to meet open access obligations.
  - Include open metadata under the Creative Common Public Domain Dedication (or equivalent), and provide information at least about the publication author(s), title, date of publication, publication venue, funding, grant project name, licensing, etc.[154]
- Research and Data Management:
  - Create and regularly update a Data Management Plan (DMP) in line with Fair principles.
  - Deposit data in a trusted repository within the deadlines set out in the DMP (EOSC-compliant if required).
  - Provide open access to data through the repository, under the latest available version of the Creative Commons Attribution International Public License (CC BY) or Creative Commons Public Domain Dedication (CC 0) or a licence with

[151] Ibid

[152] European Commission, Research Executive Agency. *Open science*.

[153] Ibid

[154] European Health and Digital Executive Agency. (2024). Page 216. *Grant Agreement: PROTECT-CHILD* (Grant Agreement No. 101137423). Brussels, Belgium

equivalent rights (following the "as open as possible as closed as necessary principle")[155]
    - Provide information via the repository about any research output or any other tools and instruments needed to re-use or validate the data.
    - Open metadata under the Creative Common Public Domain Dedication (or equivalent), and provide information at least about the publication author(s), title, date of publication, publication venue, funding, grant project name, licensing, etc.[156]
- Additional Open Science Practices:
    - Follow any extra obligations regarding open science practices imposed if imposed by call conditions.
    - If there is a call condition for a validation of scientific publications, the beneficiaries must provide (digital or physical) access to data or other results needed for validation of the conclusions of scientific publications
    - If there is a call condition for public emergencies, the beneficiaries must deposit outputs immediately and provide open access (or license under fair terms if open access is not possible)
    - Regularly update a plan for exploitation, dissemination, and communication.[157]

5.1.3 Informed and Freely Given Consent in Medical Research

Obtaining consent during medical research is one of the key principles of research ethics. It should be collected before the start of the research.[158] The consent needs to be freely given and informed. The process of informed consent serves two primary purposes: ethical and legal. Firstly, it serves to safeguard patient rights. Secondly, it fosters transparency between healthcare professionals and patients. Thirdly, it serves to promote trust between the aforementioned parties.[159] In order for the consent to qualified as informed, the patients must understand the risks, benefits, alternatives, and potential consequences of medical interventions, allowing them to weigh their options and participate actively in their treatment plans.[160] Conversely, children younger than 18 cannot provide informed consent, therefore the consent must be provided for them by their legal guardians.[161] Beneficiaries of the project who gather study participants' data must take this into account and offer a suitable consent procedure in accordance with this ethical standards.

[155] Results and data may be kept closed if making them public in open access is against the researcher's legitimate interests.

[156] European Health and Digital Executive Agency. (2024). Page 217. *Grant Agreement: PROTECT-CHILD* (Grant Agreement No. 101137423). Brussels, Belgium

[157] Ibid, Pages 217-218

[158] Shah, P., Thornton, I., Kopitnik, N. L., & Hipskind, J. E. (2025, January). *Informed Consent*. In StatPearls. StatPearls Publishing. Retrieved from https://www.ncbi.nlm.nih.gov/books/NBK430827/

[159] Ibid

[160] Ibid

[161] Ibid

This principle is laid down for example in the Declaration of Helsinki,[162] Universal Declaration on Bioethics and Human Rights,[163] Oviedo Convention,[164] and International Covenant on Civil and Political Rights.[165]

5.1.4 Ethical Management of Incidental Findings

Clinical research can result in incidental findings which fall outside of the scope of the principal research project. The disclosure of these finding can have a significant impact on the participants of the study mentally and physically.[166] Furthermore, they might uncover further information about participants' sex life, abuse or neglect, or drug- abuse.[167]

There is an ethical obligation to disclose any incidental finding in the EU.[168] Therefore, any results found incidentally during the PROTECT-CHILD project need to be reported to the participants and their legal guardians where necessary.

5.2 Ethics Guidelines for Trustworthy AI

The PROTECT-CHILD federated algorithms should be developed in accordance with Ethics Guidelines for Trustworthy AI. According to these principles AI should be complying with all applicable laws and regulations (lawful), ensuring adherence to ethical principles and values (ethical), and robust both from social and technical side.[169] Moreover, the AI must respect fundamental human rights and the following four ethical principles: (i) Respect for human autonomy, (ii) Prevention of harm, (iii) Fairness, and (iv) Explicability.[170]

To turn the high-level principles of Trustworthy AI into practice, concrete requirements must be applied across all stages of the AI system life cycle. These requirements guide the actions of developers**,** deployers**,** end-users and the span systemic, individual, and societal dimensions, covering:

[162] World Medical Association. (2024, October). Articles 25-32. *Declaration of Helsinki: Ethical principles for medical research involving human participants* (8th revision, adopted by the 75th WMA General Assembly). Retrieved from https://www.wma.net/policies-post/wma-declaration-of-helsinki/

[163] United Nations Educational, Scientific and Cultural Organization. (2005, October 19). Article 6. *Universal Declaration on Bioethics and Human Rights*. UNESCO. Retrieved from https://unesdoc.unesco.org/ark:/48223/pf0000142825

[164] Council of Europe. (1997, April 4). Chapter III. *Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine* (European Treaty Series No. 164). Council of Europe. Retrieved from https://rm.coe.int/168007cf98

[165] United Nations General Assembly. (1966, December 16). *International Covenant on Civil and Political Rights* (GA Res. 2200A (XXI), United Nations Treaty Series, vol. 999, p. 171). Entered into force March 23, 1976. United Nations. Retrieved from https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

[166] European Commission, Directorate-General for Research and Innovation. (2021, July 5). Page 7. *Identifying serious and complex ethics issues in EU-funded research (Guidelines on serious and complex cases)*. Prepared by the Research Ethics and Integrity Sector with ethics experts under the supervision of Albena Kuyumdzhieva and Ben Hayes. Retrieved from https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/guidelines-on-serious-and-complex-cases_he_en.pdf

[167] Ibid

[168] Ibid

[169] High-Level Expert Group on Artificial Intelligence. (2019, April 8). Page 2. *Ethics Guidelines for Trustworthy AI*. Publications Office of the European Union. Retrieved from https://ec.europa.eu/digital-strategy/en/library/ethics-guidelines-trustworthy-ai

[170] Ibid, page 12

- Human agency and oversight: Protecting fundamental rights, supporting human decision-making, and ensuring human oversight.
- Technical robustness and safety: Guaranteeing security, resilience, fallback mechanisms, accuracy, and reliability.
- Privacy and data governance: Safeguarding privacy, maintaining data quality and integrity, and controlling data access.
- Transparency: Ensuring traceability, explainability, and clear communication about AI processes.
- Diversity, non-discrimination, and fairness: Avoiding bias, ensuring accessibility, and promoting stakeholder inclusion.
- Societal and environmental well-being: Minimising negative social impact, supporting democracy, and fostering sustainability.
- Accountability: Providing mechanisms for auditing, minimising harm, addressing trade-offs, and enabling redress.[171]

5.3 Relevant International Law and Soft Law Encompassing Ethical Principles

Table 3. Overview of the Applicable Laws and Soft Laws Encompassing Ethical Principles

Primary focus	Name of the Obligations	EU/ International	Relevant Principles
General	Universal Declaration of human Rights[172]	International	○ Dignity, ○ Equality, ○ Non-discrimination, ○ Right to privacy
	European Convention on Human Rights[173]	International (Council of Europe)	○ Right to private life
	Charter of Fundamental Rights of the EU[174]	EU	○ Right to dignity, ○ Privacy, data protection, ○ Children's rights,

[171] Ibid, page 35

[172] United Nations General Assembly. (1948, December 10). *Universal Declaration of Human Rights* (GA Res. 217A (III)). Adopted by the General Assembly on 10 December 1948. United Nations. Retrieved from https://www.un.org/en/about-us/universal-declaration-of-human-rights

[173] Council of Europe. (1950, November 4). *European Convention on Human Rights, as amended by Protocols Nos. 3, 5, 8, 11, 14, and 15* (ETS No. 5). Entered into force September 3, 1953. Council of Europe. Retrieved from https://www.echr.coe.int/documents/d/echr/convention_ENG

[174] European Union. (2000, December 18). *Charter of Fundamental Rights of the European Union* (2000/C 364/01). Official Journal of the European Communities. Retrieved from https://www.europarl.europa.eu/charter/pdf/text_en.pdf

Primary focus	Name of the Obligations	EU/ International	Relevant Principles
			○ Health care
	International Covenant on Civil and Political Rights Ethical Principles[175]	International	○ Right to privacy - protection from arbitrary interference with one's privacy
	International Covenant on Economic, Social and Cultural Rights Ethical Principles[176]	International	○ Right to highest attainable standard of health, ○ Protection of the Family, Mothers, Children, and Young Persons
Medical	WMA Declaration of Taipei on Ethical Considerations regarding Health Databases and Biobanks Ethical Principles[177]	International	○ Respect for persons, ○ Informed Consent, ○ Transparency and accountability, ○ Data protection, ○ Ethical review, ○ Benefit to the society, ○ Participants and inclusion, ○ Governance arrangements ○ International cooperation
	Declaration of Helsinki[178]	International	○ Prioritising participant protection and respect ○ Safeguarding life, dignity, autonomy, and privacy ○ Following ethical, legal, and regulatory standards ○ Minimising environmental harm

[175] United Nations General Assembly. (1966, December 16). *International Covenant on Civil and Political Rights* (GA Res. 2200A (XXI), UNTS Vol. 999, p. 171). Entered into force March 23, 1976. United Nations. Retrieved from https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

