This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No 101092889, Topic HORIZON-CL4-2023-HUMAN-01-21

LUMINOUS

Language Augmentation for Humanverse

Project Reference No	101135724
Deliverable	D5.2. H - Requirement 2 (POPD)
Work package	WP5: Ethics Requirements
Nature	D (Deliverable)
Dissemination Level	PU - Public
Date	29/02/2024
Status	Final v1.0
Editor(s)	**Eleni Mangina (UCD)** Muhammad Zeshan Afzal (DFKI) Daniel Perez-Marcos (Mindmaze) Florendia Fourli (Hypercliq) Oier Lopez de Lacalle (EHU/UPV) Nicoletta Cioria (Mindesk) Ander Salaberria (EHU/UPV) Marco Bianchi (LUDUS) EEAB Members Didier Stricker (DFKI)
Involved Institutions	All Partners
Document Description	This deliverable presents the POPD Ethics requirement for the Luminous project.

CONTENTS

LIST OF TABLES

Table 1: List of Abbreviations

Term / Abbreviation	Definition
EEAB	External Ethics Advisory Board
GDPR	General Data Protection Regulation
FAIR	Findability, Accessibility Interoperability and Reusability
nFADP	New Federal Act on Data Protection
IDS	Intrusion Detection Systems
DPIA	Data Protection Impact Assessment

1 INTRODUCTION

1.1 PURPOSE OF THE DOCUMENT

WP5, Ethics Requirements, encompasses three deliverables: D5.1 for overseeing human participation, **D5.2 for personal data protection,** and D5.3 for managing ethics risks related to AI, research participants, and end-users. These deliverables focus on ethical monitoring throughout the project's duration. Additionally, the project planned the appointment of an External Ethics Advisory Board (EEAB) in M1, as described in D5.1. The EEAB's role includes overseeing ethical and legal compliance aspects during the project.

The EEAB provides feedback to the project's Ethics Manager, Prof. Eleni Mangina from University College Dublin, who coordinates the LUMINOUS consortium's internal ethics monitoring activities.
The current document is covering the activities involving the protection of Personal Data and reflecting the consortium's ability to identify and address all relevant ethical issues as the LUMINOUS project progresses.

1.2 STRUCTURE OF THE DOCUMENT

The structure of the document that follows addresses all ethics requirements as raised in LUMINOUS ethics appraisal, namely the following:

Table *2* – Structure of D5.2

Section 1	Introduction and rationale of the document
Section 2	General Ethical and Legal Principles for the Protection of Personal Data
Section 3	Protection of personal data, explaining the processes and procedures to be followed: the Record of Processing Activities (RoPA), the Data Flow of the Project, the Data Protection Impact Assessment (DPIA)
Section 4	Ethics risks for LUMINOUS project
Section 5	Non-EU partners in the LUMINOUS Project
Section 6	Technical and organizational measures to be implemented to safeguard the rights and freedoms of the data subjects/research participants
Section 7	Security measures that will be implemented to prevent unauthorized access to personal data or the equipment used for processing
Section 8	LUMINOUS website, newsletters, and social media plug- ins
Annex I	DATA PROCESS IMPACT ASSESSMENT (DPIA) OF THE LUMINOUS PROJECT

2 GENERAL ETHICAL AND LEGAL PRINCIPLES FOR THE PROTECTION OF PERSONAL DATA

The LUMINOUS consortium is aware of the ethical, privacy, copyright and data protection issues that might be raised by the activities to be performed in the scope of the project. The consortium deemed it appropriate to peruse the legal framework that governs the activities of the project. Specifically:

[1] The Charter of Fundamental Rights of the European Union[1]

[2] The European Union e-Privacy Directive 2002/58/EC[2]

[3] The Directive 2016/680 of the European Parliament and of the Council of April 27th, 2016, on the protection of natural persons with regards to the processing of personal data by the competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and on the free movement of such data thus repealing Council Framework Decision 2008/977/JHA[3]

[4] The Directive 95/46/EC on the protection of personal data[4]

[5] The Council of Europe Convention No. 108/1981[5] for the protection of individuals regarding automatic processing of personal data

[6] The (EU) Regulation 2016/679 of the European Parliament and of the Council of April 27th, 2016, on the protection of natural persons with regards to the processing of personal data and on the free movement of such data thus repealing Directive 95/46/EC[6]

[7] The European Convention of Human Rights and Fundamental Freedoms[7] (Article 8 - protection of private and family life)

[8] ST 9565 2015 INIT - Proposal for a Regulation of the European Parliament and of the Council on the protection of the individuals about the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Preparation of a general approach[8]

On the other hand, the ethical guidelines for research projects in the EU under Horizon 2020 which must comply with the ethical principles and the relevant national and EU legislation i.e.

[9] Horizon 2020 Rules for Participation: Ethics Reviews (Article 14)[9]

[10] Horizon 2020 - Regulation of Establishment: Ethical principles (Article 19)[10]

[11] Model Grant Agreement: Ethics (Article 34)[11] and d) the document "Horizon Europe Program Guidance - How to complete your ethics self-assessment"[12].

The LUMINOUS consortium will act in accordance with the above-mentioned legislation and Horizon Europe ethical principles, as it pertains to any individual that might be involved in the project either as a participant or not.

---

[1] Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

[2] Available at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058

[3] Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L0680

[4] Available at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A31995L0046

[5] Available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

[6] Available at HTTPS://EUR-LEX.EUROPA.EU/LEGAL-CONTENT/EN/TXT/PDF/?URI=CELEX:32016R0679

[7] Available at https://www.echr.coe.int/documents/convention_eng.pdf

[8] Available at https://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf

[9] Available at https://ec.europa.eu/research/participants/data/ref/h2020/legal_basis/rules_participation/h2020-rules-participation_en.pdf#page=10

[10] Available at https://ec.europa.eu/research/participants/data/ref/h2020/legal_basis/fp/h2020-eu-establact_en.pdf#page=11

[11] Available at https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/amga/h2020-amga_en.pdf

[12] Available at https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf

3 PROTECTION OF PERSONAL DATA

LUMINOUS will integrate emerging technologies from all three pilots. The LUMINOUS consortium has initiated the following processes to safeguard partnership's GDPR compliance and has an overview of how project' data are handled and mapping potential risks and mitigation measures.

Table *3* – Consortium partners list per pilot

# #	Participant organisation name	Country	Type	PILOT 1	PILOT 2	PILOT 3
1.	DFKI – Deutsches Forschungszentrum für Künstliche Intelligenz GmbH	Germany	RES	DFKI	DFKI	DFKI
2.	Ludus – Ludus Tech SL	Spain	SME		LUDUS	
3.	MINDESK – Mindesk SRL	Italy	SME			MINDESK
4.	MindMaze – MindMaze SA	Switzerland	LE	MindMaze		
5.	CHUV – Centre hospitalier universitaire vaudois	Switzerland	RES	CHUV		
6.	UCL – University College London	UK	RES	UCL		
7.	HHI – Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V.	Germany	RES			
8.	EHU – University of the Basque Country - EHU	Spain	RES	EHU	EHU	EHU
9.	VICOM – Fundación centro de tecnologias de interacción visual y comunicaciones Vicomtech	Spain	RES	VICOM	VICOM	VICOM
10.	UCD – University College Dublin, National University of Ireland	Ireland	RES	UCD (Ethics)	UCD (Ethics)	UCD (Ethics)
11.	HC – Hypercliq IKE	Greece	SME	HC	HC	HC
12.	RICOH – Ricoh International B.V. – Niederlassung Deutschland	Germany	LE	RICOH	RICOH	RICOH

3.1 RECORD OF PROCESSING ACTIVITIES

In accordance with Article 30 of GDPR regulation, the partners have provided the Record of Processing Activities (RoPA) (D5.1, Annex 2). The RoPA is a document that outlines an project's data processing activities, such as how personal data is collected, used, stored, and shared. This live document ensures that the involved organizations are aware of the data processing activities, they have taken the necessary steps to comply with the GDPR and have implemented appropriate measures to protect personal data. In the case of non-member states of the EU, the pilots will refer to the adopted GDPR in its national legislation (Pilot 1).

