



D1.4 Data Management Plan (v3)

Deliverable No.	D1.4	Due Date	28/02/2025
Description	The final Data Management Plan provides the main principles, as well as ethical and data protection strategies adopted within the project regarding the data management, knowledge and IPR issues. It also includes the data management strategies of each consortium partner and pilots. This document presents the results of a living process carried out during the lifetime of the project, and which reflected the changes that took place at a project level and at the pilots' level.		
Type	ORDP	Dissemination Level	Public
Work Package No.	WP1	Work Package Title	Project Management and Coordination
Version	1.0	Status	Final



Authors

Name and surname	Partner name	e-mail
Adrian Quesada Rodriguez	UDGA	aguesada@udgalliance.org
Andre Cardozo Sarli	UDGA	acsarli@udgalliance.org
Renata Radocz	UDGA	rradocz@udgalliance.org
Vasiliki Tsiompanidou	UDGA	vtsiompanidou@udgalliance.org
Ana María Pacheco Huamani	UDGA	admin@udgalliance.org
Vasileios Lolis	CERTH	vaslwlis@iti.gr
Matthew Salanitro	CUB	matthew.salanitro@charite.de
Lorenzo Mucchi	MedICT	lorenzo.mucchi@unifi.it
Daphne Plati	FORTH	daphni.plati@gmail.com
Andres Iborra Martin	INETUM	andres.iborra-martin@inetum.com
Gisela Hagmair	MINDS SPARKS &	gisela.hagmair@mindsandsparks.org
Paula Currás	MDT	paula.curras@medtornic.com
Alba Hernández	MDT	alba.hernandez@medtronic.com
Francesco Agnoloni	MEDEA	project@medeaproject.eu
Joanna Orłowska	MUL	joanna.orłowska@umed.lodz.pl
Pilar Sala	MYS	psala@mysphera.com
Stephan Nijssen	Phillips	stephan.nijssen@philips.com
Raquel Juliá Ros	Robotnik	rjulia@robotnik.es
Víctor Solaz Estevan	Robotnik	vsolaz@robotnik.es
Paula Algarín	SAS	paula.algarin@juntadeandalucia.es
María Luaces	SERMAS	mluaces@salud.madrid.org
Jorge Nieto	SERMAS	jnietov@salud.madrid.org
Laura Llorente	SERMAS	lllorentes@salud.madrid.org
Gastone Ciuti	SSSA	gastone.ciuti@santannapisa.it
Lampis Papakostas	THL	lampis.papakostas@twi.gr

Name and surname	Partner name	e-mail
Giuseppe Fico	UPM	gfico@lst.tfo.upm.es
Leandro Pecchia	UOW	l.pecchia@warwick.ac.uk
Nevio Luigi Tagliamonte	UCBM	n.tagliamonte@unicampus.it
Saskia Haitjema	UMCU	s.haitjema@umcutrecht.nl

History

Date	Version	Change
11/01/2024	0.1	Creation of initial draft
01/01/2025	0.2	Finalization of structure and general content
01/04/2025	0.3	Last questionnaire answer received. Deliverable submission to peer review
02/04/2025	1.0	Peer review results integrated, deliverable submitted

Key data

Keywords	Data; Data Protection; Data Management; FAIR Data; IPR; Ethics; Privacy
Lead Editor	Adrian Quesada Rodriguez (UDGA)
Internal Reviewer(s)	FORTH, CERTH

Abstract

This document presents the final instance of the ODIN Data Management Plan (DMP) showcasing the aggregated results of the partners data management activities. This deliverable is the third and final version of the DMP. This document identifies the data that was generated during the project's execution, alongside data for potential use beyond the scope and time of ODIN. This report also identifies Intellectual Property practices and outcomes within the scope of data management practices. This document is accompanied by a confidential annex (available upon request) which includes the direct inputs provided by all partners to the DMP.