[176] United Nations General Assembly. (1966, December 16). *International Covenant on Economic, Social and Cultural Rights* (GA Res. 2200A (XXI), UNTS No. 993, p. 3). Entered into force January 3, 1976. United Nations. Retrieved from https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-economic-social-and-cultural-rights

[177] World Medical Association. (2016, October). *Declaration of Taipei on Ethical Considerations regarding Health Databases and Biobanks* (Revised version). Adopted by the 67th WMA General Assembly. Retrieved from https://www.wma.net/policies-post/wma-declaration-of-taipei-on-ethical-considerations-regarding-health-databases-and-biobanks/

[178] World Medical Association. (2024, October). *Declaration of Helsinki: Ethical principles for medical research involving human subjects*. Adopted by the 75th World Medical Association General Assembly. Retrieved from https://www.wma.net/policies-post/wma-declaration-of-helsinki/ en.wikipedia.org+15

Primary focus	Name of the Obligations	EU/ International	Relevant Principles
			○ Balancing benefits and risks through risk assessment ○ Adhering to scientific principles ○ Justifying research ethically and legally ○ Ensuring informed and voluntary consent ○ Publishing complete and accurate results ○ Ensuring transparency ○ Providing appropriate medical care ○ Maintaining accountability ○ Ensuring participant safety ○ Fair participant inclusion ○ Fulfilling monitoring duties ○ Promoting economic sustainability ○ Protecting intellectual property ○ Upholding diversity
	International Ethical Guidelines for Health-related Research Involving Humans[179]	International	○ Respect for persons ○ Community engagement ○ Informed consent ○ Privacy and confidentiality ○ Risk-benefit assessment ○ Fair participant selection ○ Vulnerability and protection ○ Independent ethics review ○ Transparency and accountability ○ Research involving children and adolescents
	Universal Declaration on Bioethics on Human Rights Ethical Principles[180]	International	○ Respect for human dignity, human rights, and fundamental freedoms ○ Prioritisation of the interests and welfare of the individual ○ Maximising benefits and minimising harm ○ Respect for autonomy and individual responsibility

[179] Council for International Organizations of Medical Sciences. (2016). *International Ethical Guidelines for Health-Related Research Involving Humans* (4th ed.) [Prepared in collaboration with the World Health Organization]. Geneva: CIOMS. Retrieved from https://cioms.ch/wp-content/uploads/2017/01/WEB-CIOMS-EthicalGuidelines.pdf

[180] United Nations Educational, Scientific and Cultural Organization. (2005, October 19). *Universal Declaration on Bioethics and Human Rights*. Adopted by the UNESCO General Conference. Retrieved from https://www.unesco.org/en/legal-affairs/universal-declaration-bioethics-and-human-rights

Primary focus	Name of the Obligations	EU/ International	Relevant Principles
			○ Free, informed, and voluntary consent (with special provisions for children) ○ Protection of persons lacking capacity to consent ○ Protection of human vulnerability and personal integrity ○ Respect for privacy and confidentiality ○ Equality, justice, and equity ○ Solidarity and international cooperation ○ Promotion of health and social responsibility ○ Equitable sharing of benefits from scientific progress ○ Protection of future generations ○ Ethical decision-making, professionalism, and transparency ○ Independent ethics review ○ Risk assessment and management ○ Oversight of transnational practices (especially in data and AI deployment)
	Oviedo Convention[181]	International (Council of Europe)	○ Consent ○ Protection of persons not able to consent ○ Protection of persons who have a mental disorder ○ Private life and right to information ○ Human Genome: Non-discrimination ○ Human Genome: Predictive genetic tests ○ Human Genome: Interventions on the human genome

[181] Council of Europe. (1997, April 4). *Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine* (European Treaty Series No. 164). Council of Europe. Retrieved from Council of Europe Treaty Collection https://rm.coe.int/168007cf98

Primary focus	Name of the Obligations	EU/ International	Relevant Principles
			○ Human Genome: Non-selection of sex ○ General Rule for scientific research ○ Protection of persons undergoing research ○ Protection of persons not able to consent to research ○ Prohibition of financial gain and disposal of a part of the human body
Protection of Children	UN Convention on the Rights of the Child[182]	International	○ Definition of child ○ Best interest of the child ○ Right to health and health services
Data Protection and Governance	UN Personal Data Protection and Privacy Principles[183]	International	○ Fairness and legitimate processing ○ Purpose specification ○ Proportionality and necessity ○ Retention ○ Accuracy ○ Confidentiality ○ Security ○ Transparency ○ Transfers ○ Accountability
	OECD Good Practice Principles for Data Ethics in the Public Sector[184]	International	○ Manage data with integrity ○ Be aware of and observe relevant government-wide arrangements for trustworthy data access, sharing and use ○ Incorporate data ethical considerations into governmental, organisational and public sector decision-making processes ○ Monitor and retain control over data inputs, in particular those used to inform the

[182] United Nations General Assembly. (1989, November 20). *Convention on the Rights of the Child* (General Assembly Resolution 44/25). United Nations. Entry into force September 2, 1990. Retrieved from https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child ohchr.org

[183] United Nations High-Level Committee on Management. (2018, October 11). *Principles on Personal Data Protection and Privacy for the United Nations System Organizations*. Adopted by the High-Level Committee on Management. United Nations. Retrieved from https://www.unsystem.org/privacy-principles

[184] OECD. (2021, March 15). *Good Practice Principles for Data Ethics in the Public Sector* (OECD Public Governance Policy Papers, No. 57). OECD Publishing. Retrieved from https://doi.org/10.1787/caa35b76-en

Primary focus	Name of the Obligations	EU/ International	Relevant Principles
			development and training of AI systems, and adopt a risk-based approach to the automation of decisions ○ Be specific about the purpose of data use, especially in the case of personal data ○ Define boundaries for data access, sharing and use ○ Be clear, inclusive and open ○ Publish open data and source code ○ Broaden individuals' and collectives' control over their data ○ Be accountable and proactive in managing risks
	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Ethical Principles[185]	International (Council of Europe)	○ Quality of data ○ Special categories of data ○ Data security ○ Additional safeguards for the data subject ○ Transborder flows of personal data and domestic law ○ Co-operation between Parties ○ Assistance to data subjects resident abroad

[185] Council of Europe. (1981). *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (ETS No. 108).

6 Contractual Framework Overview

The contractual framework in the protect child project has been defined through a multi-layered approach, which combines obligations arising from the Grant Agreement signed with the European health and Digital Executive Agency (HADEA), the draft Consortium Agreement (currently being finalized amongst the beneficiaries), and a dedicated set of additional contractual instruments that are being prepared to ensure the ethical and legal compliance of data sharing, governance and exploitation beyond the project life-cycle.

6.1 Restatement of Grant Agreement provisions:

The GA establishes the binding obligations of all beneficiaries in relation to the implementation of the project (Project 101137423 — PROTECT-CHILD). The following Articles are particularly relevant to the activities addressed in this deliverable:

- Article 11 – Proper Implementation of the Action: Beneficiaries must implement the action in accordance with Annex 1 and ensure compliance with applicable EU, national, and international law.
- Article 12 – Conflict of Interests: Parties must avoid situations that could compromise the project's objectives or compliance.
- Article 13 – Confidentiality and Security: Sets out obligations for handling sensitive information, including protection of classified and non-classified sensitive data.
- Article 14 – Ethics and Values: Requires compliance with ethical standards and values, aligned with EU principles.
- Article 15 – Data Protection: Establishes obligations under EU data protection legislation, notably GDPR, for all data processing activities.
- Article 16 – Intellectual Property Rights (IPR), Background and Results: Regulates ownership of results, access rights, and use of background information.
- Article 17 – Communication, Dissemination, and Visibility: Requires beneficiaries to promote the action and disseminate results, while ensuring visibility of EU funding.
- Article 25 – Checks, Reviews, Audits and Investigations: Provides for audits and investigations by the granting authority, the Commission, OLAF, EPPO, and ECA.
- Article 43 – Applicable Law and Settlement of Disputes: Establishes EU law and Belgian law as governing law, with disputes to be settled before EU courts (for EU beneficiaries) or Brussels courts (for non-EU beneficiaries).

6.2 Relevant Provisions of the Draft Consortium Agreement

The draft CA (v.4.0, July 2024) supplements the GA by regulating internal relationships among beneficiaries. While subject to final approval, the following draft articles are of direct relevance:

- Section 4 – Responsibilities of Parties: Each party must implement the project diligently, cooperate with others, and comply with both GA and CA provisions.
- Section 5 – Liability towards each other: Clarifies liability for breaches and establishes procedures for handling defaulting parties.

- Section 6 – Governance Structure: Defines the Steering Board and other bodies responsible for decision-making, including ethical oversight mechanisms.
- Section 8 – Results: Sets rules for ownership of results generated under the project.
- Section 9 – Access Rights: Establishes principles for granting access to background and results, based on the "Needed" standard (for implementation and exploitation).
- Section 10 – Non-Disclosure of Information: Regulates confidentiality obligations among parties.

Notably, the draft CA also foresees that specific data processing and/or data sharing agreements may need to be concluded among parties to comply with GDPR and national laws

6.3 Additional Contractual Framework for Implementation

In addition to the GA and CA, further contractual instruments are being developed to ensure effective, timely, and compliant implementation of project activities. A **three-stage approach** is foreseen:

- Material and Data Sharing Agreement (Short-Term, Urgent Needs)
  - Being drafted by the pilot sponsor (Hospital Universitario La Paz).
  - Ensures the rapid execution of urgent project activities in line with institutional practices.
  - Provides a practical framework for initial data and material exchanges among relevant partners.
- Umbrella Agreement on Data for the Federated Platform (Medium-Term, Core Operations)
  - Will regulate all data-related aspects linked to the PROTECT-CHILD federated platform.
  - Currently in development: a questionnaire has been circulated to technical partners; first draft expected by October; thereafter, review by legal departments with two rounds of clarifications before signature.
  - The umbrella agreement will be deeply aligned with the technical architecture and deployment details of the platform to ensure feasibility and compliance.
- Exploitation-Oriented Agreement (Long-Term, Post-Project Sustainability)
  - A modified version of the umbrella agreement, tailored for the exploitation of project results beyond the funded period.
  - Will include governance and contractual provisions for sustained use and further development of the PROTECT-CHILD technologies.
  - Designed to be expansible, allowing new organizations outside the original consortium to adopt or test the platform and associated tools.