3.2 PROVISION OF THE PROJECT DATAFLOW

The data flow diagrams (D5.1 – Annex 7) illustrate how data is communicated (or else "flows") through a project's systems and processes. It outlines the different stages of the data's journey, from its initial collection to its final disposal or deletion. By identifying the sources of personal data, the diagram helps to ensure that the project team is aware of all the ways in which personal data are handled. This can include activities such as storage, analysis, sharing, and transfer of data. By mapping out these activities, the diagram helps the project team to identify any potential vulnerabilities or risks in the data processing chain.

3.3 OPINION ON THE NECESSITY OF THE DATA PROTECTION IMPACT ASSESSMENT

Article 35 of General Data Protection Regulation 2016/679[13] foresees carrying out an assessment of the impact of the envisaged processing operations on the protection of

[13] Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

personal data, in case these processing operations are "likely to result in a high risk to the rights and freedoms of natural persons".

The GDPR identifies several specific circumstances that would trigger the need for a DPIA:

1. **Evaluation or scoring:** If the processing involves evaluating or scoring individuals, for example, profiling: this is applied to the LUMINOUS project; the implementation of a qualitative methodology including evaluation questionnaires, satisfaction/experience online surveys, and self-assessment questionnaires are foreseen within the framework of the LUMINOUS Pedagogical Framework.
2. **Automated decision-making:** If the processing involves automated decision-making that could impact an individual's rights: this is not applicable in the LUMINOUS project.
3. **Systematic monitoring:** If the processing involves systematic monitoring of a publicly accessible area on a large scale: this is not applicable in the LUMINOUS project.
4. **Sensitive data:** If the processing involves the use of sensitive data, such as data relating to health, ethnicity, religion, or sexual orientation: this is not applicable in the LUMINOUS project.
5. **Cross-border data transfers**: If the processing involves the transfer of personal data to a country outside of the EU or the European Economic Area: although non-EU countries are members of the LUMINOUS consortium, this is not applicable in the LUMINOUS project; this requirement is separately handled in Section 4.
6. **Innovative use of new technologies:** If the processing involves the use of new technologies, such as artificial intelligence, facial recognition, or biometric data: this is applicable in the LUMINOUS project; the LUMINOUS solution involves AI technologies, namely the development of an AI-boosted toolkit that provides different types of educational and training stakeholders with explainable recommendations for smart search and identification of educational resources. This requirement will be separately handled in D8.3, due in M12.
7. **Large-scale processing:** If the processing involves the processing of a large amount of personal data on a regular basis; this is not applicable in the LUMINOUS project.
8. **Systematic and extensive profiling**: This occurs when personal data is used to analyse or predict an individual's behaviour, preferences, or attitudes. This could include tracking an individual's online activity, using automated decision-making systems, or creating detailed profiles based on multiple data sources: this is applicable in the project, since the LUMINOUS solution foresees the design of personalized learning profiles that considers individual actors' characteristics, needs, and preferences.

Summarizing this input, it turns out that **cases 1, 6, and 8 are applicable** to the LUMINOUS project. Considering the above, we state the opinion that LUMINOUS project data processing operations have a considerable probability to result in high risk to the rights and freedoms of natural persons and Data Protection Impact Assessment, according to Article 35 of General Data Protection Regulation 2016/679, is necessary.

The LUMINOUS consortium recognizes the importance of conducting a DPIA for each pilot, to identify potential ethics risks in the pilot implementation, including how pilots will be carried out, participant involvement, data collection and processing in compliance with GDPR regulations. To this end a DPIA template has been prepared for each pilot to include a thorough assessment of relevant risks and the implementation of appropriate mitigation measures by M6. LUMINOUS DPIA template is available in Annex I and the detailed DPIA will be provided for each pilot at the Annex of D6.1, D6.2 and D6.3 respectively for each pilot.

3.4 PROCEDURES FOR PERSONAL DATA COLLECTION

All the data collection and the processing tasks within the LUMINOUS consortium will be GDPR compliant and will be carried out according to the EU and the national legislation.

Any data collected by the LUMINOUS consortium will be anonymised and the responsible partner should explain how all the data they intend to process is relevant and limited to the purposes of their intended task (in accordance with the “data minimization” principle). The Ethics Manager under the guidance of the EAB will review the request and will give feedback to the partner to follow the due process. Any confidential data collected from the users will be handled only by the involved partners using local data management and storage systems, obtainable with different levels of access, regulated by the Partner acting as the Controller of the data. The Partner acting as the Controller will also be responsible for the data management, the secure storage, and the deletion of the confidential data beyond the lifetime of the project. The publicly available data will be stored on the GDPR compliant Cloud platform, with different levels of access, regulated by the Project Coordinator. Any data that is publicly available will be accessible through the FAIR (Findability, Accessibility Interoperability and Reusability) principle. The LUMINOUS consortium will submit an explicit confirmation to the External Ethics Advisory Board that the data is publicly available and can be freely used for the purposes of the project. At the completion of the project, all the responsibilities concerning the long-term data management and the secure storage of the publicly available data will fall on the selected service for storing the project data based on the decision and agreement established by the Procedures for Data Storage, Protection and Retention.

In case Personal Data are collected during the LUMINOUS project, they will be stored by the partner in charge and all data will be pseudonymized before shared or transferred to any other partner; this in practice means that actual data will be extracted and replaced with a coded reference (a ‘key’); the connection of the “coded reference” with the actual data will be kept by the partner in charge, whereas the coded, pseudonymized data will be transferred to the partner that wishes to analyse them.

3.5 PROCEDURES FOR DATA DESTRUCTION

The LUMINOUS project has established procedures for data destruction to ensure the protection of confidential information. If any confidential data is collected during the project, it will be securely deleted from the project's data storage after a period of five (5) years following the completion of the project. This time frame allows for the appropriate retention of data for analysis and evaluation purposes while also ensuring that personal information is not retained indefinitely. The data destruction process will be carried out in a manner that adheres to relevant privacy regulations and best practices to safeguard the confidentiality and privacy of the collected data.

4 ETHICS RISKS FOR LUMINOUS PROJECT

This section lists the main risks related to the data processing activities in this research project taking into consideration an initial evaluation and those identified in the DPIA. It follows an assessment of these risks, considering the LUMINOUS specifics, methods, and practices. It should be highlighted that the AI risks are presented in the D5.3, under section 6 Ethical Risk Assessment and Mitigation in AI Lifecycle.

