D7.1 Ethical and Legal Framework

Deliverable No.	D7.1	**Due Date**	30/11/2023
Description	The objective of this deliverable is to report on the Framework with the relevant regulatory, privacy and ethical initiatives.		
Type	Report	**Dissemination Level**	PU
Work Package No.	WP7	**Work Package Title**	Legal and Ethics
Version	V1.0	**Status**	Final

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement N° 101057747

Authors

Name and surname	Partner name	e-mail
Christos Koziaris	QUAN	Christos.koziaris@gmail.com
Kyriaki Karydou	VILABS	kyriaki-karydou@vilabs.eu
Nikolaos Vasileiou	ICCS	nvasileiou@biomed.ntua.gr

History

Date	Version	Change
08/11/2023	V0.1	1st Draft (Outline)
	V0.2	2nd Draft - Includes contribution by VILABS for chapter 6 'Gender Equality' - Includes contribution by ICCS for chapter 6 'Gender Equality'
30/11/2023	V3.0	Final Draft (Consolidated) for Review - All chapters were completed + Annexes
08/12/2023	V1.0	Final for Submission - Following reviews comments and suggestions, texts have been incorporated and track changes cleared (accepted/deleted) - Deliverable approved by the PC and submitted

Key data

Keywords	Legal, Ethical, Personal Data, GDPR
Lead Editor	(QUAN) Christos Koziaris
Internal Reviewer(s)	(VILABS) Kyriaki karydou (ICCS) Nikos Vasileiou, Maria Haritou

Abstract

The document presents a comprehensive and detailed report on the Ethical and Legal Framework of the TeleRehaB DSS project, which includes an overview of relevant regulatory, privacy, and ethical initiatives.

The report aims to provide a thorough understanding of the current landscape, identify any gaps, and propose potential solutions that can help improve the overall effectiveness and compliance of the Framework.

Additionally, the report will highlight any key challenges, risks, and opportunities associated with the Framework and provide recommendations for mitigating these issues. Overall, the report will serve as a valuable resource for stakeholders involved in the development, implementation, and monitoring of the Framework.

Statement of originality

This deliverable contains original unpublished work except where clearly indicated otherwise.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

Table of contents

1 Introduction

1.1 Background

TeleRehaB DSS is an ambitious innovative project that aims to revolutionise balance rehabilitation training using Artificial Intelligence (AI). The primary goal is to develop an AI-based Decision Support System (DSS) that will improve precision treatment for patients at risk of falls, both in clinical settings and through remote home-based care. This comprehensive tool will cover the entire clinical pathway, offering personalised rehabilitation interventions, assessing prognostic factors, and providing automated balance intervention planning and management.

In TeleRehaB DSS, AI will play a crucial role in supporting decision-making processes for healthcare professionals. This will involve analysing retrospective and also prospective data for risk assessment and treatment effectiveness, introducing automated intervention planning, and real-time monitoring using wearables and IoT devices. The AI models will ensure effective and affordable treatments for patients while providing valuable insights at the public health policy level.

Ultimately, TeleRehaB DSS embodies the future of balance rehabilitation, integrating cutting-edge AI technologies to optimise patient care and enhance overall public health outcomes.

1.2 Scope

In the context of the TeleRehaB DSS project (Dec 2022 – Nov 2025) [1], this document covers the ethical and legal framework applicable in three major areas: personal data processing, AI processing, and the clinical study

Personal data are any piece of information that relates to an identified or identifiable living individual, which can be used to identify the person, either directly or indirectly. This includes, but is not limited to, name, address, email, identification number, location data, and online identifier. In some cases, even a combination of seemingly innocuous information can be used to identify an individual.

The data collected during the clinical study are considered personal data, as it pertains to the health and medical history of an individual. This data includes all information collected during the clinical trial, such as participants' medical records, test results, and any genetic or biometric data. The governance of clinical data is essential to ensure privacy and confidentiality of the participants according to the relevant regulatory framework.

On the other hand, personal data that has been fully anonymised are not considered personal data. This means that all identifiable information has been removed from the data to ensure that it can no longer be linked to an individual.

The clinical study will run from month 12 to month 32, with the aim of validating the TeleRehaB DSS based on artificial intelligence (AI), by comparing its benefits and cost-effectiveness with the standard-of-care. The University of Ioannina (UOI), as technical coordinator, will support the clinical study and oversee all technical matters related to the use of the platform and its components [2].

1.3 Purpose and Objectives

This document aims to provide a comprehensive analysis of the legal and ethical landscape that is relevant to the project. It will delve into the intricate details of the framework and explore the various issues that arise within it. Additionally, it will provide actionable initiatives that can be taken to address these issues and capitalise on the opportunities that exist within this landscape.

1.4 Document Structure

The document contains the following main chapters

Overview of the Legal and Ethical Framework. This chapter outlines the legal and ethical framework that applies to the project and lists the relevant areas that will be further analysed.

In the upcoming chapters, the document delves into a more detailed analysis of each specific area and examine it in the context of the regulatory framework that applies to it. By doing so, the objective is to gain a comprehensive understanding of how these areas function and the impact that regulations have on the project:

- **Clinical Trials Regulation | Ethical Standards and Guidelines.** The chapter covers the Clinical Trials regulation that applies to the clinical study.
- **AI Framework.** The chapter covers the AI act which is proposed to take effect that applies to the AI processing.
- **Data Transfers.** This chapter addresses the issues that arise when transferring personal data within EU or outside EU that GDPR has to be applicable taking privacy and security measures.
- **General Data Protection Regulation Compliance.** The chapter covers the AI act which is proposed to take effect that applies to the AI processing.
- **CE Mark.** The chapter covers the AI act which is proposed to take effect that applies to the AI processing.
- **Gender Equality.** The chapter covers the Gender Equality in order to perform a more inclusive and unbiased clinical study.

The document also focuses on specific areas with significant impact, such as:

- **Joint Controllers and Data Processors Agreement**. This chapters addresses the agreement that has to be in place before the clinical study and before collecting personal data. The agreement has to be signed off by all parties that will process personal data.

- **Security and Privacy Measures.** This document provides a concise explanation of the specific technical measures that need to be taken in order to ensure compliance with relevant security and privacy frameworks. It outlines the steps that must be taken to protect sensitive data, prevent unauthorised access, and maintain the integrity of the network and systems.

2 Overview of the Legal and Ethical Framework

As previously stated, in the introduction paragraph, (1.1 Background) the TeleRehaB DSS project aims to conduct a clinical study involving participants. The study will involve processing their personal information to provide customised rehabilitation interventions, assessing prognostic factors, and offering automated balance intervention planning and management.

Given that the project is funded by the EU and will mostly take place within the EU, the regulatory environment of the EU has been taken into account. Therefore, the following legal and ethical aspects must be incorporated into the framework:

- **Clinical Ethical Standards and Guidelines and relevant Regulation,**
- **AI Act and relevant Regulation,**
- **Data Transfers,**
- **General Data Protection Regulation,**
- **Gender Equality,**
- **CE Mark.**

The document also focuses on specific areas with significant impact, such as:

- **Joint Controllers and Data Processors Agreement,**
- **Security and Privacy Measures.**

The following chapters provide in-depth analysis of the aforementioned areas and expound on the relevant requirements.

3 Clinical Trials Regulation | Ethical Standards and Guidelines

The members of the consortium fully support the TeleRehaB DSS study's conformity with the current legislation and regulations in the countries where the research will be conducted. This implies that the Consortium respects people, their dignity, and ensures a fair distribution of the benefits and burden of research, while protecting the research participants' values, rights, and interests. Additionally, the TeleRehaB DSS study complies with relevant EU legislation, such as:

- the Charter of Fundamental Rights of the EU, the Declaration of Helsinki (World Medical Association - Declaration of Helsinki) [3],
- the regulation 2016/679/EC on "the protection of individuals with regard to the processing of personal data and the free movement of such data" [4],
- the directive 2002/58/EC on "processing of personal data and the protection of privacy in the electronic communications sector." [4]
- the opinions of the European Group of Advisers on the Ethical Implications of Biotechnology (1991-1997) [5] and
- the opinions of the European Group on Ethics in Science and New Technologies (as from 1998).

Before conducting any TeleRehaB DSS studies, the research teams will ensure that ethical committee approval has been obtained in each country where the study will take place. This means that the study will only be conducted after receiving approval from the respective ethical committees and data protection authorities of each country.

The ethical committee approval process involves a thorough review of the study protocol and procedures to ensure that the study will be conducted in an ethical and safe manner. The review will assess the potential risks and benefits of the study for participants, as well as the measures in place to protect their privacy and personal data.

Once the ethical committee approves the study, the research team can proceed with data collection and analysis. However, if the study does not receive approval from the ethical committee or data protection authorities of a country, the research team will not be able to conduct the study in that country. This ensures that the rights and safety of study participants are always protected and respected.

Detailed information about the study protocols in compliance with the current EU regulations (536/2014) is available and also the process to obtain ethics approval for the five clinical sites has been completed in time for the clinical validation study to be conducted, in the TeleRehaB document D5.1 Study initiation package [2]

3.1 Informed Consent (IC)

An essential condition for acquiring a subject's (person's) Informed Consent to participate in clinical research is the satisfaction of the scientific and ethical rigor principles.

With regard to ethical principles and their application to the IC the following must be taken into particular consideration:

- the principle of respect for the dignity of the subject (person);
- the principle of respecting the right to self-determination of the competent subjects involved in the trial;
- the fairness of the risk/benefit ratio

It is crucial to ensure that the consent request and information documents are worded in a manner that guarantees complete compliance and application of the principles that guide the practice of Informed Consent. The aim is to make the participant aware that they are not merely being subjected to the experiment, but are actively choosing to participate in it.