6.4 Compliance with Legal and Ethical Framework

All contractual instruments are to be interpreted and applied consistently with the regulatory and ethical framework detailed in this deliverable (Section 4 and Section 5).

In particular, they must ensure compliance with:

- The General Data Protection Regulation (GDPR) and national implementations.
- The European Health Data Space (EHDS) Regulation, the Data Governance Act, the Data Act, and relevant cybersecurity legislation (e.g. CRA, NIS2).
- Ethical requirements derived from the Declaration of Helsinki, Oviedo Convention, and UNCRC.

7 Stakeholder Requirements

The requirements detailed in the following table were synthesized through a multi-stage process. First, core obligations were extracted directly from the primary legal texts (e.g., GDPR, EHDS Regulation) and foundational ethical guidelines. Second, these abstract obligations were mapped onto the specific activities, work packages, and deliverables defined in the PROTECT-CHILD Description of Action. Finally, these legal and project-based requirements were integrated with the stakeholder-defined functional and non-functional needs identified through the co-design process (T2.1), particularly the user stories related to governance, security, and access control. The result is a set of requirements that are legally grounded, project-relevant, and stakeholder-validated.

Table 4. Overview of Stakeholder Requirements

Req. ID	Requirement Description	Primary Legal/Ethical Source	Affected WPs	Primary Responsible Stakeholder(s)	Key Implementation Measures & Verification Evidence
A. Data Protection & Privacy					
A.1	Ensure a valid legal basis is established and documented for all processing of personal health and genomic data for research purposes.	GDPR Art. 6, Art. 9(2)(j)	WP2, WP8, WP11	Clinical Partners, UGR, UDGA	D2.2 Stakeholder Requirement and Legal Framework; D8.4 Study Protocol; Documented legal basis in Data Management Plan (D1.2).
A.2	Adhere strictly to the principles of data minimization and purpose limitation in all data processing activities.	GDPR Art. 5(1)(b,c)	All WPs	All Partners	D2.3 Platform Architecture demonstrating federated design; Data Permit system (D6.4) enforcing purpose-specific access; Audit logs.
A.3	Conduct and document a Data Protection Impact Assessment (DPIA) prior to processing high-risk data.	GDPR Art. 35	WP2, WP6, WP11	UPM (Coordinator), UDGA, DPOs	Completed DPIA report signed off by relevant Data Protection Officers and submitted as part

					of project documentation.
A.4	Ensure all transfers of personal data to non-EU partners (e.g., GTRC in the US) are covered by an appropriate legal transfer mechanism.	GDPR Chapter V	WP1, WP2, WP6	UPM (Coordinator), UDGA	Executed Standard Contractual Clauses (SCCs) or other valid transfer mechanism documented and on file.
A.5	Implement a clear and accessible mechanism for data subjects to exercise their right to opt-out of secondary data use.	EHDS Regulation Art. 71	WP6, WP7	Clinical Partners, BELIT, CERTH	Functionality within the Consent Management system (D6.3) and a public-facing information page on the project website (D10.10).
B. Ethical Conduct & Participant Rights					
B.1	Implement a dynamic, documented process for obtaining parental permission and child assent, respecting the evolving capacity of the minor.	UNCRC Art. 12; 45 CFR 46 Subpart D	WP6, WP8, WP11	Clinical Partners, BELIT, UGR	D6.3 Consent Management System; Approved, age-appropriate assent form templates; Documented procedures in D8.4 Study Protocol.
B.2	Establish and implement a clear policy for managing and communicating incidental findings to participants/and relevant authorities.	WMA Declaration of Taipei; D12.2	WP9, WP11	SERMAS (as study lead), IEAB, UGR	D11.3/D11.4 ELSI Recommendations; A documented policy approved by the IEAB; A formal record of any incidental findings.
B.3	Develop and implement a procedure for re-consenting	D12.2 Ethics Req.	WP6, WP8, WP11	Clinical Partners, UGR, IEAB	A documented re-consent protocol within the ELSI

	participants who reach the age of legal majority during the project's lifecycle.				Framework (D11.2); Records of re-consent attempts and outcomes.
B.4	Ensure all research activities involving human participants have received prior approval from all relevant institutional and national ethics committees.	Declaration of Helsinki	WP8, WP11, WP12	Clinical Partners, SERMAS	D8.5 Report on pilot study approval, containing copies of all relevant ethics approval letters for each participating site.
C. Data & System Security					
C.1	Implement and enforce strong, role-based access control (RBAC) and multi-factor authentication (MFA) for all access to the PROTECT-CHILD platform and data.	GDPR Art. 32; NIS2 Art. 21	WP3, WP4, WP6	Technical Partners (UPM, INTM)	D6.1 AAA Services; System architecture documents (D2.3); Records of access control policies; Penetration test results.
C.2	Ensure all personal data are encrypted both in transit and at rest using state-of-the-art cryptographic standards.	GDPR Art. 32	WP3, WP4, WP5	Technical Partners (INTM, CERTH)	D5.2 SMPC services
C.3	Establish and maintain a formal incident response plan and report any significant security incidents to the relevant authorities and data subjects as required by law.	GDPR Art. 33-34; NIS2 Art. 23	WP1, WP3, WP6	UPM (Coordinator), Technical Partners	A documented Incident Response Plan; Records of any incident reports made to supervisory authorities.
C.4	Ensure the platform architecture	EHDS Regulation Art. 73	WP3, WP4	Technical Partners	D4.1 Core capsule and orchestration

	constitutes a Secure Processing Environment (SPE) that prevents the unauthorized extraction of data.			(BIOMERIS, INTM)	services documentation; Technical validation report confirming data cannot be downloaded from the SPE.
D. Governance & Accountability					
D.1	All data access for secondary use must be preceded by a formal Data Permit application and granted via the established governance process.	EHDS Regulation Art. 45-46	WP6, WP7	Data Holders (Clinical Partners), CERTH	D6.4 Data Permit Management System; D7.2 Data Permit Dashboard; A complete audit trail of all permit applications and decisions.
D.2	Maintain comprehensive and up-to-date records of all data processing activities as required by GDPR Article 30.	GDPR Art. 30	All WPs	All Partners, coordinated by UPM & UGR	A central, accessible Register of Processing Activities; Regular updates to the Data Management Plan (D1.3).
D.3	Ensure all data and research outputs are managed in accordance with FAIR principles (Findable, Accessible, Interoperable, Reusable).	Grant Agreement Annex 5	WP1, WP2, WP5	All Partners	D1.2 Data Management Plan detailing FAIR implementation; D2.3 Data and metadata models; D5.1 Data discovery services.
D.4	Appoint an independent, external Ethics Board (IEAB) with the required expertise to provide ongoing oversight of the project.	D12.2 Ethics Req.	WP11, WP12	UPM, UGR	D11.1 Report on the inaugural meeting of the IEAB; IEAB membership list and terms of reference; Regular reports from the IEAB

8 Conclusions

Deliverable 2.2 fulfils the objectives of Protect Child WP 2 by providing a comprehensive analysis of the legal, ethical and contractual requirements of relevance to the project. Following an identification of the relevant national and European regulatory instruments, it clarifies the obligations arising from the grant agreement and the draft consortium agreement and addresses the specific stakeholder requirements to be considered by the project's upcoming activities whilst also defining the future contractual framework required for securing lawfully and ethically compliant management of sensitive paediatric health and genomic data.

This deliverable and its annexes serve as a baseline for the upcoming and ongoing compliance activities envisaged by WP11, and clarifies how the project's obligations are being met while ensuring all consortium partners are aware of viable pathways for compliance demonstration (e.g. certification). The work expected from WP11 towards the operationalization of the contractual instruments and the alignment and integration of their dispositions with the project's solutions is of the highest importance to the project's activities, and should be closely followed by all consortium partners (and particularly by technical partners) to ensure the successful completion of the project and maintain data subject trust in its enablers.