4.1 USAGE OF PERSONAL DATA FROM PUBLIC /OPEN-SOURCE SOURCES

Risk identification: The use of public or open-source data for research purposes is a common and widely accepted practice. However, it is important to acknowledge that utilizing such sources can present certain ethical risks. Therefore, it is crucial to ensure that the data found in these sources can be ethically used for research purposes. Additionally, data processing operations carried out while working with these sources must have a legitimate basis.
Risk Assessment: it has been agreed that if there is a need to utilize publicly available personal data, partners must confirm the following:

- The data is openly and publicly accessible and can be used for research purposes.
- The data being used has been intentionally made public by the respective data subjects.
- Partners have a lawful and legitimate basis for processing the data.

It is important to note that public sources may also be used for dissemination purposes, such as contacting national and regional officials, policy makers, journalists, etc., whose contact details are publicly available for publicity and public relations purposes. Taking into consideration the explanation, the probability of the risk of improper handling or misuse of publicly available personal data is evaluated as low.

4.2 USAGE DATA FROM SOCIAL MEDIA SOURCES

Risk identification: Similarly, to the above, while using data from social media sources, it must be ensured that the data were intended to be public and that data processing operations intended by LUMINOUS have lawful / legitimate basis.
Risk assessment: The LUMINOUS partners are not planning to use any personal data from social media networks; however, usage of such data cannot be excluded. For example, data from social media networks might be used also for dissemination purposes (e.g. contacting researchers whose research interests are in the field relevant/adjacent to LUMINOUS, journalists, etc.), whose contact details are made open for collaboration proposal, publicity, and public relation purposes.
Considering the explanation above, we evaluate the probability of the risk of improper handling/misuse of personal data available in social media networks as low.

4.3 PROTECTION OF HUMAN PARTICIPANTS

Risk identification: Identifying and abiding with the informed consent procedures is of primary importance; the consent process must ensure that individuals are voluntarily participating in the research with full knowledge of the relevant risks and benefits and can opt out at any time without any justification and repercussion. Additionally, confidentiality and privacy should be respected; maintaining privacy and confidentiality helps to protect

participants from potential harm including psychological harm, such as embarrassment or distress.

Risk assessment: In the case of humans as research participants, signed consent forms will be gathered from all stakeholders prior to the interview/ focus group/ pre-pilot and pilot. The consent form contains all the information to the interviewee, so that s/he is aware of the process, rights, risks, and benefits. At the same time, participants will be informed about the right they have to access, change, and delete their personal data, as well as the procedure they will have to follow to submit the relevant request.

The interview sheets will not contain any personal information about the interviewee, only the interviewee's code. Personal information of the interviewees will be only available on the signed consent forms. Pseudonymization techniques will be implemented to hide an individual's real identity, as well as to support un-link ability across different data processing domains. All relevant information is available in D5.1.

4.4 COLLECTION OF GENETIC, BIOMETRIC AND/OR HEALTH DATA

Risk identification: Genetic, biometric and/or health data is considered as a special category of personal data which may entail higher ethics risk and thus should be handled with special care.

Risk assessment: The LUMINOUS project does not involve the processing of personal data that identifies racial or ethnic origin, political opinion and beliefs, trade union membership, genetic data, biometric data, health data, information concerning health, sex life, or sexual orientation of individuals. This approach ensures that the project respects individuals' privacy rights and adheres to relevant data protection regulations. By avoiding the processing of sensitive data without explicit consent, the project maintains a strong commitment to privacy and data protection principles while still working towards inclusivity and addressing the needs of vulnerable groups.

However, in case sensitive data is processed, apart from the consent form, a declaration of compliance with the respective national legal framework(s), will be shared. This declaration will serve as confirmation that the research project adheres to the specific requirements and regulations outlined in the country's laws concerning the processing of genetic, biometric, and/or health data. By submitting this declaration, researchers will demonstrate their commitment to conducting the research in accordance with applicable legal provisions and safeguarding the rights and privacy of the data subjects involved. The purpose of these checks and declarations will ensure that the research activities involving sensitive data are conducted in a lawful and compliant manner, considering the specific regulations and protections that apply to genetic, biometric, and health data under the national legislation of the country where the research is taking place. Considering the explanation above, we evaluate the probability of the risk of improper handling/misuse of personal data containing health data as low.

4.5 USAGE OF PERSONAL DATA FROM PREVIOUS PROJECTS AND RESEARCH ACTIVITIES

Risk identification: Usage of personal data from previous projects and research activities may provide a valuable source of information. However, necessary measures shall be taken to minimize potential ethical risks, such as improper procedures for initial data collection, methodology and informed consent. Moreover, permission from the owner/manager of the dataset(s) so as to use the data in other projects/activities must be ensured.

Risk assessment: At this time, there are no specific plans for usage of personal data that were collected from previous research projects, however some partners might use such data, if it is necessary for the project purposes. In case of such necessity, partners shall ensure that the initial data collection, methodology and informed consent procedure were compliant with relevant GDPR articles. Additionally, these partners will have to confirm that they have permission from the owner/manager of the dataset(s) to use the data in LUMINOUS for research purposes, ensuring the probability of the risk of improper handling/misuse of personal data collected from previous research is low.

4.6 USAGE OF PERSONAL DATA COLLECTED IN LUMINOUS FOR OTHER RESEARCH PROJECTS.

Risk identification: While cross-fertilization and reuse of findings in research is an important aspect, the ethical aspect shall be handled with care. For example, data subjects whose personal information will be collected in LUMINOUS must have the opportunity to opt out of the further processing operation(s) –including those conducted by other research projects.
Risk assessment: Several partners of the consortium may use information and findings of the LUMINOUS for their further research activities and this may apparently also include personal data collected by the LUMINOUS. Considering this, prior to the collection of any personal data, consent forms shall be designed in a way giving data subjects the opportunity to opt out of the further processing operation(s). Ensuring that the probability of the risk of improper handling/misuse of personal data collected in the LUMINOUS for further research is low.

4.7 TRANSFER PERSONAL DATA TO NON-EU COUNTRIES AND/OR COLLECT PERSONAL DATA OUTSIDE THE EUROPEAN UNION.

Risk identification: This aspect is of increased sensitivity, due to the relatively high degree of uncertainty related to the data protection frameworks of non-EU countries and adequacy of these frameworks to the standards of the EU.
Risk assessment: At the time of submission of the present deliverable, Pilot 1 will involve users from non-EU countries (UK and Switzerland). Any transfers to parties located outside the European Union will be in line with the legal and regulatory provisions of the GDPR and applicable local legislation as amended from time to time. Thus, we evaluate the probability of research data as high and is extensively handled in section 5.

4.8 STORAGE OF RAW DATA

Risk identification: While organizational and technical measures to pseudonymize raw data might be appropriate and secure, storing of raw data might be required by internal policy or stakeholders of organizations participating in research. Thus, to minimize ethics risk it is important to apply appropriate organizational and technical measures also for the storage of raw data if the latter is planned.
Risk assessment: The protection of raw data is described in section 3.4, namely in the pseudonymization techniques that will be implemented and in sections 6 and 7, namely in the organizational /technical and security measures that will be implemented at consortium and partner level.

4.9 PARTICIPATION OF VULNERABLE GROUPS

Risk identification: LUMINOUS does not target any minors. Pilot 1 involves vulnerable group (neurohabilitation patients).

Risk assessment: To protect the vulnerable group, a certain policy has been prepared, available in D5.1, section 6, describing the process that will be followed and will be updated as needed, within the lifetime of the project.