The IC and the patient information form tend to guarantee the alliance or therapeutic agreement between doctor/investigator and patient; they should take a formulation that explicitly declares and specifies the positions of the subjects in question, their respective obligations, and rights, commitments, and waivered required and expected. From an ethical and deontological point of view, these aspects do not have a value. They are only theoretical, but they imply a practical commitment in the doctor / patient relationship context.

These preliminary considerations are described in particular by the paragraph "Informed Consent, Special Communication: arts. 25-32 "of the Declaration of Helsinki (D.H.: World Medical Association Declaration of Helsinki, Ethical Principles for Medical Research Involving Human Subjects) [3] to which a series of clearly expressed and shared criteria are reported. Specifically, art. 22. of the D.H. reads:

"*The design and performance of each research study involving human subjects must be clearly described and justified in a research protocol. The protocol should contain a statement of the ethical considerations involved and should indicate how the principles in this Declaration have been addressed. The protocol should include information regarding funding, sponsors, institutional affiliations, potential conflicts of interest, incentives for subjects, and information regarding provisions for treating and/or compensating subjects who are harmed as a consequence of participation in the research study. In clinical trials, the protocol must also describe appropriate arrangements for post-trial provisions.* "

Here, it implicitly refers to the following ethical principles explained explicitly in other articles:

- the duty of the doctor/investigator to safeguard the health, well-being, and rights of the patient (D.H., art.4);

- the commitment of the doctor/investigator to protect life, health, dignity, integrity, right to self- determination, privacy, and confidentiality, as well as the affirmation that the responsibility for the protection of research subjects always lies with the doctor or health professionals and never with the research subjects (D.H., art.9);
- the duties regarding the scientific and technical standards with which the research is conducted (D.H., articles 12 and 21);
- the patient's right not to participate in the experimental project or to withdraw from it, at any time, without risking any form of retaliation (D.H., art.26).

It is essential to document the informed consent process using a written form that should be signed and personally dated by the subject and the experimenter doctor/investigator who provided the relevant information. The form must comply with the principles of Helsinki, which are in accordance with "good clinical practice" and should be assessed and approved by the independent ethical committee.

Throughout the study, the text of the informed consent can be modified following an amendment every time there is new information about the study protocol. The changes made must be approved by the Ethical Committee, and the person involved must be informed and must sign the new consent form.

It is important to note that the subject has the right to withdraw his/her consent during the study at any time.

In any case, the offer of a written consent form may replace the personalised interview.

For this purpose, it is advisable to carry out the interview in a comfortable environment and in a relaxed and serene atmosphere, aiming to comprehensively inform the participant in an effective and efficient way, avoiding information overload. Criteria of exhaustiveness, conciseness, cost-effectiveness, efficiency, and effectiveness, aimed at preventing information overload, are particularly relevant in drafting the form of information that the participant will have to read and subscribe to.

Before granting one's consent, the subject must have the time necessary to inquire about the details of the experimentation, reflect and decide without any pressure or constraint. In fact, there is talk of the process of informed consensus that is marked several times:

1. First meeting with the reference doctor of the study in which the clinical study illustrates and dialogues with the person involved so that the experimentation is understood. The doctor/investigator provides the documents and illustrates all aspects in detail: Module of informed consent, in its two substantially related sections i.e., Information section relating to the protocol and the rights of the person; Section for the expression of consent; Authorisation to the processing of personal and sensitive data, as ordered by the privacy law (Legislative Decree no. 196/2003, and subsequent amendments);
2. Time to reflect in which the person involved has the opportunity to carefully read the information received from the doctor/investigator, to confront third parties, family members, and friends, with their doctor.
3. If the subject agrees to participate in the study, he/she is asked to date and sign the informed consent at the doctor's office. A copy of this document is delivered to the patient.

4. Willing to confront and talk to the patient during the study continuously and on the basis of the planned phases. In fact, informed consent is a continuous information process that takes place throughout the clinical study, including the follow-up period, and is not an impromptu act.

The art. 26 of the D.H:

"*In medical research involving human subjects capable of giving informed consent, each potential subject must be adequately informed of the aims, methods, sources of funding, any possible conflicts of interest, institutional affiliations of the researcher, the anticipated benefits and potential risks of the study and the discomfort it may entail, post-study provisions and any other relevant aspects of the study. The potential subject must be informed of the right to refuse to participate in the study or withdraw consent to participate at any time without reprisal. Special attention should be given to the specific information needs of individual potential subjects as well as to the methods used to deliver the information. After ensuring that the potential subject has understood the information, the physician or another appropriately qualified individual must then seek the potential subject's freely-given informed consent, preferably in writing. If the consent cannot be expressed in writing, the non-written consent must be formally documented and witnessed. All medical research subjects should be given the option of being informed about the general outcome and results of the study*".

3.2 Difference between INFORMED CONSENT and PRIVACY CONSENT

In the field of scientific research, it is essential to understand the difference between:

- Informed consent of participants in research projects involving subjects (persons), and
- consent to the processing of their personal data (so-called "privacy consent")

The differences are both conceptual and operational, and also the "Preliminary Opinion on Data Protection and Scientific Research" of the European Data Protection Supervisor (EDPS) urges not to consider them as a single and indivisible requirement [6].

The privacy consent does not concern the research project as a whole, but the processing of the participant's personal data (so-called "*interested*") that the data controller (investigator centre, pharmaceutical company, or medical device company who holds the role of promoter/sponsor, etc.) carried out in the context of a clinical study.

The GDPR defines consent to the processing of personal data as an "*Unequivocal positive act by which the interested party expresses the free, specific, informed and unequivocal intention to accept the processing of personal data concerning him [...]*".

As far as the interaction between the General Data Protection Regulation 2016/679 (GDPR) [4], which entered into force on 25 May 2018, and the Regulation [7] on clinical trials (CTR), that came into full effect in 2022 and replaced the Clinical Trials Directive (2001/20/EC) [8], it's important to underline that the GDPR guarantees the protection of individuals with regard to the processing of personal data and harmonised rules on

the free circulation of such data, the CTR aims to ensure greater harmonisation of the rules on the conduct of clinical trials across the EU. These two regulations apply simultaneously, and that the CTR constitutes a sectoral regulation that includes specific provisions relevant from the point of view of data protection and does not derogate from the GDPR.

In order to clarify the difference between informed consent based on the regulation for clinical trials and the (privacy) consent of the GDPR, and avoid possible misunderstanding, the following apply:

- The requirement of informed consent by the CTR must not be confused with the privacy consent as a legal reason for the processing of personal data referred to in Article 6, paragraph 1, letter a) of the GDPR.
- The IC required by The Clinical Trials Regulation serves as an ethical standard and procedural obligation. IC under the CTR is the basic condition under which a person can be included in a clinical trial. It is not intended as a tool for compliance with data processing.

Processing data related to clinical trials under GDPR involves various operations, which include research-related operations and those necessary for the protection of health or carried out in the public interest. These processing operations may be based on different legal grounds, depending on the situation. For instance, if data processing is necessary for the protection of vital interests of the data subject or another person, the legal basis would be Article 6(1)(d) of the GDPR. However, if the processing is carried out for scientific research purposes, the legal basis would be Article 9(2)(j) of the GDPR.

It is the responsibility of the controller to assess and implement the most appropriate legal basis for each processing operation. The controller must ensure that the legal basis used is lawful and that the processing operation complies with GDPR requirements.

When it comes to personal data processing, explicit consent is required. This means that the data subject must provide clear and affirmative consent for their data to be processed. Consent must be free, specific, informed, and unambiguous, particularly for sensitive data like health information. The data controller must ensure that they obtain explicit consent before processing any data and must keep records of such consent. Additionally, data subjects have the right to withdraw their consent at any time.

4 AI Framework

The European Union (EU) is at the forefront of developing guidelines and regulations for artificial intelligence (AI). In 2018, the EU Commission published Ethics Guidelines for Trustworthy AI [9], which outlined seven key requirements for trustworthy AI systems:

- **Human agency and oversight**: AI systems should empower human beings, allowing them to make informed decisions and fostering their fundamental rights. At the same time, proper oversight mechanisms need to be ensured, which can be achieved through human-in-the-loop, human-on-the-loop, and human-in-command approaches.
- **Technical Robustness and safety**: AI systems need to be resilient and secure. They need to be safe, ensuring a fallback plan in case something goes wrong, as well as being accurate, reliable and reproducible. That is the only way to ensure that also unintentional harm can be minimised and prevented.
- **Privacy and data governance**: besides ensuring full respect for privacy and data protection, adequate data governance mechanisms must also be ensured, taking into account the quality and integrity of the data, and ensuring legitimised access to data.
- **Transparency**: the data, system and AI business models should be transparent. Traceability mechanisms can help achieving this. Moreover, AI systems and their decisions should be explained in a manner adapted to the stakeholder concerned. Humans need to be aware that they are interacting with an AI system, and must be informed of the system's capabilities and limitations.
- **Diversity, non-discrimination and fairness**: Unfair bias must be avoided, as it could have multiple negative implications, from the marginalisation of vulnerable groups, to the exacerbation of prejudice and discrimination. Fostering diversity, AI systems should be accessible to all, regardless of any disability, and involve relevant stakeholders throughout their entire life circle.
- **Societal and environmental well-being**: AI systems should benefit all human beings, including future generations. It must hence be ensured that they are sustainable and environmentally friendly. Moreover, they should take into account the environment, including other living beings, and their social and societal impact should be carefully considered.
- **Accountability**: Mechanisms should be put in place to ensure responsibility and accountability for AI systems and their outcomes. Auditability, which enables the assessment of algorithms, data and design processes plays a key role therein, especially in critical applications. Moreover, adequate and accessible redress should be ensured.