REFERENCES

- *Advies nr. 1–2005*. (2005). Gegevensbeschermingsautoriteit. Retrieved from https://www.gegevensbeschermingsautoriteit.be/publications/advies-nr.-1-2005.pdf
- *Advies nr. 110–2018*. (2018). Gegevensbeschermingsautoriteit. Retrieved from https://www.gegevensbeschermingsautoriteit.be/publications/advies-nr.-110-2018.pdf
- *Advies nr. 117–2018*. (2018). Gegevensbeschermingsautoriteit. Retrieved from https://www.gegevensbeschermingsautoriteit.be/publications/advies-nr.-117-
- *Advies nr. 36–2020*. (2020). Gegevensbeschermingsautoriteit. Retrieved from https://www.gegevensbeschermingsautoriteit.be/publications/advies-nr.-36-2020.pdf
- Agencia Española de Protección de Datos & European Union Agency for Cybersecurity. (2024). *Técnicas de seudonimización en el sector sanitario*. Retrieved from https://www.aepd.es/documento/tecnicas-seudonimizacion-sector-sanitario-enisa.pdf
- Agencia Española de Protección de Datos. (2024). *Adecuación del RGPD a la inteligencia artificial*. Retrieved from https://www.aepd.es/guias/adecuacion-rgpd-ia.pdf
- Agencia Española de Protección de Datos. (2024). *Aproximación a los espacios de datos y el RGPD*. Retrieved from https://www.aepd.es/guias/aproximacion-espacios-datos-rgpd.pdf
- Agencia Española de Protección de Datos. (2024). *Guía sobre generación de datos sintéticos*. Retrieved from https://www.aepd.es/guias/guia-sobre-generacion-datos-sinteticos.pdf
- Agencia Española de Protección de Datos. *Infografía: Consentimiento de menores*. Retrieved from https://www.aepd.es/infografias/infografia-consentimiento-menores.pdf
- Agencia Española de Protección de Datos. *Informes y resoluciones: Informes jurídicos*. Retrieved from https://www.aepd.es/informes-y-resoluciones/informes-juridicos?f%5B0%5D=conceptos%3A1418
- Agencia Española de Protección de Datos. *Novedades LOPD sector privado*. Retrieved from https://www.aepd.es/guias/novedades-lopd-sector-privado.pdf
- Agencia Española de Protección de Datos. *Novedades LOPD sector público*. Retrieved from https://www.aepd.es/guias/novedades-lopd-sector-publico.pdf
- Autoriteit Persoonsgegevens – Archief. *Archive overview*. Retrieved from https://autoriteitpersoonsgegevens.archiefweb.eu/#archive
- Autoriteit Persoonsgegevens. (2025, March 19). *Toets Wet versterking rechtsbescherming in de jeugdbescherming*. Retrieved from https://www.autoriteitpersoonsgegevens.nl/documenten/toets-wet-versterking-rechtsbescherming-in-de-jeugdbescherming
- Autoriteit Persoonsgegevens. (2025, March 27). *Investigation into handling data breaches in youth care*. Dutch Data Protection Authority. Retrieved from https://www.autoriteitpersoonsgegevens.nl/en/documents/investigation-into-handling-data-breaches-in-youth-care

- Baker McKenzie Resource Hub. *Key Data & Cybersecurity Laws—Greece*. Retrieved from https://resourcehub.bakermckenzie.com/en/resources/global-data-and-cyber-handbook/emea/greece/topics/key-data-and-cybersecurity-laws
- Brussels-Capital Region. (2023, October 31). *The challenges of the Data Governance Act*. Retrieved from https://be.brussels/en/about-region/challenges-data-governance-act
- CMS. (2025, April 28). *Capgemini and CMS: German Data Act Implementation Act – German Federal Network Agency to become enforcement authority*. Retrieved from https://cms-lawnow.com/en/ealerts/2025/04/capgemini-and-cms-german-data-act-implementation-act-german-federal-network-agency-to-become-enforcement-authority
- Council for International Organizations of Medical Sciences. (2016). *International Ethical Guidelines for Health-Related Research Involving Humans* (4th ed.) [Prepared in collaboration with the World Health Organization]. Geneva: CIOMS. Retrieved from https://cioms.ch/wp-content/uploads/2017/01/WEB-CIOMS-EthicalGuidelines.pdf
- Council of Europe. (1950, November 4). *European Convention on Human Rights, as amended by Protocols Nos. 3, 5, 8, 11, 14, and 15* (ETS No. 5). Entered into force September 3, 1953. Council of Europe. Retrieved from https://www.echr.coe.int/documents/d/echr/convention_ENG
- Council of Europe. (1981). *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (ETS No. 108).
- Council of Europe. (1997, April 4). *Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine* (European Treaty Series No. 164). Council of Europe. Retrieved from Council of Europe Treaty Collection https://rm.coe.int/168007cf98
- Council of Europe. (1997, April 4). *Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine* (European Treaty Series No. 164). Council of Europe. Retrieved from https://rm.coe.int/168007cf98
- Dal Molin, L., Bühler, G., Wesiak-Schmidt, K., & Al Abiad, T. (2025, February 13). *Swiss AI regulation: Tailored rules instead of a Swiss AI Act*. Homburger AG. Retrieved from https://www.homburger.ch/en/insights/swiss-ai-regulation-tailored-rules-instead-of-a-swiss-ai-act
- DLA Piper. (2025, February 28). *Spanish government approves draft law for ethical, inclusive and beneficial use of artificial intelligence*. Retrieved from https://knowledge.dlapiper.com/dlapiperknowledge/globalemploymentlatestdevelopments/2025/spanish-government-approved-draft-law-for-ethical-inclusive-and-beneficial-use-of-artificial-intelligence
- Đukanović, J., & Spasojević, D. (2025, February 20). *If you are doing clinical research in Serbia, you must appoint a Data Representative and/or a DPO*. Zunic Law. Retrieved from https://zuniclaw.com/en/clinical-research-in-serbia-data-representative-dpo/
- European Commission, Directorate-General for Research and Innovation. (2021, July 5). *Identifying serious and complex ethics issues in EU-funded research (Guidelines on serious and complex cases)*. Prepared by the Research Ethics and Integrity Sector with

ethics experts under the supervision of Albena Kuyumdzhieva and Ben Hayes. Retrieved from https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/guidelines-on-serious-and-complex-cases_he_en.pdf

- European Commission, Research Executive Agency. *Open science*. Retrieved from https://rea.ec.europa.eu/open-science_en
- European Commission. (2017, October 13). *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (wp248rev.01). Retrieved from https://ec.europa.eu/newsroom/article29/items/611236
- European Data Protection Board. (2020, January 8). *Reply to the European Commission questionnaire on processing of personal data for scientific research***.** Retrieved from https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_replyec_questionnaireresearch_final.pdf
- European Data Protection Board. (2020, January 8). *Reply to the European Commission questionnaire on processing of personal data for scientific research***.** Retrieved from https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_replyec_questionnaireresearch_final.pdf
- European Data Protection Board. (2020, October 20). *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, version 2.0***.** Retrieved from https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf
- European Data Protection Board. (2021, March 2). *Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak*. Retrieved from https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032020-processing-data-concerning-health-purpose_en
- European Data Protection Board. (2022, February 4). *Legal study on appropriate safeguards under Article 89(1) GDPR for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes*. Retrieved from https://www.edpb.europa.eu/our-work-tools/our-documents/legal-study-appropriate-safeguards-under-article-891-gdpr-processing_en
- European Health and Digital Executive Agency. (2024). *Grant Agreement: PROTECT-CHILD* (Grant Agreement No. 101137423). Brussels, Belgium
- European Parliament & Council of the European Union. (2016, April 27). *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)***.** *Official Journal of the European Union*, L 119, 1–88.
- European Parliament & Council of the European Union. (2016, April 27). *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)*. *Official Journal of the European Union*, L 119, 1–88.
- European Parliament & Council of the European Union. (2022, December 14). *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). *Official Journal of the European Union*, L 333, 80–152. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555

- European Parliament & Council of the European Union. (2022, May 30). *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)*. *Official Journal of the European Union*, L 152, 1-44
- European Parliament & Council of the European Union. (2023, December 13). *Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act)*. *Official Journal of the European Union*, L 2023, 1–64.
- European Parliament & Council of the European Union. (2024, October 23). *Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)*. *Official Journal of the European Union*, L 2847, 1–52
- European Parliament & Council of the European Union. (2025, February 11). *Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847*. *Official Journal of the European Union*, L 2025/327, 1–120
- European Parliament and of the Council. (2024, June 13) *Regulation (EU) 2024/1684 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence 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)*, OJ L 22024/1689, 12.7.2024.
- European Union Agency for Cybersecurity. (2023). *NIS 2 technical implementation guidance*. Retrieved from https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance
- European Union. (2000, December 18). *Charter of Fundamental Rights of the European Union* (2000/C 364/01). Official Journal of the European Communities. Retrieved from https://www.europarl.europa.eu/charter/pdf/text_en.pdf
- European Union. (2024, November 20). *Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Regulation)* (OJ L 2847, 20.11.2024, pp. 1–81). Retrieved from https://www.boe.es/buscar/doc.php?id=DOUE-L-2024-81720
- Federal Ministry for Economic Affairs and Climate Action. (n.d.). *Guidelines on the protection of health data*. Retrieved from https://www.bundeswirtschaftsministerium.de/Redaktion/EN/Dossier/guidelines-on-the-protection-of-health-data.html