4.10 PRIVACY CONCERNS

Risk identification: The collection and processing of stakeholders' data, including personal information and preferences, pose privacy risks. Inadequate data protection measures may lead to unauthorized access, data breaches, or misuse of personal information, impacting learners' privacy and potentially causing harm or identity theft.

Risk assessment: A Privacy by Design approach will be implemented; it will minimize the collection of personally identifiable information and adopt pseudonymization/anonymisation techniques.

4.11 SECURITY VULNERABILITIES

Risk identification: The LUMINOUS toolkit may be susceptible to security vulnerabilities, such as hacking or malware attacks. Breaches in security could lead to unauthorized access to learner data, compromising the confidentiality and integrity of personal information.

Risk assessment: Secure data transmission protocols will be implemented, such as encryption, when transferring user data between the AI-boosted toolkit and the XR technologies.

5 NON-EU PARTNERS IN THE LUMINOUS PROJECT

Within the partnership there is one partner based in UK (UCL) and two associated partners in Switzerland (MindMaze & Centre Hospitalier Universitaire Vaudois).

Table 3 – non-EU partners in LUMINOUS project

Partner Name	Country	Role in the project
University College London	UK	The UCL Queen Square Institute of Neurology is an institute within the Faculty of Brain Sciences of University College London (UCL). Together with the National Hospital for Neurology and Neurosurgery, the institute forms a major centre for teaching, training and research in neurology and allied clinical and basic neurosciences. Alex Leff, Professor of Cognitive Neurology and Consultant Neurologist at the UCL Queen Square Institute of Neurology will be the main expert participating in LUMINOUS on behalf of UCL. His main clinical and academic interest is in cognitive rehabilitation, especially in the field of acquired language disorders and vision. He has developed a range of web-based rehabilitation tools that can be used by therapists and patients with visual or language problems. At the UCLH National Hospital for Neurology and Neurosurgery he has a specialist out-patient MDT assessment clinic for patients with hemianopia and/or higher disorders of vision. He also helps run the Queen Square Intensive Comprehensive Aphasia Programme. Role: scientific and clinical input into S&Ts 3 & 5 and Pilot 1 (WP6). The project is now registered under, reference No **Z6364106/2024/02/11 clinical research** in line with UCL's Data Protection Policy.
Centre Hospitalier Universitaire Vaudois	Switzerland	With its 16 clinical and medico-technical departments & services, CHUV provides care to >50000 in- patients/year & 3400 out-patients/day. Newsweek magazine has included CHUV in its world's 10 best hospitals ranking. Role: lead of validation of Pilot 1 (WP6).
MindMaze	Switzerland	Founded in 2012, MindMaze is a global leader in FDA-cleared and CE-marked digital therapeutics (DTx) solutions for patients with neurological diseases. MindMaze's work is at the intersection of neuroscience, biosensing, mixed reality & AI. Role: Leader of Pilot 1 (WP6) and the leader of the Key Exploitable Asset on Digital Therapeutics Platform. Currently, MindMaze offers solutions for motor and cognitive rehabilitation. The deployment of patient-tailored therapeutic protocols addressing language deficits will enable MindMaze to offer an integrated approach to the management of acquired brain injury, both in clinic and at-home settings. The new tool will be integrated into MindMaze's existing B2B business model for rehab hospitals, and a B2B2P business model targeting private practices & patients willing to perform supervised home therapy. Approved Clinical protocol: https://clinicaltrials.gov/study/NCT05728840

The LUMINOUS consortium confirms that, in case any transfer of Personal Data occurs, respective non-EU partners will sign a declaration confirming their compliance with the Chapter V of the GDPR 2016/679 and the corresponding national laws while the appropriate justification that such transfers comply with the laws of the country in which the data was collected will also be provided.
The Ethics Manager, Prof. Eleni Mangina, in collaboration with the DPOs of all partners, and under the guidance of the External Ethics Advisory Board will oversee all the processes followed within the framework of the project and will review all the documentation, as needed.
Below it is presented the reference to the GDPR along with the respective national laws of the UK and Switzerland that should be taken under consideration.

Table 4 – Protection of personal data and reference frameworks

Protection of Personal Data		
EU Countries	**Non-EU Countries**	
Reference Framework: General Data Protection Regulation[14]	UK: The Data Protection Act 2018 is the UK's implementation of the GDPR[15].	Switzerland: New Federal Act on Data Protection (nFADP) enacted from 1st of September 2023[16].

[14] Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
[15] Available at https://www.gov.uk/data-protection
[16] Available at https://www.kmu.admin.ch/kmu/en/home/facts-and-trends/digitization/data-protection/new-federal-act-on-data-protection-nfadp.html

6 TECHNICAL AND ORGANIZATIONAL MEASURES TO BE IMPLEMENTED TO SAFEGUARD THE RIGHTS AND FREEDOMS OF THE DATA SUBJECTS/ RESEARCH PARTICIPANTS.

The LUMINOUS consortium implements a series of technical and organizational measures which are summarized as follows:

6.1 TECHNICAL MEASURES

[1] Pseudonymization of data: Personal data collected during the research will be pseudonymized to protect the privacy and identity of research participants.

[2] Data will be stored in accordance with Partners' data protection policy, and solely for the duration of the project. Usage of non-safe storage devices, such as memory sticks will be avoided.

[3] Data will be destroyed five years after the end of the project; the data management plan will include provisions for the long-term preservation and sharing of relevant research data beyond the completion of the project, ensuring its availability for future use and potential publication.

[4] Research documents will be stored on a data repository initiated for the research teams. Each research protocol will describe the procedures to be followed to ensure compliance with data protection regulations.

[5] Access controls: In addition to restricting access to authorized personnel only, access controls will also include role-based access controls and unique user accounts with strong passwords to ensure that each user has appropriate access rights to the research data. Access will also be regularly reviewed and updated as necessary, and any unauthorized access attempts will be detected and reported.

[6] Data monitoring: The Ethics Manager along with the External Ethics Advisory Board and Internal Ethics Advisory Board will have a key role in monitoring the use of research data to ensure that it is being handled in accordance with data protection regulations and ethical standards. This will involve regular reviews of data handling practices and monitoring of data usage to detect any potential breaches or misuse of data. Any issues that may arise will be reported to the relevant authorities and corrective actions will be taken as necessary.

[7] Data transfer protocols: Secure data transfer protocols will be used to ensure that any data that is transmitted between project partners and stakeholders is done so in a secure and confidential manner. In addition, data transfer protocols will be regularly reviewed and updated to ensure that they continue to meet the highest standards of security and privacy.

[8] Data breach response plan: A data breach response plan will be in place to ensure a timely and appropriate response to any potential data breaches or security incidents. The plan will outline the steps that should be taken in the event of a breach or incident, including:

- Identifying and containing the breach: The first step will be to identify the breach and contain it to prevent any further damage. This might involve disabling affected systems, blocking unauthorized access attempts, or taking other measures to limit the impact of the breach.

- Assessing the scope and severity of the breach: The project team will need to assess the scope and severity of the breach to determine what data has been compromised and what impact it might have on the project and its stakeholders.
- Notifying affected individuals: If the breach has affected personal data, the project team will need to notify affected individuals in a timely and appropriate manner. This will involve providing clear and concise information about the breach, the steps that are being taken to address it, and any actions that individuals should take to protect themselves.
- Reporting the breach to relevant authorities: Depending on the scope and severity of the breach, the project team may need to report it to relevant authorities, such as data protection regulators or law enforcement agencies.