According to the Guidelines, trustworthy AI should also be:

(1) **lawful** - respecting all applicable laws and regulations

(2) **ethica**l - respecting ethical principles and values

(3) **robust** - both from a technical perspective while taking into account its social environment

In 2021, the EU Commission proposed a Regulation on Artificial Intelligence, which is the first comprehensive regulation of AI in the world. The Regulation classifies AI systems into four risk categories: unacceptable risk, high risk, limited risk, and minimal risk.

Unacceptable risk AI systems are those that pose a serious threat to fundamental rights or safety, such as AI systems that could be used to manipulate people or create social unrest. These systems are prohibited from being developed or placed on the market in the EU.

High risk AI systems are those that pose a significant risk to fundamental rights or safety, such as AI systems used in medical applications or self-driving cars. These systems must comply with a number of strict requirements before they can be placed on the market, including undergoing a conformity assessment by a notified body.

Limited risk AI systems are those that pose a lower risk, such as AI systems used in chatbots or product recommendation systems. These systems are subject to less stringent requirements, but they must still comply with certain basic requirements, such as providing transparency to users about how they work and why they make the decisions they do.

Minimal risk AI systems are those that pose no significant risk, such as AI systems used in video games or spam filters. These systems are not subject to any specific requirements under the Regulation.

The EU AI Regulation is currently under development, but it is expected to be finalised and come into effect in 2023. Once it is in effect, it will be the most comprehensive regulation of AI in the world.

In addition to the AI Regulation, the EU has also issued a number of other guidelines and regulations that are relevant to AI, such as the General Data Protection Regulation (GDPR) and the Digital Services Act (DSA). The GDPR sets out a number of requirements for the collection and use of personal data, including data that is used to train and operate AI systems. The DSA sets out a number of requirements for online platforms and services, including requirements related to transparency, accountability, and risk management.

The EU's guidelines and regulations for AI are designed to ensure that AI is developed and used in a safe, responsible, and ethical manner. The EU's approach to AI regulation is based on the following principles:

- Human-centric AI: AI systems should be developed and used in a way that respects human rights and fundamental values.
- Trustworthy AI:AI systems should be transparent, accountable, and robust.
- Inclusive AI: AI systems should benefit all members of society and avoid discrimination.
- Sustainable AI: AI systems should be developed and used in a way that is environmentally friendly and sustainable.

The EU's guidelines and regulations for AI are still under development, but they are already having a significant impact on the global AI landscape. Many other countries are looking to the EU for guidance on how to regulate AI in a responsible and ethical manner.

The proposal for the AI Act [10] defines AI systems as high risk in article 6(1, 2):

'Article 6 - Classification rules for high-risk AI systems

1. Irrespective of whether an AI system is placed on the market or put into service independently from the products referred to in points (a) and (b), that AI system shall be considered high-risk where both of the following conditions are fulfilled:

(a) the AI system is intended to be used as a safety component of a product, or is itself a product, covered by the Union harmonisation legislation listed in Annex II;

(b) the product whose safety component is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment with a view to the placing on the market or putting into service of that product pursuant to the Union harmonisation legislation listed in Annex II.

2. In addition to the high-risk AI systems referred to in paragraph 1, AI systems referred to in Annex III shall also be considered high-risk.',

and Annex III [11], Annexx II, (1) reads:

'High-risk AI systems pursuant to Article 6(2) are the AI systems listed in any of the following

areas:

1. Biometric identification and categorisation of natural persons:

(a) AI systems intended to be used for the 'real-time' and 'post' remote biometric

identification of natural persons;

Therefore, the TeleRehaB DSS system should be considered as High Risk and as such implement measures that mitigate those risks and comply to the proposed regulation depicted in chapter 3 of the AI Act [10]

4.1 Mitigating Risks and Implementing Measures

Mitigating risks associated with high-risk AI systems requires a comprehensive approach that encompasses technical, ethical, and organisational measures. Here's an overview of key measures to consider:

Technical Measures:

a. **Data Governance**: Implement robust data governance practices to ensure data quality, relevance, and representativeness. Employ data cleansing techniques to address biases and anomalies in training data.

b. **Model Robustness**: Design AI models to be robust against adversarial attacks, noise, and unexpected inputs. Employ techniques like differential privacy and adversarial training to enhance model resilience.

c. **Explainability and Transparency**: Develop AI models that are explainable and transparent, allowing for understanding of their decision-making processes. Utilise techniques like explainable AI (XAI) to provide insights into model behaviour.

d. **Security and Privacy**: Implement stringent security measures to protect sensitive data and prevent unauthorised access. Employ encryption, access control mechanisms, and intrusion detection systems.

Ethical Measures:

a. **Bias Mitigation**: Identify and address potential biases in AI systems, particularly those that could lead to unfair or discriminatory outcomes. Employ bias detection tools and fairness-aware training techniques.

b. **Human Oversight**: Establish clear lines of human oversight and control for AI systems, ensuring that humans retain ultimate responsibility for critical decisions.

c. **Accountability**: Implement clear accountability mechanisms to identify and address potential harms caused by AI systems. Establish transparent reporting processes and accountability frameworks.

Organisational Measures:

a. **Risk Assessment**: Conduct thorough risk assessments to identify, prioritise, and address potential risks associated with AI systems. Employ risk management frameworks and methodologies.

b. **Governance and Compliance**: Establish clear governance structures and compliance mechanisms to ensure adherence to ethical principles, regulatory requirements, and industry standards.

c. **Stakeholder Engagement**: Engage with stakeholders, including users, experts, and policymakers, to gather feedback, address concerns, and build trust in AI systems.

d. **Training and Education**: Provide training and education to employees on AI ethics, responsible AI practices, and risk management techniques to foster a culture of responsible AI development and deployment.

By implementing these measures, organisations can effectively mitigate the risks associated with high-risk AI systems, ensuring their responsible development, deployment, and use.

Initiatives and more information on the above have been elaborated in the reports:

(a) TeleRehaBDSS_WP9_DEL_D9.3_AI Requirement No 3, [12] and

(b) TeleRehaBDSS_WP9_DEL_D9.4_AI Requirement No 4, [13].

5 Data Transfers

5.1 General Requirements

In order to justify that a transfer of personal data from the EU to a non-EU country or international organisation is in accordance with Chapter V of the General Data Protection Regulation 2016/679 (GDPR), [14] the following must be demonstrated:

- To ensure that personal data is adequately protected, it's important to first check if the recipient country or organisation is on the European Commission's list of countries with an adequacy decision. If the recipient country is not on the list, it's necessary to implement other safeguards such as standard contractual clauses or binding corporate rules. These additional measures will ensure that personal data is protected even when It's transferred to countries that don't have an adequate level of protection.
- The transfer is necessary for one of the specific purposes listed in Article 49 of the GDPR [14]. These purposes include:
  - ✓ The performance of a contract between the data subject and the controller or the taking of steps at the request of the data subject prior to entering into a contract.
  - ✓ The conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person.
  - ✓ For compelling legitimate interests pursued by the controller or a third party, 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.
- To ensure the safety and privacy of personal data, it is crucial to have appropriate safeguards in place. Such safeguards should include a thorough verification process to ensure that the recipient country or organisation has adequate technical and organisational measures in place to protect the personal data from unauthorised access, usage, disclosure, alteration, or destruction.

  This verification process should include a comprehensive evaluation of the security measures employed by the recipient organisation. This includes assessing the security protocols, encryption techniques, access controls, and any other security measures implemented to prevent data breaches. Additionally, it is important to verify that the recipient organisation complies with all applicable data protection laws and regulations.

  By implementing such safeguards, we can ensure that personal data remains secure and confidential, and that individuals can trust that their personal information is being handled with the utmost care and responsibility. The justification for the transfer should be documented and submitted to the relevant data protection authority (DPA) upon request.

Furthermore, as already mentioned, the transfers of personal data from a non-EU country to the EU, should comply with the laws of the country in which the data was collected.

5.2 Stage A | Processing Retrospective Data, as Test Data, before Clinical Trials (during the project)

The TeleRehaB DSS project prior to the clinical study initiation, will use retrospective data coming from other research studies as test data for the main system. Such data will be strictly anonymised and therefore these are not considered personal data. In this case and for this purpose a data sharing agreement has been composed. Anonymised or Non-personal data are any data that cannot be used to directly identify an individual.

Furthermore, anonymised data are not considered personal data, therefore there is no need to comply with the GDPR framework.

A data sharing agreement (DSA) is a legal document that establishes the terms and conditions for sharing data between two or more parties. Primarily used in business-to-business (B2B) relationships, DSAs are also employed in various other contexts such as research collaborations or government partnerships. By outlining the responsibilities and obligations of each party, DSAs ensure that data is shared in a responsible and ethical manner. Additionally, DSAs help safeguard the privacy of individuals as they specify how personal data will be collected, used, and disclosed. These agreements are crucial in regulating data sharing practices and promoting transparency and accountability.

DSAs can be used to share both personal data and non-personal data. However, it is important to note that DSAs must comply with all applicable data protection laws and regulations.