- Garante per la protezione dei dati personali. (2009, November 19). *Linee guida in tema di referti on-line* (Doc. web n. 1683328). Retrieved from https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1683328
- Garante per la protezione dei dati personali. (2021, July 10**).** *Linee guida in materia di cookie e altri strumenti di tracciamento* (Doc. web n. 9677876). Retrieved from https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9677876
- Garante per la protezione dei dati personali. *Main decisions*. Retrieved from https://www.garanteprivacy.it/web/garante-privacy-en/main-decisions
- Garante per la protezione dei dati personali. *Oblio oncologico (Oncology "Right to Be Forgotten")*. Retrieved from https://www.garanteprivacy.it/temi/sanita-e-ricerca-scientifica/oblio-oncologico
- Gegevensbeschermingsautoriteit. (2023, April 27). *Advies nr. 83/2023 van 27 april 2023: Voorontwerp van ordonnantie betreffende het elektronisch uitwisselingsplatform voor gezondheidsgegevens* (Advies nr. 83/2023). Retrieved from https://www.gegevensbeschermingsautoriteit.be/publications/advies-nr.-83-2023.pdf
- Gegevensbeschermingsautoriteit. (2024, May 17). *Advies nr. 52/2024 van 17 mei 2024: Voorontwerp van koninklijk besluit over de toegang tot gezondheidsgegevens* (Advies nr. 52/2024). Retrieved from https://www.gegevensbeschermingsautoriteit.be/publications/advies-nr.-52-2024.pdf
- Gesetze-im-Internet. *Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG***)**. Retrieved from https://www.gesetze-im-internet.de/ttdsg/
- GO FAIR. *FAIR Principles***.**
- Government of Serbia. (2024, December 27). *Belgrade Ministerial Declaration on Artificial Intelligence adopted***.** Retrieved from https://www.ai.gov.rs/vest/en/1419/belgrade-ministerial-declaration-on-artificial-intelligence-adopted.php
- Government of the Netherlands**.** *Regeling WGK014627*. Retrieved from https://wetgevingskalender.overheid.nl/Regeling/WGK014627
- High-Level Expert Group on Artificial Intelligence. (2019, April 8). *Ethics Guidelines for Trustworthy AI*. Publications Office of the European Union. Retrieved from https://ec.europa.eu/digital-strategy/en/library/ethics-guidelines-trustworthy-ai
- *Law No. 5188: Measures for the implementation of Regulation (EU) 2022/868 (Data Governance Act) – Designation of competent authority for Regulation* (EU) 2024/903 (Interoperable Europe Regulation). Retrieved from https://search.et.gr/el/fek/?fekId=779379
- Linklaters. (2024, March). *Data Protected – Belgium*. Retrieved from https://www.linklaters.com/en/insights/data-protected/data-protected---belgium
- Linklaters. *Data Protected – Germany*. Retrieved from https://www.linklaters.com/insights/data-protected/data-protected---germany#:~:text=Are%20there%20any%20special%20rules,the%20field%20of%20employment%20law
- Ministero dell'Economia e delle Finanze. (2025, February 27). *Decreto 27 febbraio 2025: Riapertura delle operazioni di sottoscrizione dei certificati di credito del Tesoro indicizzati*

al tasso Euribor a sei mesi ("CCTeu"), godimento 15 ottobre 2024, scadenza 15 aprile 2033, quinta e sesta tranche (Gazzetta Ufficiale, Serie Generale, No. 53 del 05-03-2025). Retrieved from https://www.senato.it/leggi-e-documenti/disegni-di-legge/scheda-ddl?tab=datiGenerali&did=59313

- Ministero della Salute. (2024, December 31). *Decreto 31 dicembre 2024: Istituzione dell'Ecosistema dati sanitari* (GU Serie Generale n. 53, 05-03-2025). Retrieved from https://www.gazzettaufficiale.it/eli/gu/2025/03/05/53/sg/pdf
- Netherlands Enterprise Agency. *Mandatory registration of data intermediation service (DGA)*. Retrieved from https://business.gov.nl/regulation/mandatory-registration-data-intermediation-service-dga
- OECD AI Policy Observatory. (2025, Month Day). *Law 4961/2022: Emerging information and communication technologies and societies—enhancing digital governance and other provisions*. Retrieved from https://oecd.ai/en/dashboards/policy-initiatives/law-n-49612022-emerging-information-and-communication-technologies-and-societies-enhancing-digital-governance-and-other-provisions-3368
- OECD. (2021, March 15). *Good Practice Principles for Data Ethics in the Public Sector* (OECD Public Governance Policy Papers, No. 57). OECD Publishing. Retrieved from https://doi.org/10.1787/caa35b76-en
- Parliament of the Netherlands. (2024). *Kamerstuk KST-36531-5*. Retrieved from https://zoek.officielebekendmakingen.nl/kst-36531-5.html
- Presidenza del Consiglio dei Ministri – Dipartimento della Protezione Civile. (2024, February 26). *Decreto 26 febbraio 2024: Approvazione del Piano straordinario di analisi della vulnerabilità delle zone …* (GU Serie Generale n. 90, 17-04-2024). Retrieved from https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9677876
- Repubblica Italiana. (2024, March 25). *Decreto Legislativo 25 marzo 2024, n. 50: Disposizioni integrative e correttive …* (GU Serie Generale n. 90, 17-04-2024). Retrieved from https://www.gazzettaufficiale.it/eli/gu/2024/04/17/90/sg/pdf
- Repubblica Italiana. (2024, October 1). *Decreto-Legge 1 ottobre 2024, n. 137: Misure urgenti per contrastare i fenomeni di violenza nei confronti dei professionisti sanitari…* (Gazzetta Ufficiale, Serie Generale, n. 230). Retrieved from https://www.gazzettaufficiale.it/eli/gu/2024/10/01/230/sg/pdf
- Repubblica Italiana. (2024, October 7). *Decreto Legislativo 7 ottobre 2024, n. 144: Norme di adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2022/868 (Data Governance Act)* (Gazzetta Ufficiale, Serie Generale, n. 238). Retrieved from https://www.gazzettaufficiale.it/eli/id/2024/10/10/24G00167/SG
- Reuters. (2024, September 5). *US, Britain, EU to sign first international AI treaty* [News article]. Retrieved from https://www.coe.int/en/web/artificial-intelligence/-/switzerland-signs-the-council-of-europe-s-global-treaty-on-ai
- Ruzicic, I. (2024, July 5). *Data Protection Laws and Regulations in Serbia*. CEE Legal Matters. Retrieved from https://ceelegalmatters.com/data-protection-2024/serbia-data-protection-2024
- Service public fédéral Chancellerie du Premier Ministre. (2024, April 26). *Loi établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt*

général pour la sécurité publique (Moniteur belge, Numac 2024202344). Belgique: Auteur. Retrieved from https://www.ejustice.just.fgov.be/cgi/article.pl?language=fr&sum_date=2024-05-17&lg_txt=f&caller=sum&s_editie=1&2024202344=4&numac_search=2024202344&view_numac=2024202344f

- Shah, P., Thornton, I., Kopitnik, N. L., & Hipskind, J. E. (2025, January). *Informed Consent*. In StatPearls. StatPearls Publishing. Retrieved from https://www.ncbi.nlm.nih.gov/books/NBK430827/
- Spain. (2002, November 14). *Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica*. (BOE No. 274, 15.11.2002). Retrieved from https://www.boe.es/buscar/act.php?id=BOE-A-2002-22188
- Spain. (2007, November 16). *Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público*. (BOE No. 276, 17.11.2007). Retrieved from https://boe.es/buscar/act.php?id=BOE-A-2007-19814
- Spain. (2011, October 24). *Real Decreto 1495/2011, de 24 de octubre, por el que se desarrolla la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, para el ámbito del sector público estatal***.** (BOE No. 269, 08.11.2011). Retrieved from https://boe.es/buscar/act.php?id=BOE-A-2011-17560
- Spain. (2022, December 27) *Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2)*. Retrieved from https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81963
- Spain. (2025, February 20). *Reglamento (UE) 2025/327 del Parlamento Europeo y del Consejo, de 11 de febrero de 2025, relativo al Espacio Europeo de Datos de Salud, y por el que se modifican la Directiva 2011/24/UE y el Reglamento (UE) 2024/2847***.** Retrieved from https://www.boe.es/buscar/doc.php?id=DOUE-L-2025-80382
- Spain. (2025, March 5). *Reglamento de Ejecución (UE) 2024/2690 de la Comisión, de 17 de octubre de 2024, por el que se establecen las disposiciones de aplicación de la Directiva (UE) 2022/2555 en lo que respecta a los requisitos técnicos y metodológicos de las medidas para la gestión de riesgos de ciberseguridad y en el que se detallan los casos en que un incidente se considera significativo con respecto a los proveedores de servicios de DNS, los registros de nombres de dominio de primer nivel, los proveedores de servicios de computación en nube, los proveedores de servicios de centro de datos, los proveedores de redes de distribución de contenidos, los proveedores de servicios gestionados, los proveedores de servicios de seguridad gestionados, los proveedores de mercados en línea, motores de búsqueda en línea y plataformas de servicios de redes sociales, y los proveedores de servicios de confianza*. Retrieved from https://www.boe.es/buscar/doc.php?id=DOUE-L-2024-81540
- United Nations Educational, Scientific and Cultural Organization. (2005, October 19). *Universal Declaration on Bioethics and Human Rights*. UNESCO. Retrieved from https://unesdoc.unesco.org/ark:/48223/pf0000142825

- United Nations Educational, Scientific and Cultural Organization. (2005, October 19). *Universal Declaration on Bioethics and Human Rights*. Adopted by the UNESCO General Conference. Retrieved from https://www.unesco.org/en/legal-affairs/universal-declaration-bioethics-and-human-rights
- United Nations General Assembly. (1948, December 10). *Universal Declaration of Human Rights* (GA Res. 217A (III)). Adopted by the General Assembly on 10 December 1948. United Nations. Retrieved from https://www.un.org/en/about-us/universal-declaration-of-human-rights
- United Nations General Assembly. (1966, December 16). *International Covenant on Civil and Political Rights* (GA Res. 2200A (XXI), UNTS Vol. 999, p. 171). Entered into force March 23, 1976. United Nations. Retrieved from https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights
- United Nations General Assembly. (1966, December 16). *International Covenant on Economic, Social and Cultural Rights* (GA Res. 2200A (XXI), UNTS No. 993, p. 3). Entered into force January 3, 1976. United Nations. Retrieved from https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-economic-social-and-cultural-rights
- United Nations General Assembly. (1989, November 20). *Convention on the Rights of the Child* (General Assembly Resolution 44/25). United Nations. Entry into force September 2, 1990. Retrieved from https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child ohchr.org
- United Nations HighLevel Committee on Management. (2018, October 11). *Principles on Personal Data Protection and Privacy for the United Nations System Organizations*. Adopted by the HighLevel Committee on Management. United Nations. Retrieved from https://www.unsystem.org/privacy-principles
- Wet tot uitvoering van Verordening (EU) 2024/2847 van het Europees Parlement en de Raad van 23 oktober 2024 betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordeningen (EU) nr. 168/2013 en (EU) 2019/1020 en Richtlijn (EU) 2020/1828 (Uitvoeringswet verordening cyberweerbaarheid) VOORSTEL VAN WET). Retrieved from: https://www.rijksoverheid.nl/actueel/nieuws/2025/03/10/internetconsultatie-uitvoeringswet-verordening-cyberweerbaarheid-van-start
- World Medical Association. (2024, October)**.** *Declaration of Helsinki: Ethical principles for medical research involving human subjects*. Adopted by the 75th World Medical Association General Assembly. Retrieved from https://www.wma.net/policies-post/wma-declaration-of-helsinki/ en.wikipedia.org+15
- Zeya. (2025, May 12***).*** *Greece adopts national cybersecurity requirements framework***.** Retrieved from https://www.zeya.com/newsletters/greece-adopts-national-cybersecurity-requirements-framework
- Zhan, S., Huang, L., Luo, G., Zheng, S., Gao, Z., & Chao, H.-C. (2025). *A review on federated learning architectures for privacypreserving AI: Lightweight and secure cloud–edge–end collaboration*. *Electronics*, *14*(13), 2512. https://www.mdpi.com/2079-9292/14/13/2512