6.2 ORGANIZATIONAL MEASURES

[1] Each partner involved in the LUMINOUS project has an assigned DPO who is responsible for overseeing the data protection strategy and the implementation, the overall aim being to ensure compliance with the GDPR requirements.

[2] The appointment of the Ethics Manager to undertake the ethical oversight of the project and review all relevant documentation. The Ethics Manager, WP5 Leader Prof. Eleni Mangina, works in close collaboration with the DPOs / Ethics Committees of all the LUMINOUS partners; she provides guidelines on how to proceed with the research protocols, reviews and provides feedback to all relevant documentation needed. Prof. Mangina acts as a liaison among the Internal, the External Advisory Boards and the consortium, overseeing ethical compliance and coordinating all relevant discussions.

[3] The formulation of the (External) Ethics Advisory Board at the early stage of the project. It advises members of the consortium on ethical issues, prepares position statements, and initiates debates on ethics. It will also consider specific ethical issues raised before, during, and after the implementation of LUMINOUS pre-pilots and pilots upon the request of the consortium members. The goal is to ensure stakeholders' well-being and create a culture of responsibility in the use of XR technology. The 4 Board Members bring into the project their expertise in Human-centred AI, Neuroscience and societal impact, Trustworthy AI systems and Data Science.

[4] The formulation of the Internal Ethics Advisory Board, including the Ethics Manager, representatives of the pilots and partners with expertise in ethics oversight. The Internal Ethics Advisory Board is responsible for ensuring that the project adheres to ethical principles and guidelines, and that any ethical issues are addressed appropriately. They work closely with the representatives of the pilots and partners to develop and implement ethical standards for the project.

[5] The arrangement of bimonthly Telcos among partners, the Ethics Manager, and the coordinating team, so as to review all processes, summarize current activities, and plan what is next, taking into consideration the project timeline; ad hoc Telcos are also organized, in case of urgent issues.

[6] The identification of a certain monitoring process during the research activities, which is clearly stated in the information sheet and consent form; *The Ethics Manager of the project will oversee that the procedures run smoothly; in case of any non-compliance, the local partner in collaboration with the relevant WP6 Leader will decide the timeline and mitigation measures, so as to take all the necessary actions in a timely manner and*

ensure full compliance with the legal and ethical requirements of the project. In all cases, all non-compliant actions will be immediately suppressed or suspended, and the partners will implement a mitigation action within 5 working days.

[7] Regular training for project personnel: Regular training sessions can be held for all personnel involved in the project, including researchers, developers, and administrators, to ensure they are aware of their responsibilities in terms of data protection and ethics.

It should be noted that further information on the setup of the External and Internal Ethics Advisory Boards is already available in D5.1 and no detailed reference will be made in the current deliverable to avoid repetition.

7 SECURITY MEASURES THAT WILL BE IMPLEMENTED TO PREVENT UNAUTHORIZED ACCESS TO PERSONAL DATA OR THE EQUIPMENT USED FOR PROCESSING

The LUMINOUS consortium implements a series of security measures which are summarized as follows:

[1] **Access controls:** Access controls limit access to personal data to only authorized individuals. Access controls can include the use of strong passwords, multi-factor authentication, and role-based access controls. Passwords will be unique, complex, and changed regularly to reduce the risk of password-based attacks. Multi-factor authentication provides an additional layer of security by requiring a second form of identification, such as a token or biometric information. Role-based access controls ensure that only individuals with a legitimate need to access personal data are granted access.

[2] **Encryption:** Encryption is the process of converting personal data into an unreadable format that can only be decrypted with a key or password. Encryption will be applied to data both at rest and in transit, reducing the risk of unauthorized access to personal data in the event of a security breach.

[3] **Firewalls and intrusion detection systems:** Firewalls and intrusion detection systems (IDS) are security measures designed to prevent unauthorized access to networks and equipment used for processing personal data. Firewalls will block unauthorized traffic to and from the network, while IDS will monitor network traffic for suspicious activity and alerts administrators of potential security breaches.

[4] **Regular security testing and vulnerability assessments:** Regular security testing and vulnerability assessments will help identify weaknesses in security measures and enable organizations to take appropriate remedial action to mitigate risks.

[5] **Regular training and awareness programs:** Regular training and awareness programs will help employees understand the importance of data protection and security best practices, reducing the risk of human error and insider threats.

8 LUMINOUS WEBSITE, NEWSLETTERS, AND SOCIAL MEDIA PLUG-INS.

Special reference should be made to all the processes that will be followed in the LUMINOUS website and subscription to the LUMINOUS newsletter and the social media accounts.
The LUMINOUS website will include the Privacy and Cookie Policy, which will cover the following sections:

- **Type of personal information that will be collected**, while visiting the project website and/ or when subscribing to the LUMINOUS newsletter.
- **Use of the personal information that will be collected,** namely:
  - contacting those that have subscribed to the project newsletter within the framework of the project dissemination, and
  - not using this information for any purpose other than those described in the Privacy Policy without informing and /or obtaining subscribers' consent first, when necessary.
- **Sharing of personal information that will be collected.**
  The website of LUMINOUS will not sell or lease its contact list to third parties. Lists of stakeholders, provided by the LUMINOUS consortium members, will be securely saved in the LUMINOUS repository, available in the Project Repository in Google Drive, accessed only by the consortium members.
- **Storage and deletion of personal information that will be collected.**
  It should be noted that any personal information provided through the LUMINOUS website section under "contact us" will be only used for communication purposes and securely stored on the LUMINOUS's website server by the coordinator, only for as long as it is necessary for the project to comply with the contractual obligations to the funding authority of LUMINOUS, and no longer than 5 years from LUMINOUS's completion, namely 12/2032.
  Newsletter recipients will be able to unsubscribe from the contact list and/or request for their personal information to be deleted anytime by opting to unsubscribe in the e-mails and/or newsletters that they receive from the project, or by directly contacting the Project Coordinator (e-mail: didier.stricker@dfki.de)
- **Security of personal information that will be collected.**
  The LUMINOUS website takes information security seriously and uses reasonable physical, electronic, and managerial procedures to help prevent unauthorized access, maintain data security and correctly use the information that is collected, namely the following:
  - **Right to be informed**: Users will have the right to be informed about the collection and use of their personal information, including the purpose for which LUMINOUS is processing this information, the period that the project will retain it and with whom it will be shared.
  - **Right of access**: Users will have the right to ask from LUMINOUS to confirm whether, within the framework of the project, personal information is processed.
  - **Right to rectification**: Users will have the right to request from LUMINOUS modifications to their personal information in case they believe that it is not up to date, complete or accurate.

- **Right to erasure** ("right to be forgotten"): Users will have the right to ask LUMINOUS to erase their personal information that the LUMINOUS website is processing.
- **Right to restrict processing**: Users will have the right to request from LUMINOUS to restrict the processing of their personal information, with a view to limiting the way that this information is used.
- **Right to data portability**: Users will have the right to ask for their personal information to be provided back to them or transferred to a third party.
- **Right to object**: Users will have the right to object to LUMINOUS processing their personal information at any time for reasons related to their particular situation.
- **Right not to be subjected to a decision based solely on automated processing** (including profiling), which produces legal effects concerning users or similarly significantly affects them.