Statement of originality

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

Acronyms

DMP Data Management Plan

DoA Description of Action

DPIA Data Protection Impact Assessment

DPO Data Protection Officer

EDPS European Data Protection Supervisor

EEA European Economic Area

EU European Union

GDPR General Data Protection Regulation

GPL General Public Licence

FLOSS Free/Libre and Open Source Software

IoT Internet of Things

IPR Intellectual Property Rights

LSPs Large Scale Pilots

PS Pilot Site

WP Work Package

Table of contents

ACRONYMS.....	5
TABLE OF CONTENTS	6
TABLE OF FIGURES	7
TABLE OF TABLES.....	8
EXECUTIVE SUMMARY	9
1 INTRODUCTION	10
1.1 THE ODIN PROJECT	10
1.2 ABOUT THIS DELIVERABLE.....	11
2 DATA SUMMARY	12
2.1 HIGH-LEVEL OVERVIEW OF DATA GOVERNANCE WITHIN ODIN	12
2.2 TYPES AND FORMATS OF DATASETS.....	16
2.3 DATA STORAGE MANAGEMENT AND RETENTION.....	27
3 FAIR PRINCIPLES.....	31
3.1 FINDABILITY	31
3.2 ACCESSIBILITY	33
3.3 INTEROPERABILITY	37
3.4 REUSABILITY	39
4 ETHICS, DATA PROTECTION AND SECURITY CONSIDERATIONS	41
4.1 ETHICAL PRINCIPLES.....	41
4.2 CONSENT FORMS	42
4.3 DATA PROTECTION PRINCIPLES	43
4.4 CONTROLLER IDENTIFICATION AND INITIAL INSTRUCTION DEFINITION	44
4.5 TECHNICAL AND ORGANISATIONAL MEASURES	45
4.6 DATA SUBJECT RIGHTS	49
4.7 DATA PROTECTION OFFICERS (DPOs)	50
5 INTELLECTUAL PROPERTY RIGHTS	52
5.1 INTELLECTUAL PROPERTY RIGHTS WITHIN ODIN.....	52
6 CONCLUSION	56
APPENDIX A DATA MANAGEMENT QUESTIONNAIRE.....	57
APPENDIX B QUESTIONNAIRE RESPONSES FROM THE PARTNERS.....	62

Table of Figures

<i>FIGURE 1: THE POSITION OF D1.2 IN ODIN MANAGEMENT</i>	10
<i>FIGURE 2: ODIN WORK PACKAGE DISTRIBUTION</i>	12
<i>FIGURE 3 ODIN STAKEHOLDER MAPPING</i>	13
<i>FIGURE 4: HIGH-LEVEL REPRESENTATION OF ODIN INFORMATION FLOWS</i>	14
<i>FIGURE 5: ODIN SIMPLIFIED DATA FLOW OVERVIEW</i>	15

Table of tables

TABLE 1 ODIN DATASET SUMMARY	21
TABLE 2 OVERVIEW OF DATA GENERATED BY ODIN PARTNERS	27
TABLE 3 DATA STORAGE MANAGEMENT & RETENTION.....	30
TABLE 4 FINDABILITY APPROACH PER PROJECT PARTNER.....	33
TABLE 5 ACCESSIBILITY APPROACH PER PROJECT PARTNER	37
TABLE 6 INTEROPERABILITY APPROACH PER PROJECT PARTNER	39
TABLE 7 REUSABILITY APPROACH PER PROJECT PARTNER	40
TABLE 9 TECHNICAL AND ORGANIZATIONAL MEASURES FOR COMPLIANCES.....	49
TABLE 8 CONTACT PERSON AND DPO IDENTIFICATION PER PARTNER	51
TABLE 10 PARTNERS BACKGROUND AND FOREGROUND IPR	54

Executive Summary

The current document presents the final iteration of the Data Management Plan (DMP) designated to the partners of the ODIN project for their data processing-related activities, as well as for the data processing activities in the different hospital use cases (pilots).

This document addresses the Data Governance and handling of personal and sensitive data during the project outlining what types of data have been generated and used, if and how it was shared and made accessible internally and, after the duration of the project, externally for verification and re-use. It explains how partners stored and protected data, considering, in particular, ethical, privacy, and security issues. All findings are based on the answers provided by the partners to dedicated Data Management Questionnaires.

This DMP covers the entire research data life cycle and is consistent with exploitation and Intellectual Property Rights (IPR) requirements, while at the same time respecting FAIR (Findable, Accessible, Interoperable and Reusable) data principles. The information it presents is closely aligned with the ethics, privacy and legal framework generated by WP8 and with the sustainability and project legacy activities undertaken by WP9.

1 Introduction

1.1 The Odin Project

The ODIN project focuses on identified hospitals’ critical challenges which were addressed by combining robotics, Internet of Things (IoT) and artificial intelligence (AI) to empower workers, medical locations, logistics and interaction with the hospital’s territory. According to their expertise, the project’s consortium has divided its management responsibilities into the areas showcased below in *Figure 1*. ODIN’s aspiration to enhance healthcare for patients, leveraging on AI, robotics, emerging techniques, approaches and methods results in critical ethical and data protection issues, such as potential harms to autonomy, dignity, privacy, moral responsibility, equality, transparency, safety, accountability, and liability. To meaningfully address these challenges and develop a commonly followed strategy for risk mitigation and compliance, the project management and coordination work package (WP1) has dedicated a task (T1.4) to Data Management and Ethics.