9 Annex 1

9.1 Annex 1.1 - High-level Self-Assessment Questionnaire

A. Legal Compliance						
No.	Requirement Area	Legal/Ethical Source	Self-Assessment Question	Yes	No	N/A
1	Legal Basis	GDPR Art. 6, Art. 9(2)(j)	Have you established and documented a valid legal basis for processing personal health and genomic data?	☐	☐	☐
2	Data Minimization & Purpose	GDPR Art. 5(1)(b,c)	Are data processing activities limited to the minimum necessary and specific research purposes?	☐	☐	☐
3	DPIA	GDPR Art. 35	Have you conducted and documented a Data Protection Impact Assessment for high-risk data?	☐	☐	☐
4	International Transfers	GDPR Chapter V	Are all transfers of personal data to non-EU partners covered by an appropriate legal mechanism?	☐	☐	☐
5	Data Subject Rights	EHDS Regulation Art. 71	Is there a clear and accessible mechanism for participants to opt-out of secondary data use?	☐	☐	☐
B. Ethical Conduct & Participant Rights						
No.	**Requirement Area**	**Legal/Ethical Source**	**Self-Assessment Question**	**Yes**	**No**	**N/A**
6	Consent & Assent	UNCRC Art. 12; 45 CFR 46 Subpart D	Is there a documented process for obtaining parental permission and child assent, respecting evolving capacity?	☐	☐	☐
7	Incidental Findings	WMA Declaration of Taipei; D12.2	Is there a clear policy for managing and communicating incidental findings?	☐	☐	☐
8	Re-Consent	D12.2 Ethics Req.	Is there a procedure for re-consenting participants who reach legal majority during the project?	☐	☐	☐
9	Ethics Approval	Declaration of Helsinki	Have all human-participant research activities received prior approval from relevant (institutional and/or national) ethics committees?	☐	☐	☐
C. Data & System Security						
No.	**Requirement Area**	**Legal/Ethical Source**	**Self-Assessment Question**	**Yes**	**No**	**N/A**
10	Access Control	GDPR Art. 32; NIS2 Art. 21	Are strong role-based access controls (RBAC) and multi-factor authentication (MFA) implemented?	☐	☐	☐

11	Encryption	GDPR Art. 32	Are personal data encrypted both in transit and at rest using current cryptographic standards?	☐	☐	☐
12	Incident Response	GDPR Art. 33-34; NIS2 Art. 23	Is there a formal incident response plan, and are significant security incidents reported as required?	☐	☐	☐
13	Secure Processing Environment	EHDS Regulation Art. 73	Does the platform architecture (SPE) prevent unauthorized data extraction?	☐	☐	☐
D. Governance & Accountability						
No.	**Requirement Area**	**Legal/Ethical Source**	**Self-Assessment Question**	**Yes**	**No**	**N/A**
14	Data Access Governance	EHDS Regulation Art. 45-46	Is all secondary data access preceded by a formal Data Permit application?	☐	☐	☐
15	Record-Keeping	GDPR Art. 30	Are records of all data processing activities comprehensive and up-to-date?	☐	☐	☐
16	FAIR Principles	Grant Agreement Annex 5	Are data and research outputs managed in accordance with the FAIR (Findable, Accessible, Interoperable, Reusable) principles?	☐	☐	☐
17	Ethics Oversight	D12.2 Ethics Req.	Has an independent, external Ethics Board (IEAB) been appointed to provide ongoing oversight?	☐	☐	☐

9.2

9.3 Annex 1.2 – Europrivacy Criteria Checklist

This Annex includes the checklist of the Europrivacy criteria, as approved by the European Data Protection Board. The consortium can leverage on these criteria as the reference for assessing and demonstrating compliance with the GDPR. These criteria are publicly available online: https://community.europrivacy.com/europrivacy-gdpr-core-criteria/.

The checklist includes the following abbreviations:

- Applicability to:
  - C: Controller
  - P: Processor
  - CP: Controller and Processor
- Type of requirement:
  - S: Specific Requirement (Assessed for each data processing activity)
  - G: Generic requirement (Assessed once per organization unless major changes apply)
- Level of application:
  - A: Applicable to all data processing
  - B: Applicable for high-risk data processing activities
  - E: Exemption condition (if applicable)

Criterion ID	Criterion Title	Applicability	Assessment (Compliant / Non-compliant / N/A)	Justification / Evidence	Actions Required
G.1	**Lawfulness of Data Processing**	Controller			
G.1.1.1	Lawfulness assessment of processing	C, S, A			
G.1.1.2	Lawfulness justification	C, S, A			
G.1.1.3	National Regulation Compliance	C, S, A			
G.1.1.4	Adequate qualification of the expert	C, S, A			
G.1.2	**Complementary requirements for valid consent** *(If consent-based)*	Consent-based			
G.1.2.1	Formal requirements for consent	C, S, A			
G.1.2.2	Absence of unnecessary constraints for consent	C, S, A			
G.1.2.3	Right to withdraw consent	C, S, A			

G.1.3	**Child's consent for Information Society Services** *(If applicable)*	ISS (Children <16)			
G.1.3.1	Lawfulness and parental consent verification	C, S, A			
G.2	**Special Data Processing** *(If applicable)*	Special Data			
G.2.1.1	Special categories of data – DPO validation	C, S, A			
G.2.1.2	Legal basis for processing special categories	C, S, A			
G.2.2.1	Data related to criminal convictions and offences	C, S, A			
G.3	**Rights of the Data Subjects**	Controller			
G.3.1.1	Duty to inform in clear language	C, S, A			
G.3.1.2	Facilitate data subject rights exercise	C, G, A			
G.3.1.3	Data subject rights management and recording	C, G, A			
G.3.1.4	Information without undue delay	C, G, A			
G.3.1.5	Electronic response	C, G, A			
G.3.1.6	Duty to inform and justify non-action	C, G, A			
G.3.1.7	Free of charge provision of information	C, G, A			
G.3.1.8	Machine-readability of icons *(If applicable)*	C, G, A			
G.3.2.1	Duty to inform at data collection	C, S, A			
G.3.2.2	Further processing communication	C, S, A			
G.3.2.3	Tolerated exemption (already informed)	C, S, A			
G.3.3.1	Duty to inform (data not obtained directly)	C, S, A			
G.3.3.2	Inform in due time (indirect collection)	C, S, A			
G.3.3.3	Inform on purpose extension (indirect)	C, S, A			

G.3.3.4	Tolerated exemption (indirect collection)	C, S, E			
G.3.4	**Right of access by data subject**	Controller			
G.3.4.1	Data subject right of access	C, S, A			
G.3.4.2	Provide a copy of data	C, S, A			
G.3.4.3	Protection of others' rights	C, S, A			
G.3.5	**Right to rectification**	Controller			
G.3.5.1	Effective rectification mechanism	C, S, A			
G.3.6	**Right to erasure ('right to be forgotten')**	Controller			
G.3.6.1	Effective erasure of data	C, S, A			
G.3.6.2	Inform other controllers *(if data made public)*	C, S, A			
G.3.6.3	Tolerated exemptions to erasure	C, S, E			
G.3.7	**Right to restriction of processing**	Controller			
G.3.7.1	Effective restriction mechanism	C, S, A			
G.3.8	**Notification obligation regarding rectification, erasure or restriction**	Controller			
G.3.8.1	Inform recipients	C, S, A			
G.3.8.2	Inform data subjects on recipients	C, S, A			
G.3.9	**Right to data portability** *(If consent/contract-based)*	Consent/Contract			
G.3.9.1	Data portability	C, S, A			
G.3.10	**Right to object**	Controller			
G.3.10.1	Effective objection mechanism	C, S, A			
G.3.10.2	Clear information on right to object	C, S, A			
G.3.11	**Right related to automated decision-making/profiling** *(If applicable)*	Automated decisions			
G.3.11.1	Automated decisions compliance	C, S, A			

G.3.11.2	Human intervention and contestation	C, S, A			
G.4	**Data Controller Responsibility**	Controller			
G.4.1.1	Documentation of technical & organisational measures	C, S, A			
G.4.1.2	Regular review/update of measures	C, S, A			
G.4.1.3	Data Protection Policies documentation	C, S, A			
G.5	**Data Processors (or sub-processors)** *(If processors involved)*	Processor			
G.5.1.1	Restriction on use of Processors	CP, S, A			
G.5.1.2	Contractual obligations (Controller)	C, S, A			
G.5.1.3	Contractual obligations (Processor)	P, S, A			
G.5.1.4	Detailed contractual obligations of Processors	CP, S, A			
G.5.1.5	Complementary demonstration of Processors' compliance	CP, S, A			
G.5.2.1	Processing under Controller instructions only	P, S, A			
G.5.3.1	Records of processing activities by Controller	C, G, A			
G.5.3.2	Records of processing activities by Processor	P, G, A			
G.5.3.3	Data processing instructions records	CP, S, A			
G.5.3.4	Completeness of processing registry	CP, S, A			
G.6	**Security of Processing & Data Protection by Design**	Controller & Processor			
G.6.1.1	Data protection by design & default	C, S, A			
G.6.1.2	Data minimisation by default	C, S, A			
G.6.2.1	Security policy	CP, G, A			