It should be noted that the LUMINOUS site visitors and /or newsletter recipients can exercise their rights, by sending a notice to the Coordinator of the project. It should also be kept in mind the right to lodge a complaint in the supervisory authority (e.g., the Data Protection Authority within the region or country) of the site visitor and/ or newsletter recipient.

- **Cookies**
  Cookies are small text files, which are saved on computers, mobile phones or tablets. They allow the website to remember users' actions and preferences (such as login, language, font size and other display preferences), so that users don't have to keep re-entering them, whenever they come back to the site. Users can control and/or delete cookies as they wish. If they do this, however, they may need to manually adjust their preferences every time they visit a website. In the LUMINOUS Privacy and Cookie Policy certain info on how to manage Cookies[17].
- **Google[18] Analytics**
  The LUMINOUS project uses tools like Google Analytics to better understand how visitors interact with the website. This will provide important information to enable the site to be more engaging. This information is not linked to visitors' personal data.
- **Social media plug-ins**
  LUMINOUS uses social media to present and communicate project work through widely used communication channels and maximize the impact of research activities. Thus, in the LUMINOUS webpage social media plug-ins are used (the so-called social media buttons) to enable this interaction. These plug-ins are small buttons, which can be recognized by bringing a social media logo, for instance the LinkedIn logo. The function of these buttons is to allow users to share the contents of the LUMINOUS website in their profile on social networks and to access via links.

[17] Available at https://ec.europa.eu/info/cookies_en#howcanyoumanagecookies
[18] Available at https://analytics.google.com/analytics/web/

8.1 THE LUMINOUS ACCOUNTS IN OTHER SOCIAL PLATFORMS

The project plans to be active in two social networks: LinkedIn, Youtube. Each social media platform has its own data protection policy, when accessing a website. If a user does not wish his/ her data to be tracked via the LUMINOUS website, then s/he should log out of his/ her social media accounts before visiting the LUMINOUS website.
Specifically, the following social media plug-ins are used:

a. LinkedIn: share/link button
   Some information is transferred to LinkedIn Corporation, 2029 Stierlin Court, Mountain View, CA 94043, USA ("LinkedIn").or comprehensive information on data protection with LinkedIn, please refer to the LinkedIn privacy statement.
b. YouTube: link button for YouTube
   In the case of YouTube, information may be transferred to the parent company Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA ("Google"). If embedded videos are added to the LUMINOUS website in the future, we will use the "extended data protection mode" provided by YouTube to minimize data exposure. This mode prevents the transfer of personal data when loading a webpage with an embedded YouTube video from the LUMINOUS official YouTube account.

9 CONCLUSION

In conclusion, D5.2 serves as a comprehensive summary outlining the ethical monitoring procedures for the protection of personal data to be implemented within the LUMINOUS project. It emphasizes the importance of safeguarding General Data Protection Regulation (GDPR) compliance while ensuring the protection of personal data. The document provides a structured approach by addressing key aspects such as general ethical and legal principles, processes and procedures for data protection, and risk assessment of potential ethical issues. The outlined procedures, including the Record of Processing Activities (RoPA), provision of the project dataflow, and necessity of Data Protection Impact Assessment (DPIA), demonstrate the commitment to maintaining transparency and accountability in handling personal data. Additionally, the document highlights specific ethical risks associated with the project, such as the usage of personal data from various sources and protection of human participants. Considering the involvement of non-EU partners, the consortium emphasizes the need for a declaration from these partners, confirming their compliance with GDPR and national data protection laws. This declaration ensures that any transfer of personal data adheres to legal requirements and respects the rights and freedoms of the data subjects.
To protect the data subjects and research participants, both technical and organizational measures will be implemented, ensuring the necessary safeguards are in place. Security measures will also be established to prevent unauthorized access to personal data and the associated processing equipment.
The document acknowledges the presence of the LUMINOUS website, newsletters, and social media plug-ins, emphasizing the need to handle personal data appropriately in these channels. The consortium recognizes the importance of maintaining GDPR compliance across all digital platforms and ensures that the necessary measures will be implemented.
Overall, D5.2 serves as a comprehensive framework and roadmap for ensuring ethical monitoring and GDPR compliance within the LUMINOUS project. It provides a clear and structured approach to protect personal data, address potential ethical risks, and establish

the necessary technical and organizational measures to safeguard the rights and freedoms of the data subjects and research participants.

REFERENCES

[1] Charter of Fundamental Rights of the European Union available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT (accessed on 25/04/2023)
[2] Charter of Fundamental Rights of the European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT (accessed on 02/06/2023)
[3] Data Protection Act 98, available at https://www.legislation.gov.uk/ukpga/1998/29/contents (accessed on 02/06/2021)
[4] Data Protection in Turkey, available at https://www.kvkk.gov.tr/Icerik/5389/Data-Protection-in-Turkey (accessed on 02/06/2023)
[5] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L0680 (accessed on 25/04/2023)
[6] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), available at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058 (accessed on 25/04/2023)
[7] H2020 Program Guidance How to complete your ethics self-assessment, available at https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf (accessed on 25/04/2023)
[8] Horizon 2020 - Regulation of Establishment: Ethical principles (Article 19), available at https://ec.europa.eu/research/participants/data/ref/h2020/legal_basis/fp/h2020-eu-establact_en.pdf#page=11 (accessed on 22/03/2021)
[9] Horizon 2020 Rules for Participation: Ethics Reviews (Article 14), available at https://ec.europa.eu/research/participants/data/ref/h2020/legal_basis/rules_participation/h2020-rules-participation_en.pdf#page=10 (accessed on 25/04/2023)
[10] International Convention of Human Rights and Fundamental Freedoms (Article 7 - protection of private and family life, home and communication and Article 8 – protection of personal data), available at https://www.echr.coe.int/documents/convention_eng.pdf (accessed on 02/06/2021)
[11] Model Grant Agreement: Ethics (Article 34), available at https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/amga/h2020-amga_en.pdf (accessed on 24/02/2023)
[12] Regulation 2016/679 of the European Parliament and of the Council of April 27th 2016 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data thus repealing Directive 95/46/EC, HTTPS://EUR-LEX.EUROPA.EU/LEGAL-CONTENT/EN/TXT/PDF/?URI=CELEX:32016R0679 (accessed on 02/05/2023)
[13] Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), available at HTTPS://EUR-LEX.EUROPA.EU/LEGAL-CONTENT/EN/TXT/PDF/?URI=CELEX:32016R0679 (accessed on 25/02/2023)
[14] The European Code of Conduct for Research Integrity, Available at https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/european-code-of-conduct-for-research-integrity_horizon_en.pdf (accessed on 25/02/2023)

ANNEX I

DATA PROCESS IMPACT ASSESSMENT (DPIA) OF THE LUMINOUS PROJECT

DPIAs for each pilot are in progress and the status of each Pilot's DPIA is provided below with a plan to provide the final versions of the DPIAs for each pilot at the Annex of D6.1, D6.2 and D6.3 respectively for each pilot.

LUMINOUS
LANGUAGE AUGMENTATION
FOR HUMANVERSE

Data Protection Impact Assessment (DPIA) Pilot [1] TBD Annex of D6.1

This template follows the process set out in our DPIA guidance, and you should read it alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

Start to fill out the template at the beginning of any major project involving the use of personal data, or if you are making a significant change to an existing process. Integrate the final outcomes back into your project plan.