Here are some of the key elements that should be included in a DSA:

- The purpose of the data sharing
- The types of data that will be shared
- The parties who will be sharing the data
- The security measures that will be taken to protect the data
- The retention period for the data
- The process for resolving disputes

It is important to have a DSA in place whenever you are sharing data with another party. This will help to ensure that the data is shared in a compliant and responsible manner.

DSAs are an important tool for ensuring that data is shared in a responsible and ethical manner. They can also help to protect the privacy of individuals by specifying how personal data will be collected, used, and disclosed.

The Template of the Data Sharing Agreement document that has been used is attached in chapter 14, 'Appendix C | Data Sharing Agreement Template' (page 48) and this will be signed off by:

- The consortium partners that will provide and share the data, and
- The consortium partners that will process the data.

5.3 Stage B | Data Storage, Transfers and Processing of Prospective Data (Clinical Study, During the Project)

The clinical study will run for 14 months, from month 19 to month 32, with the aim of validating the AI-based TeleRehaB DSS. The study will compare the benefits and cost-effectiveness of the DSS with the current standard of care. The University of Ioannina (UOI) will act as the technical coordinator, overseeing all technical matters related to the platform's use and its components [2]. The project partners are listed in chapter 16, 'Appendix B | Joint Data Controllers and Data Processors Agreements' (page50). As expected, organisations (3), (7), (11), (12), (13) are expected to carry out the clinical study [2]. Most of the participants are based in EU. The exceptions are the following:

- **CHULALONGKORN UNIVERSITY (KCMH)**, (3)
- **UNIVERSITY COLLEGE LONDON (UCL)**, PIC 999975620, established in Gower Street, London WC1E 6BT, England, United Kingdom, (13)
- **GUYS AND ST THOMAS' NHS FOUNDATION TRUST (HIN)**, PIC992185938 in St Thomas' Hospital, Westminster Bridge Rd, London SE1 7EH, United Kingdom. (14)

As a result, for the above-mentioned cases, safeguards are necessary as GDPR requirements should apply.

The data centre that will host the data is located in Athens, Greece, at the premises of the Biomedical Eng. Lab. of ICCS, which is located at the Campus of the National Technical University of Athens, Central Computer Building, 1st floor.

Furthermore, it is important to note that based on the Clinical Study Plan, (a) no personal data will be collected within the study database or transferred outside of the study and partners, and (b) pseudonymised data (including specialist data such as information about the subject's health) will be collected and may be transferred to the research group centres in Spain, Germany, and Greece (within the EEA) [2].

The personal data collected during the study is expected to be securely stored in each clinical site according to country-specific legislation and within encrypted online platforms such as e.g. the UK-based UCL Data Safe Haven [15] for UCL's data. The data will be kept for the duration of the study. After the study ends, the data will be anonymised and shared with consortium members within the EU (EEA) for analysis and processing purposes using an encrypted cloud storage platform. The data that will be collected has been described above and will be stored within the platform databases [2].

According to the UCL Records Retention Policy, UCL, who is the sponsor, will keep the research data collected during the study for 20 years after the research study concludes. After this period, the data will be securely destroyed [2].

Similar procedures are expected to be applied in the remaining clinical partners' settings.

5.4 Stage C | Data Storage and Transfers of Data (After the Project)

Following the project, the datasets will be transferred to Zenodo Repository [16], a repository created and developed by researchers, to ensure that everyone can join in Open Science [17].

All data transfers will be conducted using SFTPs, which is a secure and encrypted method to transfer files with Anonymised datasets.

5.5 Standard Contractual Clauses

The Standard Contractual Clauses (SCCs) are pre-approved contractual templates developed by the European Commission to facilitate lawful transfers of personal data from the European Economic Area (EEA) to third countries that do not have an adequacy decision. SCCs are a type of data transfer mechanism under the General Data Protection Regulation (GDPR) and serve as a safeguard to ensure that personal data transferred outside the EEA are protected in accordance with GDPR standards.

The standard contractual clauses (see chapter 15, Appendix D | Standard Contractual Clauses, page 49) are analysed further in the report that describes the security, privacy and GDPR compliance for Data Transfers within the project [18]. The document covers the following:

(a) the transfers of personal data from the EU to a non-EU country or international organisation, are in accordance with Chapter V of the General Data Protection Regulation 2016/679, and

(b) the transfers of personal data from a non-EU country to the EU, comply with the laws of the country in which the data was collected.

5.6 Security and Privacy Technical Measures

The same document mentioned above also elaborates in measures for security, privacy and GDPR compliance for Data Transfers within the project [18], covering the following:

- **Retrospective Data (During the Project)**
  - Anonymisation

- **Prospective Data (During the Project)**
  - Other Measures
  - Pseudonymisation
  - Physical Security
  - Incorporation of Advanced Data Encryption

- **Rationale Behind Selecting the Advanced Encryption**
  - Standard (AES)
  - Key Management Protocols within TeleRehaB
  - Operational Implications of AES Integration

- **Prospective Data (After the Project)**
  - Data Security

6 General Data Protection Regulation Compliance

As the TeleRehaB DSS project will process personal data, the General Data Protection Regulation (GDPR) [4] is highly regarded, and ethical, legal, and privacy concerns will be addressed accordingly. The TeleRehaB DSS management structure will consist of several Data Controllers, Data Processors and the DPO, a person responsible for monitoring Data Protection principles, with significant expertise in GDPR. The designated Data Protection Officer (DPO) prof. Christoph Maurer (UKLFR) will oversee data protection strategy and implementation to ensure compliance with GDPR requirements and also will work closely with the local Data Protection Officers and Data Controllers of the beneficiary organisations.

The consortium partners will make arrangements and take appropriate actions and apply organisational and technical measures to protect the confidentiality of the clinical study participants and their data, and all personal information collected will be considered private information. It will be dealt with in a manner that does not compromise the personal dignity of the participant or infringe upon their right to privacy. Before obtaining consent, the researchers will inform prospective participants of any potential risks that might mean that the confidentiality or anonymity of personal information may not be guaranteed. They will also inform them of the purpose for which personal information will be used.

Regarding the rights to privacy and to the protection of personal data, TeleRehaB DSS will adhere to the provisions of:

- The EU Charter on Fundamental Rights (art. 7 and 8), [19];
- The European Convention for the Protection of Human Rights and Fundamental Freedoms (art. 8), [20];
- The IEEE journal article, "Toward privacy-assured and searchable cloud data storage services," Network, IEEE, vol. 27, no. 4, pp. 56–62, 2013, , [21];
- The Convention 108 and Protocols for the Protection of Individuals concerning Automatic Processing of Personal Data (2018) [22]
- Regulation 2016/67 EC (General Data Protection Regulation) [4]

TeleRehaB DSS is aware that it is likely that some standards, in particular, but not exclusively, the European data protection framework, may evolve within the lifetime of the project. The consortium is committed to monitoring and taking into account such evolutions as well as issues emerging from different enforcement regulations.

There are some key principles that need to be followed when processing personal data. These include:

- Only processing personal data for specific and clear purposes;
- Obtaining informed consent from the individuals whose data is being processed, including providing details about the purpose of the research, who is funding and organising it, and what will happen to the results;
- Ensuring that the processing of personal data is done fairly and lawfully, with a clear legal basis for doing so;
- Minimising the amount of data that is collected;
- Only collecting data that is relevant and necessary for the purpose at hand;
- Ensuring that personal data is accurate and up-to-date;
- Only retaining personal data for as long as necessary;
- Respecting the rights of individuals whose data is being processed;
- Implementing technical and organisational measures to ensure the security of personal data;
- Ensuring that personal data is protected when transferred to third countries outside of the EU.

Participants who will participate in the clinical study and have their data collected and processed will be fully informed about the data collection, storage, and protection processes by each clinical partner responsible for the activity. They will also be informed about the study's purpose and their rights to access, modify, and erase their personal data, as well as how to exercise these rights.

The data collected from the participants will only be used for the purposes that are explicitly required for the smooth functioning of the TeleRehaB DSS activity. However, if the data can be utilised for future analysis, the participants will be asked for specific informed consent for the same. The data will only be retained as long as it is required as per the relevant regulations.

It is crucial to implement specific measures to safeguard any collected data, whether it be personal or sensitive. Furthermore, it is necessary to ensure the secure destruction or deletion of such data once the TeleRehaB DSS's purpose is fulfilled, or when requested by any participant or volunteer. The conservation and destruction of data, both physical and digital, must adhere to the best practices so that any destroyed data cannot be retrieved.

6.1 Mitigating Risks and Implementing Measures

There are a number of measures that TeleRehaB DSS should take to comply with the GDPR. These include:

- **Appointing a data protection officer (DPO)**: A DPO is responsible for overseeing an organisation's compliance with the GDPR. They must have the necessary expertise and resources to carry out their role effectively. The role has been already assigned to prof. Christoph Maurer (UKLFR).

- **Conducting a data protection impact assessment (DPIA)**: A DPIA is a process that helps organisations identify and assess the risks to the rights and freedoms of individuals posed by their processing of personal data. It must be carried out for any processing that is likely to result in a high risk to individuals' rights and freedoms.
- **Implementing appropriate technical and organisational measures to protect personal data**: These measures must be proportionate to the risks posed by the processing of personal data. They may include measures such as encryption, access controls, and data minimisation.
- **Providing individuals with information about how their personal data is being processed**: This information must be clear, concise, and easily understandable. It must also be provided in a timely manner.
- **Obtaining consent from individuals before processing their personal data**: Consent must be freely given, specific, informed, and unambiguous. It must also be easy to withdraw.
- **Giving individuals the right to access, rectify, erase, restrict, and object to the processing of their personal data**: These rights are known as the "right to access," "right to rectification," "right to erasure," "right to restriction," and "right to object."
- **Notifying the supervisory authority of data breaches**: A data breach is a security breach that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Organisations must notify the supervisory authority of any data breaches within 72 hours of becoming aware of them.