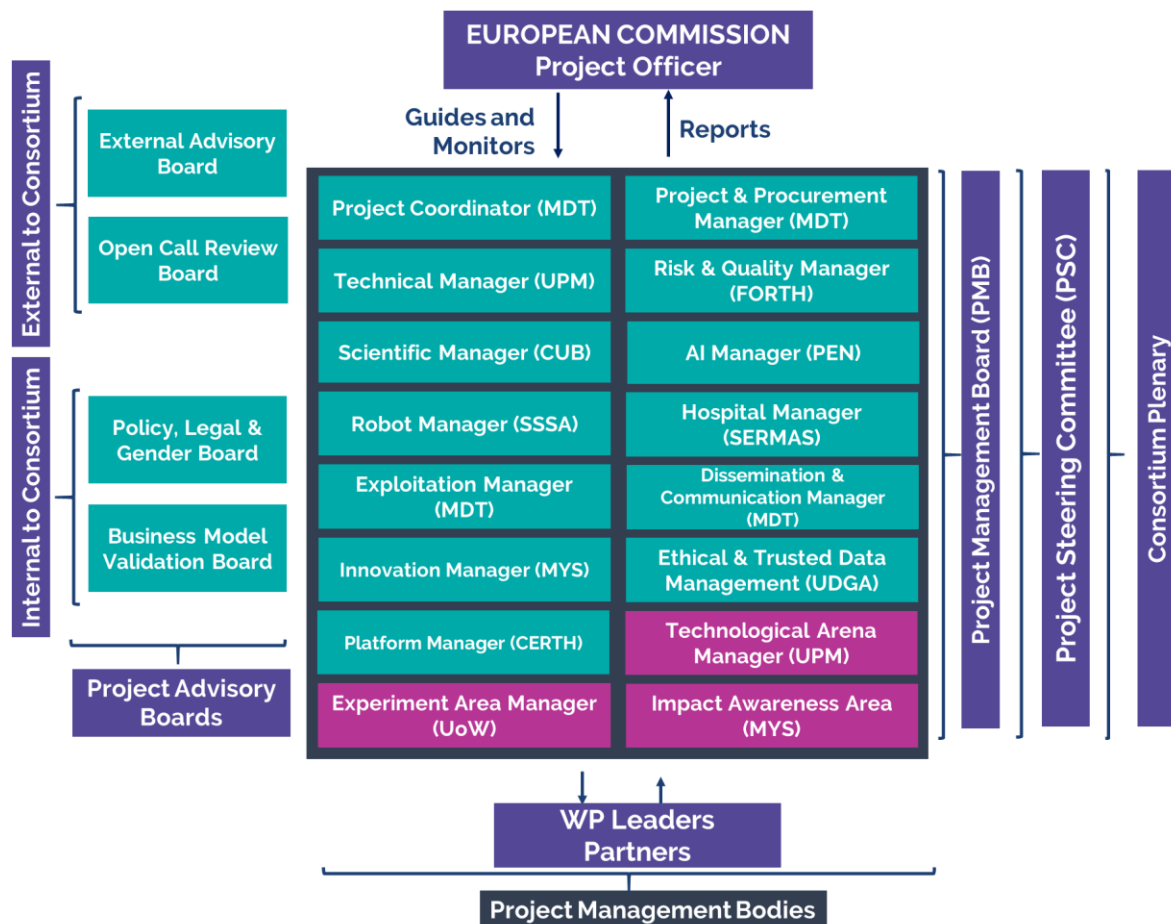


Figure 1: The position of D1.2 in ODIN Management

1.2 About this Deliverable

The European Commission defines¹ Data Management Plans (DMPs) as key elements of good data management. A DMP should describe the data management life cycle for the data to be collected, processed and/or generated. As part of making research data findable, accessible, interoperable and re-usable (FAIR), a DMP should include information on:

- The handling of research data during & after the end of the project;
- What data will be collected, processed and/or generated;
- Which methodology & standards will be applied;
- Whether data will be shared/made open access;
- How data will be curated & preserved (including after the end of the project).

The earlier versions of Deliverable D1.2 functioned as a plan for ethical and GDPR-compliant data management among the ODIN consortium. It is a product of task T1.4 “Data Management and Ethics” and fulfilled the purpose of summarizing the data to be generated within the project and the data processing activities. The current deliverable is the final version of the plan. It was a recurrent live deliverable, which has constantly been updated according to partners’ inputs and, thus, reflected on any changes regarding data generation, usage, processing, storage, and ethical management.

¹ https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-data-management/data-management_en.htm.