10 STEP 1: IDENTIFY THE NEED FOR A DPIA.

LUMINOUS aims to contribute towards the creation of the next generation of Language Augmented XR systems and applications, where natural language-based communication and Large Language Models redefine the future interaction with novel extended reality (XR) technology and enhances understanding of the users' situation and environment even in situations that are encountered for the first time. The Main Objective is the creation of an integrated language-augmented multimodal platform that adapts to individual, not predefined user needs and unseen environments. This will enable future XR users to interact fluently with their environment while having instant access to constantly updated global as well as domain-specific knowledge sources to accomplish novel tasks. In this direction, we aim to exploit Large Language Models (LLMs) for efficient generalisation over unseen situations and objects with effective means of communication supported by novel XR components.

The need for a Data Protection Impact Assessment (DPIA) arises from the handling of sensitive data from a vulnerable population, in particular adults with neurological damage.

11 STEP 2: DESCRIBE THE PROCESSING.

Describe the nature of the processing:

We will include hospitalized patients, as well as healthy participants, having agreed to participate in the research studies. All participants for the study will be provided a participant information sheet and a consent form describing the study and providing sufficient information for participant to make an informed decision about their participation in the study. Each participant will be informed that the participation in the study is voluntary and that he/she may withdraw from the study at any time and that withdrawal of consent will not affect his or her subsequent medical assistance and treatment. A copy of the signed informed consent will be given to the study participant. The consent form will be retained as part of the study records, for ten years, in a locked drawer.
Irrespectively of the data type, each source of data will only be identifiable by a unique patient code. To reduce the risk of loss of privacy, the correspondence key linking this code to the participants' names will be stored only in printed form in a locked drawer.
Paper and pencil data consist of neuropsychological tests and questionnaires. All paper source (coded) data will be kept in locked drawers for ten years after the last publication related to this study.
Electronic CRF are registered on REDCap, a secure web-based application designed to support data capture for research studies (Harris, 2009), providing 1) an intuitive interface for validated data entry; 2) audit trails for tracking data manipulation and export procedures; 3) automated export procedures for seamless data downloads to common statistical packages; and 4) procedures for importing data from external sources. Several questionnaires are filled in directly on REDCap. Relevant coded results from tests/questionnaires are transcribed to REDCap, by hand for paper and pencil versions and by copy/pasting for electronic versions, and formatted accordingly for subsequent statistical analyses. In addition, all electronic CRF will be copied to secured and password-protected servers located at Sponsor facilities.
See the attached data flow diagram for further details.
The planned studies have been identified as low-risk studies. See risk assessment report attached.

Describe the scope of the processing:
The data collected will be basically personal data and they will not include special category or criminal offence data. In particular, source data is all information in original patient records, questionnaires, clinical observations, and other recorded activities acquired during the study, e.g. audiovisual recordings. They take one of two forms: paper and pencil or electronic. Data generated by the computer-based tests and data generated by the VR-based programs (e.g. game performance, time spent in each activity, movement data, eye tracking data, list and parameters of activities) are recorded in CSV and JSON files locally. After these 10 years, all data will be definitively erased and destroyed.
A total of 20 acquired brain injury patients in Switzerland & the UK will be involved in the co-design & evaluation of the system.

Describe the context of the processing:
Data will be collected from acquired brain injury patients and healthcare professionals by researchers from the involved partners. They will be in control of their own data in accordance with current national regulations, which provide for the possibility to delete their data, among other things, at any time.
Clinical study protocols will be approved by the corresponding Ethics Committees.

Describe the purposes of the processing:
Including patients with cognitive deficits due to stroke is necessary to obtain useful evidence on specific benefits that our rehabilitation training may have. Audios and videos recordings will be made during several assessment and training sessions to determine if, and how, sessions are titrated to the patient's needs, by evaluating the interactions patients/therapists in relation with the performances of the patients during the training and assessments, and the outcome of the rehabilitation training.
The population of stroke patients included in this study are adults at subacute and chronic stages post-stroke with capacity to give informed consent. Emergency patients with acute stroke are excluded. Other vulnerable persons such as children, adolescents, pregnant women or embryos / foetuses are also excluded.

12 STEP 3: CONSULTATION PROCESS

Consider how to consult with relevant stakeholders:

Pseudoanonymized (coded) data will be shared with selected project partners involved in the pilot, and only on a need basis for research activities related to the project. Already identified partners include CHUV, UK, MindMaze, DFKI, EHU and VICOMTECH.
Data sharing agreements among involved partners of the consortium are in place.

13 STEP 4: ASSESS NECESSITY AND PROPORTIONALITY

Describe compliance and proportionality measures:

We will collect feedback from the people involved at different phases of the studies: at baseline, during the training program, and after completion of the study.
The key personnel directly involved in the data collection have received extensive training in the design and conduct of research with human subjects and are well acquainted with the standards of good clinical practice. Furthermore, they have gained considerable experience in working with human subjects through several years of research. Students who will assist with data acquisition will be under the supervision of at least one of the key personnel. A Standard Operation Procedure (SOP) will be put in place. For quality assurance of the studies, monitoring visits will be made.

All involved partners constantly review, audit and update their technologies, processes, and practices designed to protect networks, computers, programs, and data from unauthorized access or damage. They do regular staff training, regarding the best practices and procedures related to cyber-security.

14 STEP 5: IDENTIFY AND ASSESS RISKS.

Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**

15 STEP 6: IDENTIFY MEASURES TO REDUCE RISK

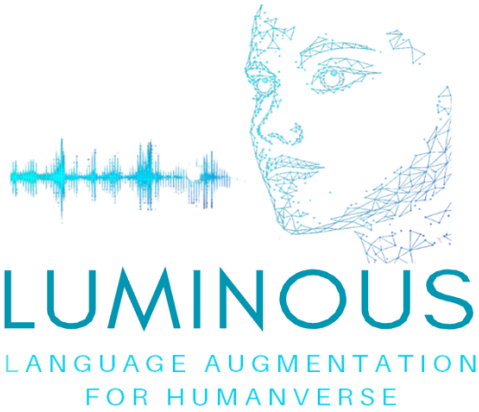
Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5

CHUV: Even though no medium-high risks were identified in step 5, EUN have foreseen measures to reduce the risks further. They are enlisted in the risk assessment report attached.

Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**

16 STEP 7: SIGN OFF AND RECORD OUTCOMES

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA



Data Protection Impact Assessment (DPIA) Pilot [2] Work in Progress TBD Annex of D6.2

This template follows the process set out in our DPIA guidance, and you should read it alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.
Start to fill out the template at the beginning of any major project involving the use of personal data, or if you are making a significant change to an existing process. Integrate the final outcomes back into your project plan.

Step 1: Identify the need for a DPIA.

Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA. LUMINOUS aims to contribute towards the creation of the next generation of Language Augmented XR systems and applications, where natural language-based communication and Large Language Models redefine the future interaction with novel extended reality (XR) technology and enhances understanding of the users' situation and environment even in situations that are encountered for the first time. The Main Objective is the creation of an integrated language-augmented multimodal platform that adapts to individual, not predefined user needs and unseen environments. This will enable future XR users to interact fluently with their environment while having instant access to constantly updated global as well as domain-specific knowledge sources to accomplish novel tasks. Such capabilities can have an unimaginable impact on future distance learning, training, entertainment, or provision of remote health services. In this direction, we aim to exploit Large Language Models (LLMs) for efficient generalisation over unseen situations and objects with effective means of communication supported by novel XR components. The LLM, in our vision, behaves like an oracle for describing novel tasks on user demand. These are then communicated through a speech interface and/or through an Avatar (e.g., Coach/Teacher) in terms of different visual aids and procedural steps for the accomplishment of the task. The need for a Data Protection Impact Assessment (DPIA) arises from the project's integration of language processing technologies, which may involve the handling of sensitive data and necessitates a comprehensive evaluation of potential privacy and security risks.