6.2 Data Protection Impact Assessment (DPIA)

A Data Protection Impact Assessment (DPIA) is a process that helps organisations identify and mitigate data protection risks. It is a systematic and comprehensive analysis of the processing of personal data, which takes into account the nature, scope, context, and purposes of the processing. The DPIA helps organisations to:

- Identify the risks to the rights and freedoms of individuals posed by the processing of personal data.
- Implement appropriate safeguards to mitigate those risks.
- Demonstrate compliance with the General Data Protection Regulation (GDPR) and other applicable data protection laws.

In TeleRehaB DSS, a DPIA is required as processing may result in a high risk to the rights and freedoms of individuals. This includes processing that:

- Involves the use of new technologies (AI).
- Processes sensitive personal data (biometric and genetic data).

- Processes personal data on a large scale (not during the project but eventually when the DSS system might come into production).
- Systematically monitors individuals.

The DPIA should be carried out before the processing begins, and it should be reviewed and updated regularly. The DPIA should be documented and made available to the supervisory authority on request.

The DPIA methodology is a structured approach to identifying and assessing the risks to the rights and freedoms of individuals posed by the processing of personal data. It is a flexible and adaptable process that can be tailored to the specific needs of the organisation and the processing activity.

Key steps in the DPIA methodology include:

(1) **Scoping**: The first step is to identify the processing activities that will be covered by the DPIA. This may involve reviewing the organisation's data protection policies and procedures, as well as any new data processing activities that are being planned.

(2) **Describing the processing**: Once the processing activities have been identified, they need to be described in detail. This includes providing information about the types of personal data that will be processed, the purposes of the processing, the categories of data subjects, and the recipients of the personal data.

(3) **Identifying risks**: The next step is to identify the potential risks to the rights and freedoms of individuals posed by the processing. This involves considering the nature of the personal data, the purposes of the processing, and the context in which the processing will take place.

(4) **Evaluating risks**: Once the risks have been identified, they need to be evaluated in terms of their likelihood and severity. This will help to determine whether the processing is likely to result in a high risk to the rights and freedoms of individuals.

(5) **Implementing safeguards**: If the processing is likely to result in a high risk, then appropriate safeguards must be implemented to mitigate the risks. This may involve implementing technical or organisational measures, such as data encryption, access controls, or data minimisation techniques.

(6) **Documenting the DPIA**: The DPIA should be documented and made available to the supervisory authority on request. The documentation should include all of the information that was considered in the DPIA process, as well as the conclusions that were reached.

(7) **Reviewing the DPIA**: The DPIA should be reviewed regularly and updated as needed. This is particularly important if there are any changes to the processing activities or the risks associated with the processing.

The DPIA methodology is an important tool for organisations that process personal data. It helps organisations to comply with the GDPR and other applicable data protection laws, and it helps to protect the rights and freedoms of individuals.

6.3 Data Security and Privacy Breach Management

Data security and privacy breach management are essential aspects of compliance with the General Data Protection Regulation (GDPR). The GDPR establishes a robust framework for safeguarding personal data and requires organisations to implement appropriate measures to protect the rights and freedoms of individuals.

The GDPR mandates that organisations implement technical and organisational measures to ensure an appropriate level of security for personal data, considering the nature, scope, context, and purposes of the processing and the risks posed by the processing. These measures should address the following principles:

- **Confidentiality**: Ensuring that personal data is only accessible to authorised individuals or entities.
- **Integrity**: Maintaining the accuracy and completeness of personal data.
- **Availability**: Ensuring that personal data is accessible to authorised individuals or entities when needed.

Specific security measures that organisations may implement include:

- **Pseudonymisation**: Replacing personal data with identifiers that cannot be directly linked to a specific individual.
- **Encryption**: Converting personal data into an unreadable format to protect against unauthorised access.
- **Access controls**: Implementing mechanisms to restrict access to personal data based on authorised roles and permissions.
- **Data minimisation**: Collecting and processing only the personal data that is necessary for the specified purposes.
- **Regular security assessments**: Identifying and addressing potential vulnerabilities and security risks.

The GDPR also mandates that organisations notify the supervisory authority within 72 hours after becoming aware of a personal data breach that poses a risk to the rights and freedoms of individuals. The notification should include:

- Description of the nature of the breach.
- Categories and approximate number of affected individuals.
- Categories and approximate number of personal data records affected.
- Contact details of the data protection officer or other point of contact.
- Description of the likely consequences of the breach.
- Measures taken or proposed to address the breach.

If the breach poses a high risk to individuals, the controller must also notify the affected individuals without undue delay. The notification should provide clear and concise information about the breach, the potential consequences, and the recommended actions for individuals to protect their rights.

TeleRehaB DSS will adopt a proactive approach to data security and privacy breach management under the GDPR by implementing the following measures:

- **Data Protection Impact Assessments**: Conducting DPIAs to assess the risks posed by processing activities and implement appropriate safeguards.
- **Employee Training and Awareness**: Providing regular training to employees on data security practices, GDPR requirements, and incident reporting procedures.
- **Third-Party Vendor Management**: Carefully selecting and managing third-party vendors that handle personal data to ensure compliance with GDPR requirements. The third parties's will be further exploited along with their security and privacy compliance.

By implementing these measures, organisations can effectively protect personal data, comply with GDPR requirements, and minimise the risk of data breaches and associated consequences.

7 CE Mark

The CE Mark is a mandatory marking that manufacturers must affix to certain products to indicate that the device meets the EU's General Safety and Performance Requirements (GSPRs), which are designed to ensure that medical devices are safe and effective.

There are four main classes of medical devices, each with different conformity assessment requirements:

- Class I: These are the lowest-risk devices, such as bandages and non-invasive thermometers. Class I devices do not require conformity assessment by a notified body, but manufacturers must still prepare technical documentation and declare compliance with the GSPRs.
- Class II: These are devices with a moderate risk, such as surgical instruments and dental implants. Class IIa devices can be self-certified by the manufacturer, while Class IIb devices require involvement from a notified body.
- Class III: These are the highest-risk devices, such as life-supporting implants and implantable heart valves. Class III devices must undergo a full conformity assessment by a notified body.
- Custom-made devices: These are devices that are specifically designed and manufactured for a particular patient. Custom-made devices are not subject to the same conformity assessment requirements as other medical devices, but manufacturers must still ensure that they comply with the GSPRs.

While the TeleRehaB DSS could be deemed a medical device, it's worth noting that the certification process is not part of this project's scope. The TeleRehaB DSS system will be developed solely for research purposes within the confines of this project and will not be released into the market. Therefore, there will be no consideration of CE Mark requirements.

Nevertheless, as the system already uses other devices, there is a list of CE Marked devices that were also used in HOLOBalance system which are listed in [23]

8 Gender Equality

The European Commission (EC) confirms its commitment towards gender equality in research and innovation, adopting specific measures within the Framework Programme 7, Horizon 2020 and lately Horizon Europe. The European Research Area (ERA) [24] Priority 4 focuses on gender equality and gender mainstreaming in R&I promoting:

- gender equality in careers at all levels,
- gender equality in decision-making,
- integration of the gender dimension into R&I content.

Horizon 2020 programme played a central role in advancing Gender Equality (GE) in Research & Innovation (R&I) policies, setting it as a general principle in Article 16 and adding it as one of the Responsible Research and Innovation (RRI) components (art. 14(I)) [25]. The Gender Equality Strategy 2020 – 2025 [26] underlines 6 main objectives to be tackled before 2025:

- being free from violence and stereotypes,
- thriving in a gender-equal economy,
- leading equally throughout society,
- gender mainstreaming and an intersectional perspective in EU policies,
- funding actions to make progress in gender equality in the EU,
- addressing gender equality and women's empowerment across the world.

Besides these within the Horizon Europe programme, new provisions have been announced, at different levels:

- Having a Gender Equality Plan (GEP) in place became since 2023 an eligibility criterion to get access to Horizon Europe [27]funding for public bodies, research organisations and higher education institutions from EU countries and associated countries. This requirement foresees five recommended thematic areas to be covered by the Plans, namely:

  - Work-life balance and organisational culture.
  - Gender balance in leadership and decision-making.
  - Gender equality in recruitment and career progression.
  - Integration of the gender dimension into research and teaching content.
  - Measures against gender-based violence including sexual harassment.

- The integration of the gender dimension into research and innovation content is a requirement by default.
- Attention will be paid to ensure gender balance in evaluation panels and in other relevant advisory bodies. Gender balance among researchers involved in projects will be strongly encouraged and will be considered for equally ranked proposals.
- Flagship measures and activities promoting gender equality under the European Innovation Council (EIC), including a target of 40% women-led companies invited to pitch their projects, a target of 50% women among members of advisory

structures, a prize for women innovators and a dedicated initiative to support women-led start-ups.

Following this paradigm and adapting the scope of a GEP to address a Horizon Europe project, *TeleRehaB DSS* having been designed following a gender sensitive approach, develops and adopts a project GEP, translating the consortium's commitment to the promotion of inclusive gender equality into an explicit project goal. The project's GEP entails a comprehensive gender strategy tailored to the needs of the project and thus increasing its societal relevance and acceptance [28] and fostering the gendered innovation process [29].