G.6.2.2	Processing on Controller instruction only	CP, G, A			
G.6.2.3	Contractual confidentiality obligations	CP, G, A			
G.6.2.4	Risk assessment on data processing	CP, S, A			
G.6.2.5	Access rights policy & registry	CP, S, A			
G.6.2.6	Access & transfer logs	CP, S, A			
G.6.2.7	Continuity, integrity & availability measures	CP, S, A			
G.6.2.8	Communication encryption	CP, S, A			
G.6.2.9	Data backup obligation	CP, S, A			
G.6.2.10	Complementary Contextual Requirements	CP, S, A			
G.6.2.11	Complementary Technical & Organisational Measures	CP, S, A			
G.7	**Management of Data Breaches**	Controller & Processor			
G.7.1.1	Documentation of data breaches	CP, G, A			
G.7.1.2	Controller notification of data breaches	C, G, A			
G.7.1.3	Processor communication of data breaches	P, G, A			
G.7.1.4	Notification content to Supervisory Authority	C, G, A			
G.7.2.1	Data breach communication to data subjects	C, G, A			
G.7.2.2	Tolerated exemptions to data breach communication	C, S, E			
G.8	**Data Protection Impact Assessment (DPIA)** *(If DPIA required)*	DPIA-required			
G.8.1.1	DPIA requirement assessment	C, S, A			
G.8.1.2	Tolerated exemptions for DPIA	C, S, E			

G.8.2.1	DPIA process requirements	C, S, A			
G.8.2.2	DPIA content requirements	C, S, A			
G.8.2.3	Data subjects' involvement in DPIA	C, S, A			
G.8.2.4	DPIA review (change of risks)	C, S, A			
G.8.2.5	Supervisory Authority consultation (high risks)	C, S, A			
G.9	**Data Protection Officer (DPO)**	Controller & Processor			
G.9.1.1	Designation of DPO	CP, G, A			
G.9.1.2	Qualification of DPO	CP, G, A			
G.9.1.3	Communication of DPO contact details	CP, G, A			
G.9.2.1	DPO mandate & involvement	CP, G, A			
G.9.2.2	DPO resources & training	CP, G, A			
G.9.2.3	DPO independence & reporting	CP, G, A			
G.9.2.4	Data subjects' access to DPO	CP, G, A			
G.9.2.5	DPO contractual clauses	CP, G, A			
G.9.2.6	Adequacy of DPO working time	CP, G, A			
G.9.3.1	Tasks & duties of DPO	CP, G, A			
G.9.3.2	Personnel training on data protection	CP, G, A			
G.10	**Transfers to third countries/international organisations** *(If applicable)*	Cross-border			
G.10.1.1	Validation of cross-border transfer legality	CP, S, A			
G.10.1.2	Cross-border transfer legal basis	CP, S, A			
G.10.1.3	Appropriate safeguards for transfer	CP, S, A			
G.10.1.4	Transfer based on derogations	CP, S, A			
G.10.1.5	Complementary risk assessment (no adequacy decision)	CP, S, A			
G.10.1.6	Binding commitment of data receiver	CP, S, A			

G.10.2.1	Complementary appropriate safeguards for transfers	CP, S, A			

9.4 Annex 1.3 –Assessment List for Trustworthy AI (ALTAI)

This Annex includes the list of self-assessment questions for Trustworthy AI, as provided by the High-Level Expert Group on AI set up by the European Commission.[186]

- **Fundamental Rights**
  1. Does the AI system potentially negatively discriminate against people on the basis of any of the following grounds (non-exhaustively): sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation?
  2. Have you put in place processes to test and monitor for potential negative discrimination (bias) during the development, deployment and use phases of the AI system?
  3. Have you put in place processes to address and rectify for potential negative discrimination (bias) in the AI system?
  4. Does the AI system respect the rights of the child, for example with respect to child protection and taking the child's best interests into account?
  5. Have you put in place processes to address and rectify for potential harm to children by the AI system?
  6. Have you put in place processes to test and monitor for potential harm to children during the development, deployment and use phases of the AI system?
  7. Does the AI system protect personal data relating to individuals in line with GDPR?
  8. Have you put in place processes to assess in detail the need for a data protection impact assessment, including an assessment of the necessity and proportionality of the processing operations in relation to their purpose, with respect to the development, deployment and use phases of the AI system?
  9. Have you put in place measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data with respect to the development, deployment and use phases of the AI system?
  10. Does the AI system respect the freedom of expression and information and/or freedom of assembly and association?
  11. Have you put in place processes to test and monitor for potential infringement on freedom of expression and information, and/or freedom of assembly and association, during the development, deployment and use phases of the AI system?
  12. Have you put in place processes to address and rectify for potential infringement on freedom of expression and information, and/or freedom of assembly and association, in the AI system?

<u>Requirement 1 - Human Agency and Oversight</u>

- **Human Agency and Autonomy**
  1. Is the AI system designed to interact, guide or take decisions by human end-users that affect humans or society?

[186] High Level Expert Group on Artificial Intelligence (AI HLEG). The Assessment List for Trustworthy Artificial Intelligence (ALTAI). 2020.

   a. Could the AI system generate confusion for some or all end-users or subjects on whether a decision, content, advice or outcome is the result of an algorithmic decision?
   b. Are end-users or other subjects adequately made aware that a decision, content, advice or outcome is the result of an algorithmic decision?

2. Could the AI system generate confusion for some or all end-users or subjects on whether they are interacting with a human or AI system?
   a. Are end-users or subjects informed that they are interacting with an AI system?
3. Could the AI system affect human autonomy by generating over-reliance by end-users?
   a. Did you put in place procedures to avoid that end-users over-rely on the AI system?
4. Could the AI system affect human autonomy by interfering with the end-user's decision-making process in any other unintended and undesirable way?
   a. Did you put in place any procedure to avoid that the AI system inadvertently affects human autonomy?
5. Does the AI system simulate social interaction with or between end-users or subjects?
6. Does the AI system risk creating human attachment, stimulating addictive behaviour, or manipulating user behaviour? Depending on which risks are possible or likely, please answer the questions below:
   a. Did you take measures to deal with possible negative consequences for end-users or subjects in case they develop a disproportionate attachment to the AI System?
   b. Did you take measures to minimise the risk of addiction?
   c. Did you take measures to mitigate the risk of manipulation?

- **Human Oversight**
  1. Please determine whether the AI system (choose as many as appropriate):
     a. Is a self-learning or autonomous system;
     b. Is overseen by a Human-in-the-Loop;
     c. Is overseen by a Human-on-the-Loop;
     d. Is overseen by a Human-in-Command.
  2. Have the humans (human-in-the-loop, human-on-the-loop, human-in-command) been given specific training on how to exercise oversight?
  3. Did you establish any detection and response mechanisms for undesirable adverse effects of the AI system for the end-user or subject?
  4. Did you ensure a 'stop button' or procedure to safely abort an operation when needed?
  5. Did you take any specific oversight and control measures to reflect the self-learning or autonomous nature of the AI system?

Requirement 2 - Technical Robustness and Safety

- **Resilience to Attack and Security**
  1. Could the AI system have adversarial, critical or damaging effects (e.g. to human or societal safety) in case of risks or threats such as design or technical faults, defects, outages, attacks, misuse, inappropriate or malicious use?
  2. Is the AI system certified for cybersecurity (e.g. the certification scheme created by the Cybersecurity Act in Europe) or is it compliant with specific security standards?

3. How exposed is the AI system to cyber-attacks?
    a. Did you assess potential forms of attacks to which the AI system could be vulnerable?
    b. Did you consider different types of vulnerabilities and potential entry points for attacks such as:
        i. Data poisoning (i.e. manipulation of training data);
        ii. Model evasion (i.e. classifying the data according to the attacker's will);
        iii. Model inversion (i.e. infer the model parameters)
4. Did you put measures in place to ensure the integrity, robustness and overall security of the AI system against potential attacks over its lifecycle?
5. Did you red-team/pentest the system?
6. Did you inform end-users of the duration of security coverage and updates?
    a. What length is the expected timeframe within which you provide security updates for the AI system?

- **General Safety**
    1. Did you define risks, risk metrics and risk levels of the AI system in each specific use case?
        a. Did you put in place a process to continuously measure and assess risks?
        b. Did you inform end-users and subjects of existing or potential risks?
    2. Did you identify the possible threats to the AI system (design faults, technical faults,
    3. environmental threats) and the possible consequences?
        a. Did you assess the risk of possible malicious use, misuse or inappropriate use of the AI system?
        b. Did you define safety criticality levels (e.g. related to human integrity) of the possible consequences of faults or misuse of the AI system?
    4. Did you assess the dependency of a critical AI system’s decisions on its stable and reliable behaviour?
        a. Did you align the reliability/testing requirements to the appropriate levels of stability and reliability?
    5. Did you plan fault tolerance via, e.g. a duplicated system or another parallel system (AI-based or ‘conventional’)?
    6. Did you develop a mechanism to evaluate when the AI system has been changed to merit a new review of its technical robustness and safety?