Step 2: Describe the processing.

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or another way of describing data flows. What types of processing identified as likely high risk are involved?

We will collect data of all volunteers taking part at Pilot 2 via company email directed to the stakeholders. We will store data in LUDUS TECH S.L. according to national law and ISO 27001, following our information classification policy.

All personal identifiable data collected during recruitment will remain and will be in the possession of LUDUS TECH S.L. and will be exclusively shared with the members of the Luminous project team.

Refer to Annex 7 (Data flow Diagram).

Considering that we will not take sensible data, there are very low risks connected to the sharing of data. There is minimal risk to participants in taking part in this research project. The LUMINOUS project follows the high ethical guidelines and standards required for EU HORIZON-CL4-2023-HUMAN-01-21 — Next Generation eXtended Reality (RIA) Project.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

The data collected will be basically personal data and they will not include special category or criminal offence data. The data will be collected from January 2026 to June 2026. We will collect those data trough:

1. Invitation acceptance (mail)
2. Consent form
3. Pilot participant datasheet
4. User details
5. Evaluation form

They will be used during the whole duration of the pilot, and we will keep them according to national law and ISO 27001. The data will cover only the European geographical area.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

The people we will prioritise to participate in the pilot will be selected from among our clients or organisations with whom we have previously carried out projects.
They will be in control of their own data in accordance with current national regulations, which provide for the possibility to delete their data, among other things, at any time.
In all cases the data will belong to persons of legal age and will follow the standards set by ISO 27001.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing for you, and more broadly?
The ultimate goal of pilot 3 is the validation of an LLM system in an XR training environment as an enhancement of the experience in terms of immersiveness, personalisation, dynamism and efficiency. No direct effect on the participants is foreseen beyond being a potential future user of the technology. There are no direct benefits related to the treatment. Only the benefit related to the technological advancement.

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts? We will collect feedback from the people involved on two occasions before and after the LLM implementation applied to the platform. It is not foreseen to involve anything other than the internal LUDUS expert in GDPR and ISO 27001.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers? The whole process will be based on existing national and international legislation and ISO 27001.

Step 5: Identify and assess risks.

Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5

EUN: Even though no medium-high risks were identified in step 5, EUN have foreseen measures to reduce the risks further. They are enlisted below:

Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**

Step 7: Sign off and record outcomes

Item	**Name/date**	**Notes**
Measures approved by:	Mikel Cearsolo Cabrejas (CEO)	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Mikel Cearsolo Cabrejas (CEO)	If accepting any residual high risk, consult the ICO before going ahead

DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA

Data Protection Impact Assessment (DPIA) Pilot [3] Work in Progress TBD Annex of D6.3

This template follows the process set out in our DPIA guidance, and you should read it alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.
Start to fill out the template at the beginning of any major project involving the use of personal data, or if you are making a significant change to an existing process. Integrate the final outcomes back into your project plan.

Step 1: Identify the need for a DPIA.

Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA. LUMINOUS aims to contribute towards the creation of the next generation of Language Augmented XR systems and applications, where natural language-based communication and Large Language Models redefine the future interaction with novel extended reality (XR) technology and enhances understanding of the users' situation and environment even in situations that are encountered for the first time. The Main Objective is the creation of an integrated language-augmented multimodal platform that adapts to individual, not predefined user needs and unseen environments. This will enable future XR users to interact fluently with their environment while having instant access to constantly updated global as well as domain-specific knowledge sources to accomplish novel tasks. Such capabilities can have an unimaginable impact on future distance learning, training, entertainment, or provision of remote health services. In this direction, we aim to exploit Large Language Models (LLMs) for efficient generalisation over unseen situations and objects with effective means of communication supported by novel XR components. The LLM, in our vision, behaves like an oracle for describing novel tasks on user demand. These are then communicated through a speech interface and/or through an Avatar (e.g., Coach/Teacher) in terms of different visual aids and procedural steps for the accomplishment of the task. The need for a Data Protection Impact Assessment (DPIA) arises from the project's integration of language processing technologies, which may involve the handling of sensitive data and necessitates a comprehensive evaluation of potential privacy and security risks.

Step 2: Describe the processing.

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or another way of describing data flows. What types of processing identified as likely high risk are involved?

We will collect data of all designers via company email directed to the stakeholders. We will store data in Mindesk's server, and it will be automatically deleted within 1 year from the end of the project.
The data source will be the BIM files shared by the stakeholders (designers, architects and engineers).

All personal identifiable data collected during recruitment will remain and will be in the possession of MINDESK and will be exclusively shared with the members of the Luminous project team.

Refer to Annex 7 (Data flow Diagram).

Considering that we will not take sensible data, there are very low risks connected to the sharing of data. There is minimal risk to participants in taking part in this research project. The LUMINOUS project follows the high ethical guidelines and standards required for EU HORIZON-CL4-2023-HUMAN-01-21 — Next Generation eXtended Reality (RIA) Project.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?
The data collected will be BIM/CAD/CAE/3D files and they will not include special category or criminal offence data.
The data will be collected from June 2024 to June 2026. Generally, we will collect 2 assets (BIM/CAD/CAE/3D files) from each stakeholder (up to 10 designers/engineers). They will be used during the whole duration of the project, and we will keep them until 1 year from the project's end. The data will cover only the European geographical area.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?
The individuals that will share with us their data set data set are our customers. They will have the whole control considering that they decide quality and quantity of data. In case they may withdraw at any time, and do not need to provide a reason and with no disadvantage.
They were totally well informed about the usage of their data (they will sign a specific DESIGNER INFORMATION).
The context does not include children or other vulnerable groups and privacy related data; there are not current issues of public concern and we have not a signed up to any approved code of conduct or certification scheme.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing for you, and more broadly?
The mail objective of accessing this dataset it to have materials for training LLM developed in the previous WP. The individuals will not be affected.

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

We will contact stakeholders on a monthly base. No one else will be involved, we are at the same time DC and DP. Given that we are more involved in the intellectual property area instead of personal privacy, we have no plans to consult external security expert.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers? Lawful basis is GDPR. We can confirm that the processing achieves our purpose. Nowadays we do not have another way to get the same outcome. About function creep, we only act as a proxy for data sources; about data quality and minimisation, we deal with third parties' dataset, and we will not share the original received files. Mindesk will make designers sign the information called “Professional Designers’ Information for the Luminous Pilot 3 Project” and will help to support their rights for the duration of the project. Data transfers are allowed only to registered users.

Step 5: Identify and assess risks.

Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Given that we are more involved in the intellectual property area instead of personal privacy, our pilot will not have impact on individuals.			

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5

No medium-high risks were identified in step 5.

Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**

Step 7: Sign off and record outcomes

Item	**Name/date**	**Notes**
Measures approved by:	Veronica Zennaro	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Veronica Zennaro	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	NA	DPO should advise on compliance, step 6 measures

		and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:	NA	If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:	NA	If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will be kept under review by:	NA	The DPO should also review ongoing compliance with DPIA