The project's GEP, found publicly on the project's website, covers measures on the 5 key thematic areas described below:

- Work-life balance
- Gender sensitiveness communication
- Gender balance in leadership and decision making
- Integration of sex/gender dimension in research content
- Measures against gender-based violence and sexual harassment.

Relevant data at consortium level will be gathered every year and respective measures will be implemented and evaluated according to the plan.

With regards, to sex and gender dimension specifically into research content, all project activities are described at the project's GEP. In addition, the project's methodological approach reflects on the 2 basic questions below for mainstreaming the gender dimension in the research process: how gender differences and inequalities will affect project results and outcomes and how the project will differentially affect men's and women's health, opportunities, and potential intervention status.

The project collects primary and secondary gender-focused data from official and non-official sources and databases. For quantitative data our research uses demographic and health surveys, along with data provided by our partners from previous relevant research and studies.

Intersectional data are being gathered regarding all aspects of social, economic and health life considering the individual level, the household, the community, health facilities and broadly the health system such as gender and sex, geographical location etc. The gender analysis provided by TeleRehaB DSS will use a combination of quantitative and qualitative methods in order to fully assess the comparative and relational aspect of gender. This combined approach will provide information on specific and measurable factors of gender that identify gaps and disparities (quantitative data) and will further study the patterns of inequities and correlations.

Last but not least, with regards to the participants of the clinical trials, equal participation of men and women will be encouraged.

9 Personal Data Processing Agreements

9.1 The Defined Purpose of the Data Processing

As TeleRehaB DSS will process personal data collected by subjects, GDPR will apply. Based on the [30], the purpose of the data processing for the data controllers and data processors on behalf of the data controllers is:

"Develop an AI-based DSS, building upon/expanding on previously developed platforms, tools, obtained results and know-how (i.e. HOLOBALANCE, SMART BEAR projects), to support effective and affordable treatment for patients at risk of fall for both in clinic and remote home-based care."

To achieve the above, a digital workspace/repository FAIR by design, will be developed, allowing consortium partners to store and share their datasets (data from the TeleRehaB project) in a centralised and secure environment, facilitating collaboration and further research development through synergies. The ultimate objective is to utilise the workspace/repository, based on AI and distributed Machine Learning technologies so that "… *DSS will be able to cover the entire pathway:*

i. *enhancing initial clinical precision treatment and patient selection for each intervention strand,*
ii. *providing comprehensive evidence-based interventions distinguishing between the effects of different factors (e.g. medical history, diagnosis, physical activity, medication, side effects, frailty, cognition),*
iii. *personalising rehabilitation interventions in terms of type and intensity of the intervention, technology used projection of compliance and expected outcomes, taking into account each patient's need and expected benefits along with available resources. TeleRehaB DSS will offer a support for challenging decision making for patients at risk of fall in many layers: appropriate intervention choice; exercise type & progression (daily/weekly); integrated communication package (for professionals, patients & carers).*
iv. *target the relevant public health sector, providing valuable information at public health policy level, in terms of cost-effectiveness (i.e. in terms of human resources and equipment needed), retro and prospectively validated with clinical study, providing required evidence to ensure clinical personnel take up and incorporate AI solutions in clinical guidelines and everyday practice."*

During the 4-year project lifetime (Dec 2022 – Nov 2025).

9.2 Description of the Data Processing

As already mentioned I chapter 5.3, Stage B | Data Storage, Transfers and Processing of Prospective Data (Clinical Study, During the Project), page 22, The AI-based TeleRehaB DSS will undergo a 14-month clinical study from month 19 to month 32 to validate its benefits and cost-effectiveness compared to the current standard-of-care. The University of Ioannina (UOI) will act as the technical coordinator, overseeing all technical matters related to the platform's use and its components [23]. The project partners are listed in chapter 0, '

The following documents are attached:

COMMISSION IMPLEMENTING DECISION on standard contractual clauses between controllers and processors under Article 28 (7) of Regulation (EU) 2016/679 and Article 29 (7) of Regulation (EU) 2018/1725

EN Standard Contractual Clauses

Standard contractual clauses for controllers and processors in the EU/EEA

EN Annex Standard Contractual Clauses

Appendix E | List of Participants (Organisations)' (page 49).

9.3 Joint Data Controllers Agreement

GDPR [4]defines the role of the "Data Controller" as an entity that alone or jointly with others determines the purposes and means of the Processing of Personal Data. Based on [23], the TeleRehaB DSS project, the following partners will collect the data and 'lead' the study assuming the role of the Data Controllers:

- **CHULALONGKORN UNIVERSITY (KCMH)**, PIC 999869211, established in PHYATHAI ROAD 254 PATHUMWAN, BANGKOK 10330, Thailand (3),
- **ETHNIKO KAI KAPODISTRIAKO PANEPISTIMIO ATHINON (NKUA)**, PIC 999643007, established in 6 CHRISTOU LADA STR, ATHINA 10561, Greece (7),

- **UNIVERSITAETSKLINIKUM FREIBURG (UKLFR)**, PIC 999881918, established in HUGSTETTER STRASSE 49, FREIBURG 79106, Germany (11),
- **DRES RIPOLL Y DE PRADO SLP (RYDP)**, PIC 889251769, established in CALLE MIGUEL HERNANDEZ 12, MURCIA 30011, Spain (12),
- **UNIVERSITY COLLEGE LONDON (UCL)**, PIC 999975620, established in Gower Street, London WC1E 6BT, England, United Kingdom (13).

Prior to collecting personal data, the data controllers will agree to a joint controller agreement that outlines their respective responsibilities for ensuring lawful processing of the data and compliance with GDPR regulations. This includes the obligation to respect the rights of the data subjects, as well as providing the information referred to in articles 13 and 14 of the GDPR [4].

A template of the agreement is attached in chapter 12, Appendix A | (page 45)

9.4 Joint Data Controllers and Data Processors Agreement

The GDPR [4]defines the role of a "Data Processor", as an entity that Processes Personal Data on behalf of one or more of the Data Controllers.

"*Process*" or "*Processing*" shall mean any operation performed on Personal Data, whether or not by automated means, such as collection, organisation, structuring, storage, use, dissemination, or otherwise making available, erasure or destruction.

In this phase 2 of the TELEREHAB DSS project, aiming at performing the research using the data collected in the pilot trial, the Data Processors are the following:

- **INSTITUTE OF COMMUNICATION AND COMPUTER SYSTEMS (ICCS)**, PIC 999654356, established in Patission Str. 42, ATHINA 10682, Greece,
- **PANEPISTIMIO IOANNINON (UOI)**, PIC 999852818, established in PANEPISTEMIOYPOLE PANEPISTEMIO IOANNINON, IOANNINA 45110, Greece,
- **VILABS OE (VILABS)**, PIC 955444375, established in THERMOKOITIDA TECHNOPOLIS VEPE TECHNOPOLI PYLAIA, THESSALONIKI 55535, Greece,
- **ISTRAZIVACKO RAZVOJNI CENTAR ZA BIOINZENJERING BIOIRC DOO (BIOIRC)**, PIC 997234012, established in PRVOSLAVA STOJANOVICA STREET 6, KRAGUJEVAC 34000, Serbia,
- **ACTIVE AGEING ASSOCIATION (ACT)**, PIC 893713187, established in RONDA AUGUSTE Y LOUIS LUMIERE Nº 23 - NAVE 13, PATERNA 46980, Spain (6)
- **ARINIMI ON BRIDG OU (BRD)**, PIC 889383495, established in HARJU MAAKOND LASNAMAE LINNAOSA LOOTSA TN 5-11, TALLIN 11415, Estonia, 1
- **UNINOVA-INSTITUTO DE DESENVOLVIMENTO DE NOVAS TECNOLOGIAS ASSOCIACAO (NOVA)**, PIC 999633889, established in CAMPUS DA CAPARICA QUINTA DA TORRE, CAPARICA 2829-516, Portugal,
- **QUANTITAS SRL (QUAN)**, PIC 915312856, established in VIA CARLO REZZONICO 6, PADOVA 35131, Italy,

- **GUYS AND ST THOMAS' NHS FOUNDATIONTRUST (HIN)**, PIC992185938 in St Thomas' Hospital, Westminster Bridge Rd, London SE1 7EH, United Kingdom.

The data processing agreement governs the processing of personal data by the data processors on behalf of the data controller. This includes the collection, registration, compilation, storage, disclosure, or combination of these activities, all of which are related to the use and processing of data in Project TeleRehaB DSS.

Before the collection of personal data, the data processors and data controller will sign a data processing agreement. This agreement is put in place to ensure that personal data is not processed illegally, wrongfully, or in a way that could lead to unauthorised access, alteration, erasure, damage, loss, or unavailability.

A template of the agreement is attached in chapter 13, Appendix B | Joint Data Controllers and Data Processors Agreement (page 47).

9.5 Sub-processors in Joint Data Controllers and Data Processors Agreement

"Sub-processor", shall mean any processor which a Data Processor engages to carry out specific Processing activities on behalf of any of the Data Controllers.

The data processor is obliged to enter into separate agreements with sub-processors that govern the sub- processor's processing of personal data in connection with the data processing agreement. Therefore, the data controller, before the data collection begins, will approve that the data processor contracts the following sub-processors to satisfy the relevant agreement. The template of the agreement is attached in chapter 13, Appendix B | Joint Data Controllers and Data Processors Agreement (page 47).

9.6 Data Security and Privacy Breach Notifications

As already mentioned, personal data breaches can be a result of various incidents, including unauthorised access or disclosure, loss, alteration, destruction, or any other form of security breach. For instance, someone may steal a computer or a USB memory stick containing sensitive information, unauthorised access to a system or network may occur through a cyber-attack, or malware infection, fire in the data centre, or sending information to the wrong recipient.