- **Accuracy**
    1. Could a low level of accuracy of the AI system result in critical, adversarial or damaging consequences?
    2. Did you put in place measures to ensure that the data (including training data) used to develop the AI system is up-to-date, of high quality, complete and representative of the environment the system will be deployed in?
    3. Did you put in place a series of steps to monitor, and document the AI system’s accuracy?
    4. Did you consider whether the AI system's operation can invalidate the data or assumptions it was trained on, and how this might lead to adversarial effects?
    5. Did you put processes in place to ensure that the level of accuracy of the AI system to be expected by end-users and/or subjects is properly communicated?

- **Reliability, Fall-back plans and Reproducibility**

1. Could the AI system cause critical, adversarial, or damaging consequences (e.g. pertaining to human safety) in case of low reliability and/or reproducibility?
    a. Did you put in place a well-defined process to monitor if the AI system is meeting the intended goals?
    b. Did you test whether specific contexts or conditions need to be taken into account to ensure reproducibility?
2. Did you put in place verification and validation methods and documentation (e.g. logging) to evaluate and ensure different aspects of the AI system's reliability and reproducibility?
    a. Did you clearly document and operationalise processes for the testing and verification of the reliability and reproducibility of the AI system?
3. Did you define tested failsafe fallback plans to address AI system errors of whatever origin and put governance procedures in place to trigger them?
4. Did you put in place a proper procedure for handling the cases where the AI system yields results with a low confidence score?
5. Is your AI system using (online) continual learning?
    a. Did you consider potential negative consequences from the AI system learning novel or unusual methods to score well on its objective function?

Requirement 3 - Privacy and Data Governance

1. Did you consider the impact of the AI system on the right to privacy, the right to physical, mental and/or moral integrity and the right to data protection?
2. Depending on the use case, did you establish mechanisms that allow flagging issues related to privacy concerning the AI system?

- **Data Governance**

1. Is your AI system being trained, or was it developed, by using or processing personal data (including special categories of personal data)?
2. Did you put in place any of the following measures some of which are mandatory under the General Data Protection Regulation (GDPR), or a non-European equivalent?
    a. Data Protection Impact Assessment(DPIA);
    b. Designate a Data Protection Officer (DPO) and include them at an early state in the development, procurement or use phase of the AI system;
    c. Oversight mechanisms for data processing (including limiting access to qualified personnel, mechanisms for logging data access and making modifications);
    d. Measures to achieve privacy-by-design and default (e.g. encryption, pseudonymisation, aggregation, anonymisation);
    e. Data minimisation, in particular personal data (including special categories of data);
3. Did you implement the right to withdraw consent, the right to object and the right to be forgotten into the development of the AI system?
4. Did you consider the privacy and data protection implications of data collected, generated or processed over the course of the AI system's life cycle?
5. Did you consider the privacy and data protection implications of the AI system's non-personal training-data or other processed non-personal data?
6. Did you align the AI system with relevant standards (e.g. ISO25, IEEE26) or widely adopted protocols for (daily) data management and governance?

Requirement 4 - Transparency

- **Traceability**
  1. Did you put in place measures that address the traceability of the AI system during its entire lifecycle?
     a. Did you put in place measures to continuously assess the quality of the input data to the AI system?
     b. Can you trace back which data was used by the AI system to make a certain decision(s) or recommendation(s)?
     c. Can you trace back which AI model or rules led to the decision(s) or recommendation(s) of the AI system?
     d. Did you put in place measures to continuously assess the quality of the output(s) of the AI system?
     e. Did you put adequate logging practices in place to record the decision(s) or recommendation(s) of the AI system?

- **Explainability**
  1. Did you explain the decision(s) of the AI system to the users?
  2. Do you continuously survey the users if they understand the decision(s) of the AI system?

- **Communication**
  1. In cases of interactive AI systems (e.g., chatbots, robo-lawyers), do you communicate to users that they are interacting with an AI system instead of a human?
  2. Did you establish mechanisms to inform users about the purpose, criteria and limitations of the decision(s) generated by the AI system?
     a. Did you communicate the benefits of the AI system to users?
     b. Did you communicate the technical limitations and potential risks of the AI system to users, such as its level of accuracy and/ or error rates?
     c. Did you provide appropriate training material and disclaimers to users on how to adequately use the AI system?

Requirement 5 - Diversity, Non-discrimination and Fairness

- **Avoidance of Unfair Bias**
  1. Did you establish a strategy or a set of procedures to avoid creating or reinforcing unfair bias in the AI system, both regarding the use of input data as well as for the algorithm design?
  2. Did you consider diversity and representativeness of end-users and/or subjects in the data?
     a. Did you test for specific target groups or problematic use cases?
     b. Did you research and use publicly available technical tools, that are state-of-the-art, to improve your understanding of the data, model and performance?
     c. Did you assess and put in place processes to test and monitor for potential biases during the entire lifecycle of the AI system (e.g. biases due to possible limitations stemming from the composition of the used data sets (lack of diversity, non-representativeness)?
     d. Where relevant, did you consider diversity and representativeness of end-users and or subjects in the data?
  3. Did you put in place educational and awareness initiatives to help AI designers and AI developers be more aware of the possible bias they can inject in designing and developing the AI system?

4. Did you ensure a mechanism that allows for the flagging of issues related to bias, discrimination or poor performance of the AI system?
    a. Did you establish clear steps and ways of communicating on how and to whom such issues can be raised?
    b. Did you identify the subjects that could potentially be (in)directly affected by the AI system, in addition to the (end-)users and/or subjects?
5. Is your definition of fairness commonly used and implemented in any phase of the process of setting up the AI system?
    a. Did you consider other definitions of fairness before choosing this one?
    b. Did you consult with the impacted communities about the correct definition of fairness, i.e. representatives of elderly persons or persons with disabilities?
    c. Did you ensure a quantitative analysis or metrics to measure and test the applied definition of fairness?
    d. Did you establish mechanisms to ensure fairness in your AI system?

- **Accessibility and Universal Design**
    1. Did you ensure that the AI system corresponds to the variety of preferences and abilities in society?
    2. Did you assess whether the AI system's user interface is usable by those with special needs or disabilities or those at risk of exclusion?
        a. Did you ensure that information about, and the AI system's user interface of, the AI system is accessible and usable also to users of assistive technologies (such as screen readers)?
        b. Did you involve or consult with end-users or subjects in need for assistive technology during the planning and development phase of the AI system?
    3. Did you ensure that Universal Design principles are taken into account during every step of the planning and development process, if applicable?
    4. Did you take the impact of the AI system on the potential end-users and/or subjects into account?
        a. Did you assess whether the team involved in building the AI system engaged with the possible target end-users and/or subjects?
        b. Did you assess whether there could be groups who might be disproportionately affected by the outcomes of the AI system?
        c. Did you assess the risk of the possible unfairness of the system onto the end-user's or subject's communities?

- **Stakeholder Participation**
    1. Did you consider a mechanism to include the participation of the widest range of possible stakeholders in the AI system’s design and development?

Requirement 6 - Societal and Environmental Well-being

- **Environmental Well-being**
    1. Are there potential negative impacts of the AI system on the environment? o Which potential impact(s) do you identify?
    2. Where possible, did you establish mechanisms to evaluate the environmental impact of the AI system’s development, deployment and/or use (for example, the amount of energy used and carbon emissions)?
        a. Did you define measures to reduce the environmental impact of the AI system throughout its lifecycle?

- **Impact on Work and Skills**
  1. Does the AI system impact human work and work arrangements?
  2. Did you pave the way for the introduction of the AI system in your organisation by informing and consulting with impacted workers and their representatives (trade unions, (European) work councils) in advance?
  3. Did you adopt measures to ensure that the impacts of the AI system on human work are well understood?
     a. Did you ensure that workers understand how the AI system operates, which capabilities it has and which it does not have?
  4. Could the AI system create the risk of de-skilling of the workforce?
     a. Did you take measures to counteract de-skilling risks? • Does the system promote or require new (digital) skills?
     b. Did you provide training opportunities and materials for re- and up-skilling? Impact on Society at large or Democracy
  5. Could the AI system have a negative impact on society at large or democracy?
     a. Did you assess the societal impact of the AI system's use beyond the (end-)user and subject, such as potentially indirectly affected stakeholders or society at large?
     b. Did you take action to minimize potential societal harm of the AI system? o Did you take measures that ensure that the AI system does not negatively impact democracy?

Requirement 7 - Accountability

1. Did you establish mechanisms that facilitate the AI system's auditability (e.g. traceability of the development process, the sourcing of training data and the logging of the AI system's processes, outcomes, positive and negative impact)?
2. Did you ensure that the AI system can be audited by independent third parties?

- **Risk Management**
  1. Did you foresee any kind of external guidance or third-party auditing processes to oversee ethical concerns and accountability measures?
     a. Does the involvement of these third parties go beyond the development phase?
  2. Did you organise risk training and, if so, does this also inform about the potential legal framework applicable to the AI system?
  3. Did you consider establishing an AI ethics review board or a similar mechanism to discuss the overall accountability and ethics practices, including potential unclear grey areas?
  4. Did you establish a process to discuss and continuously monitor and assess the AI system's adherence to this Assessment List for Trustworthy AI (ALTAI)?
     a. Does this process include identification and documentation of conflicts between the 6 aforementioned requirements or between different ethical principles and explanation of the 'trade-off' decisions made?
     b. Did you provide appropriate training to those involved in such a process and does this also cover the legal framework applicable to the AI system?
  5. Did you establish a process for third parties (e.g. suppliers, end-users, subjects, distributors/vendors or workers) to report potential vulnerabilities, risks or biases in the AI system?
     a. Does this process foster revision of the risk management process?
6. For applications that can adversely affect individuals, have redress by design mechanisms been put in place?