It is the responsibility of both the controller and processor of personal data [14] to implement and maintain adequate technical and organizational measures to safeguard personal data against unauthorized access and disclosure. This includes employing robust security protocols, such as encryption and access controls, as well as establishing clear policies and procedures for handling sensitive information. By taking these precautions, the controller can mitigate the risk of data breaches and uphold the privacy rights of individuals.

It is imperative for all data controllers to be proactive in anticipating and preparing for potential personal data breaches. This can be achieved by developing comprehensive guidelines that outline the necessary steps to take in the event of a breach, as well as establishing a well-defined plan of action to respond swiftly and effectively to any security incidents that may occur. By putting these measures in place, controllers can minimize the damage caused by breaches and safeguard the privacy and security of personal data.

When a personal data breach occurs, it can lead to a variety of negative consequences, including the loss of control over personal data, identity theft, fraud, damage to reputation, or loss of confidentiality of personal data. The level of risk associated with the breach will dictate the measures that the controller must take in response. For instance, the controller may need to document the personal data breach in detail, including any information about the nature and scope of the breach, the potential consequences, and the steps taken to mitigate the damage. Additionally, the controller may need to notify the supervisory authority, which is responsible for enforcing data protection laws and regulations. The notification should include all relevant information about the breach, including the data that has been affected, the cause of the breach, and the measures taken to prevent future breaches. Finally, the controller may also need to inform the data subjects, who are the individuals whose personal data has been compromised. This notification should be clear, concise,

There is also an obligation to document all personal data breaches, their effects and corrective actions taken, regardless of any measures required by the personal data breach. Failure to comply with the documentation or notification obligations constitutes a violation of the General Data Protection Regulation (GDPR) and may result in the sanctions specified therein.

The data controllers are responsible for compliance with Article 33 of the GDPR, that is, within 72 hours on notification of a personal data breach to the supervisory authority concerning the Personal Data they provide.

The data processors are responsible for compliance with Article 34 of the GDPR on communication of a personal data breach to the Data Subject concerning the Personal Data they provide.

After having become aware of a personal data breach, within 36 hours, a data controller must inform the other Data Controllers of the breach. The Parties should agree to provide reasonable assistance as is necessary to each other to facilitate the handling of any data breach in an expeditious and compliant manner.

10 Technical and Organisational Measures

10.1 Security and Privacy Technical Measures

Safeguarding, preserving confidentiality and upholding regulatory adherence concerning medical data throughout storage and transmission are pivotal facets of healthcare information administration. These elements were thoroughly considered in formulating a security and privacy strategy for the TeleRehaB DSS project. The subsequent measures have been instituted in pursuit of this objective:

- **Encryption in Transit:** Encryption during data transmission involves the application of cryptographic techniques to encode information, rendering it indecipherable to unauthorised entities while traversing networks or communication channels. This process ensures the confidentiality and integrity of sensitive data, including personal and medical information, by converting it into unreadable ciphertext that can only be deciphered with the corresponding decryption key. SSL (Secure Sockets Layer) encryption, a fundamental security protocol, creates a secure link between servers and clients, upholding data confidentiality, integrity and authentication on the internet. SSL certificates, acquired from trusted Certificate Authorities (CAs), not only establish trust and credibility for websites but also fulfil compliance requirements for data protection regulations such as GDPR. Implementing SSL/TLS (Transport Layer Security) and HTTPS protocols guarantees a secure, encrypted connection for data transmission, safeguarding it from unauthorised access and ensuring adherence to stringent security standards throughout the TeleRehaB DSS project.
- **Authentication, Authorisation and Access Controls:** The adopted authentication and authorisation framework within the TeleRehaB DSS project centres around the utilisation of JSON Web Tokens (JWTs), which serve a dual purpose in web applications, enabling both authentication and authorisation processes. In the context of authentication, subsequent to user credential submission, the server verifies and generates a JWT token encompassing pertinent user data, such as user ID, subsequently sent back to the client for storage, often within local storage or memory. For authorisation, these tokens can encapsulate user roles, permissions, or access control information. The server validates the token's integrity using a secret key, extracting and scrutinising encoded user roles or permissions to make informed decisions regarding user access to specific resources or functionalities. This implementation not only ensures a stateless architecture but also enhances security, enabling controlled access to platform modules exclusively for authenticated and authorised users. This approach safeguards medical data transfers solely for authenticated users and restricts access to diverse data sources based on the respective roles of users, including administrators, clinicians and technicians, within the TeleRehaB DSS project.
- **Encryption at Rest:** Encryption at rest involves the protection of data stored in databases or storage mediums while in an idle state, ensuring its confidentiality by rendering it incomprehensible to unauthorised entities who might gain access to the storage infrastructure. Employing cryptographic algorithms, this process transforms plaintext data into ciphertext using encryption keys, necessitating appropriate

decryption keys for authorised users or systems to revert the ciphertext to its original form. The primary objective is to maintain data confidentiality, mitigating potential risks arising from unauthorised access, theft or data breaches, by ensuring that encrypted data remains unreadable without the requisite decryption keys. Encryption at rest not only aligns with various data protection regulations but also fulfils compliance requirements, safeguarding sensitive information within the TeleRehaB DSS project. Adopting Database-Level Encryption for specific fields within the non-FHIR database, such as clinicians' and patients' personal identifiable information, including names, surnames, contact details and addresses, underscores the project's commitment to securing sensitive data, mitigating potential vulnerabilities and ensuring confidentiality even during periods of data dormancy or storage.

- **Medical Data Pseudonymisation:** Pseudonymisation stands as a widely embraced methodology in data management, serving to uphold the privacy of individuals within datasets by modifying personal information to prevent direct identification without supplementary data. The core objective of pseudonymisation is to mitigate potential risks associated with data breaches while allowing for legitimate use of data, such as research and analysis. Its essence lies in striking a balance between safeguarding individual privacy and preserving data utility, yet it's crucial to note that while pseudonymisation reduces the probability of re-identification, it does not guarantee absolute anonymity due to its reversible nature. Within the framework of the TeleRehaB DSS project, medical data will reside in a FHIR database following the Fast Healthcare Interoperability Resources standard. This involves the utilisation of two distinct patient identifiers: a FHIR ID linked to the medical data and an exposed ID used by other modules. Processes involving data entry by clinicians will associate information with the exposed patient's ID, which will be substituted by the FHIR ID through a pseudonymisation component before storage in the FHIR database. Conversely, data retrieval will initiate with a GET request using the exposed ID, converting to the FHIR ID for querying the database and subsequently reverting to the exposed ID to ensure return data accessibility to the experts' dashboard.

10.2 Summary Table of Measures

A summary table listing the measures mentioned in previous paragraphs has been created in chapter 12, Appendix A | Organisational & Technical Measures Summary Table, in page 45.

11 References

[1] TeleRehaB DSS, "TeleRehaB DSS | TeleRehaB Decision Support System (DSS) targets the promotion of AI adoption in everyday clinical practice for balance rehabilitation training.," 2023. [Online]. Available: https://telerehab-project.eu/.

[2] TeleRehaB DSS, "TeleRehaB DSS | D5.1 Study initiation package," TeleRehaB DSS Project, 2023b.

[3] The World Medical Association (WMA), "(WMA) Declaration of Helsinki, Ethical Principles for Medical Research involving Human Subjects," 6 9 2022. [Online]. Available: https://www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects/.

[4] The European Parliament and of the Council of the EU, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr 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 Da," 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj. [Accessed 04 2021].

[5] European Commission , Secretariat-General (European Commission), "Group of advisers on the ethical implications of biotechnology to the European Commission," EU Publications, 1995.

[6] The European Data Protection Supervisor (EDPS), "A Preliminary Opinion on data protection and scientific research," 6 1 2020. [Online]. Available: https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf.

[7] The European Parliament and of the Council of the EU, "Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC Text with EEA relevance," 2014. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014R0536.

[8] "Directive 2001/20/EC of the European parliament and of the Council, of 4 April 2001, on the approximation of the laws, regulations and administrative provisions of the Member States relating to the implementation of good clinical practice in the conduct o," 4 4 2001. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2001/20/2022-01-01.

[9] The High-Level Expert Group on AI (AI HLEG), "Ethics guidelines for trustworthy AI," 8 4 2019. [Online]. Available: file:///C:/Users/chris/Downloads/ai_hleg_ethics_guidelines_for_trustworthy_ai-en_87F84A41-A6E8-F38C-BFF661481B40077B_60419.pdf.

[10] The European Parliament and of the Council of the EU, "Proposal for a Regulation of the EU Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts," 21 4 2021. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206.

[11] The European Parliament and of the Council of the EU, "Anexxes to the Proposal for a Regulation of the EU Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts," 21 4 2021. [Online]. Available: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_2&format=PDF.

[12] TeleRehaB DSS, "TeleRehaB DSS | D9.3 AI Requirement No 3," TeleRehaB DSS Project, 2023d.

[13] TeleRehaB DSS, "TeleRehaB DSS | D9.4 AI Requirement No 4," TeleRehaB DSS Project, 2023e.

[14] The European Parliament and of the Council of the EU, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr 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 Da," 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj. [Accessed 04 2021].

[15] UCL, "UCL Data Safe Haven | Service providing a technical solution for storing, handling and analysing identifiable data.," 2023. [Online]. Available: https://www.ucl.ac.uk/isd/services/file-storage-sharing/data-safe-haven-dsh.

[16] TeleRehaB DSS, "TeleRehaB DSS | D1.1 Data Management Plan," 2023a.

[17] Zenodo.org, "Zenodo.org," 2023. [Online]. Available: https://zenodo.org.

[18] TeleRehaB DSS, "TeleRehaB DSS | D9.2 POPD Requirement No 2 (Data Trasfers)," TeleRehaB DSS Project, 2023c.

[19] The European Parliament and of the Council of the EU, "Charter of Fundamental Rights of the European Union," 26 10 2012. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT.

[20] Council of Europe, "European Convention on Human Rights," 1 8 2021. [Online]. Available: https://www.echr.coe.int/documents/d/echr/Convention_ENG.

[21] S. Y. K. R. W. L. Y. T. H. Ming Li, "Toward privacy-assured and searchable cloud data storage services," *IEEE Network,* vol. 27, no. 4, pp. 56-62, 7-8 2013.

[22] Council of Europe, "Convention for the protection of individuals," 18 5 2018. [Online]. Available: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.

[23] TeleRehaB DSS, "TeleRehaB DSS | D5.1 Study initiation package," TeleRehaB DSS Project, 2023b.

[24] European Comission, "Gender equality in the European Research Area (ERA)," 2000, 2018. [Online]. Available: https://research-and-innovation.ec.europa.eu/strategy/strategy-2020-2024/democracy-and-rights/gender-equality-research-and-innovation_en#gender-equality-in-the-european-research-area-era.

[25] The European Parliament and of the Council of the EU, "Regulation (EU) No 695/2021 of the European Parliament and of the Council of 28 April 2021 on establishing Horizon Europe – the Framework Programme for Research and Innovation," 21 4 2021. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2021/695/oj.

[26] European Commission, "A Union of Equality: Gender Equality Strategy 2020-2025," 5 3 2020. [Online]. Available: file:///C:/Users/chris/Downloads/gender_equality_strategy_2020_2025_en_77C86437-0983-F10D-E0FF41E71D577EE0_68222.pdf.

[27] European Commission, "Gender equality in research and innovation & Gender equality in Horizon Europe," [Online]. Available: https://research-and-innovation.ec.europa.eu/strategy/strategy-2020-2024/democracy-and-rights/gender-equality-research-and-innovation_en#gender-equality-in-horizon-europe.

[28] European Commission, Structural change in research institutions: Enhancing excellence, gender equality and efficiency in research and innovation,, Luxembourg: Publications Office of the European Union, 2012b, p. 13.

[29] L. Schiebinger, "What is Gendered Innovations?," 2011,2020. [Online]. Available: https://genderedinnovations.stanford.edu/what-is-gendered-innovations.html.

[30] TeleRehaB DSS, *TeleRehaB DSS | Description of the Action (DoA),* TeleRehaB DSS Project, 2022.

[31] IAPP-EY, "Annual Privacy Governance Report 2019," IAPP-EY, 2019.

[32] Directorate-General for Justice and Consumers, "Standard contractual clauses for controllers and processors in the EU/EEA," 21 06 2021. [Online]. Available: https://commission.europa.eu/publications/standard-contractual-clauses-controllers-and-processors-eueea_en.

[33] Directorate-General for Justice and Consumers, "Standard contractual clauses for international transfers," 21 06 2021. [Online]. Available: https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en.

[34] European Commission, "New Standard Contractual Clauses - Questions and Answers overview," 21 06 2021. [Online]. Available: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en.

[35] The European Parliament and of the Council of the EU, "Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 Oct 2018, on the protection of natural persons with regard to the processing of personal data by the Union," 2018. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1725.

[36] Directorate-General for Research and Innovation (European Commission), "European Group on Ethics in science and new technologies," EU Publications, 2021.

[37] TeleRehaB DSS, "TeleRehaB DSS | D1.1 Data Management Plan," TeleRehaB DSS Project, 2023a.

12 Appendix A | Organisational & Technical Measures Summary Table

In order to provide a comprehensive overview, a table has been created to list all of the measures discussed in the previous paragraphs. Each measure has been assigned a corresponding ethical or legal framework, which is noted in the table for easy reference.

Measure	CTR	AI	GDPR	CTR	GE	Other
Organisational Measures						
Defined Processing Purpose **Mentioned in** **Chapter 9.1, The Defined Purpose of the Data Processing, page 34**	-	Applicable	Applicable	-	-	-
Informed Consent **Mentioned in** **Chapter 3.1, Informed Consent (IC), page 11**	Applicable	-	Applicable	-	-	-
Data Sharing Agreement **Mentioned**	-	-	-	-	-	Sharing Agreement for Anonymised Data
Joint Controllers Agreement	-	-	Applicable	-	-	-
Dtaa Processors Agreement	-	-	Applicable	-	-	-
Purpose Definition	-	-	Applicable	-	-	-
Privacy/Security Breach Management of Personal Data	-	-	Applicable	-	-	-
Technical Measures						

Measure	CTR	AI	GDPR	CTR	GE	Other
Encryption at Rest	-	-	Applicable	-	-	-
Measures mentioned in chapter 5.6, Security and Privacy Technical Measures, page 24	-	Applicable	Applicable	-	-	-
Measures mentioned in chapter 4.1 Mitigating Risks and Implementing Measures, page 18	-	Applicable	-	-	-	-
Measures mentioned in chapter 5.6, Security and Privacy Technical Measures, page 24	-	Applicable	Applicable	-	-	-
Data Security and Privacy Breach Management mentioned in Chapter 6.3, Data Security and Privacy Breach Management, page 29	-	Applicable	Applicable	-	-	-

13 Appendix B | Joint Data Controllers and Data Processors Agreements

The following documents are attached:

TeleReHaB DSS - Joint Controllers Ter

TeleReHaB DSS - Data Processors Agr

14 Appendix C | Data Sharing Agreement Template

The following documents are attached:

Data Sharing Agreement for Anor

15 Appendix D | Standard Contractual Clauses

The following documents are attached:

COMMISSION IMPLEMENTING DECISION on standard contractual clauses between controllers and processors under Article 28 (7) of Regulation (EU) 2016/679 and Article 29 (7) of Regulation (EU) 2018/1725

EN Standard Contractual Clauses

Standard contractual clauses for controllers and processors in the EU/EEA

EN Annex Standard Contractual Clauses

16 Appendix E | List of Participants (Organisations)

This is the list of the organisations participating in the consortium for the TeleRehaB DSS project. Furthermore organisations (3), (7), (11), (12), (13) are expected to carry out the clinical study [23], therefore 'lead' the personal data processing by defining the purpose and taking the role of Data Controllers .

(1) **INSTITUTE OF COMMUNICATION AND COMPUTER SYSTEMS (ICCS)**, PIC 999654356, established in Patission Str. 42, ATHINA 10682, Greece,

(2) **PANEPISTIMIO IOANNINON (UOI)**, PIC 999852818, established in PANEPISTEMIOYPOLE PANEPISTEMIO IOANNINON, IOANNINA 45110, Greece,

(3) **CHULALONGKORN UNIVERSITY (KCMH)**, PIC 999869211, established in PHYATHAI ROAD 254 PATHUMWAN, BANGKOK 10330, Thailand,

(4) **VILABS OE (VILABS)**, PIC 955444375, established in THERMOKOITIDA TECHNOPOLIS VEPE TECHNOPOLI PYLAIA, THESSALONIKI 55535, Greece,

(5) **ISTRAZIVACKO RAZVOJNI CENTAR ZA BIOINZENJERING BIOIRC DOO (BIOIRC)**, PIC 997234012, established in PRVOSLAVA STOJANOVICA STREET 6, KRAGUJEVAC 34000, Serbia,

(6) **ACTIVE AGEING ASSOCIATION (ACT)**, PIC 893713187, established in RONDA AUGUSTE Y LOUIS LUMIERE Nº 23 - NAVE 13, PATERNA 46980, Spain,

(7) **ETHNIKO KAI KAPODISTRIAKO PANEPISTIMIO ATHINON (NKUA)**, PIC 999643007, established in 6 CHRISTOU LADA STR, ATHINA 10561, Greece,

(8) **ARINIMI ON BRIDG OU (BRD)**, PIC 889383495, established in HARJU MAAKOND LASNAMAE LINNAOSA LOOTSA TN 5-11, TALLIN 11415, Estonia, 1

(9) **UNINOVA-INSTITUTO DE DESENVOLVIMENTO DE NOVAS TECNOLOGIASASSOCIACAO (NOVA)**, PIC 999633889, established in CAMPUS DA CAPARICA QUINTA DA TORRE, CAPARICA 2829-516, Portugal,

(10) **QUANTITAS SRL (QUAN)**, PIC 915312856, established in VIA CARLO REZZONICO 6, PADOVA 35131, Italy,

(11) **UNIVERSITAETSKLINIKUM FREIBURG (UKLFR)**, PIC 999881918, established in HUGSTETTER STRASSE 49, FREIBURG 79106, Germany,

(12) **DRES RIPOLL Y DE PRADO SLP (RYDP)**, PIC 889251769, established in CALLE MIGUEL HERNANDEZ 12, MURCIA 30011, Spain,

(13) **UNIVERSITY COLLEGE LONDON (UCL)**, PIC 999975620, established in Gower Street, London WC1E 6BT, England, United Kingdom,

(14) **GUYS AND ST THOMAS' NHS FOUNDATIONTRUST (HIN)**, PIC992185938 in St Thomas' Hospital, Westminster Bridge Rd, London SE1 7EH, United Kingdom.

This page is left intentionally blank

End of Doc