2 Data Summary

Data in the context of ODIN was collected at the project level by non-pilot owners and at the pilots’ level by pilot-owners. In the context of ODIN, data was collected for production of deliverables, for training AI algorithms (and, consequently, robots), for initial analysis of requirements and use-case catalogue production, as well as for model validation. The following section presents various tables and figures showcasing the characteristics of the various datasets used in the scope of the project by its partners. The established interconnections would facilitate data mapping, which is particularly relevant in terms of data sharing within the consortium. Detailed information about the generated data by each partner is provided in the submitted Data Management Questionnaires

2.1 High-Level Overview of Data Governance within ODIN

The ODIN project’s commitment to interdisciplinary research has led to the development of a distributed data ecosystem where consortium members were deeply engaged in the diverse data processing activities (from data compilation, creation, processing, analysis, visualization, storage and deletion). Data has been sourced both from background datasets facilitated by its project partners, and through the multiple activities undertaken by the ODIN pilot sites, which gathered clinical, technical, research and organizational information to ensure the project’s success.

As defined in the Grant Agreement, management of data within the project has been aligned with the partners’ roles within the project and their involvement and need to access or process data as part of the diverse tasks they lead. The figure below provides a high-level overview of the distribution of responsibilities and tasks among the different work packages.

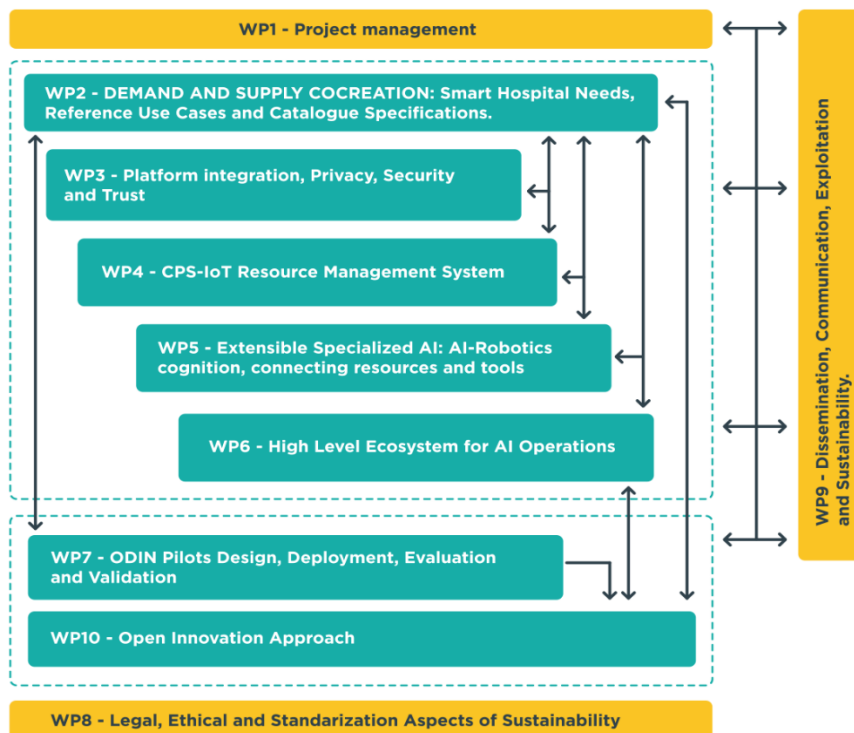


Figure 2: ODIN Work Package Distribution

In line with this approach, each partner, including pilot owners, were originally requested to clarify *who is in charge of what*, and more specifically, who are the data controller(s) and the data

processor(s) and are there established joint controllerships. Pilot owners needed to clarify and explicitly define how their work is organized, to know and communicate what personal data are/will be collected and thus to allow a data flow mapping, as is reported of the previous iteration of the present deliverable. In order to facilitate the identification of the roles of the partners, the first Data Management Plan had already provided a guide to help partners determine what their role in the personal data processing is, and what obligations ensue.

For the definition of the data processing activities, partners were provided with Data Management Questionnaires (Appendix A). As the work on local and general data management plans was always understood as an ongoing work, the exercise in data mapping continued over the course of the project.

In the context of the ODIN project, personal data has been processed with the aim of working on solutions with technologies for the better quality of life and (health) care. The purpose of all data processing activities was fundamentally aligned with the dispositions of the Grant Agreement to ensure and maximize the management of stakeholder participation in the project.

The outcomes of T2.1 “Co-creation strategy, stakeholders’ definition and mapping” of Work Package 2 complemented the identification process of the roles and obligations within the consortium. The following figure offers a comprehensive map of the different clusters in the consortium and partners could determine, according to their expertise, to which of the “circles” they belong, what are other stakeholders with similar profiles and explore the dimensions of the work related to their activities.

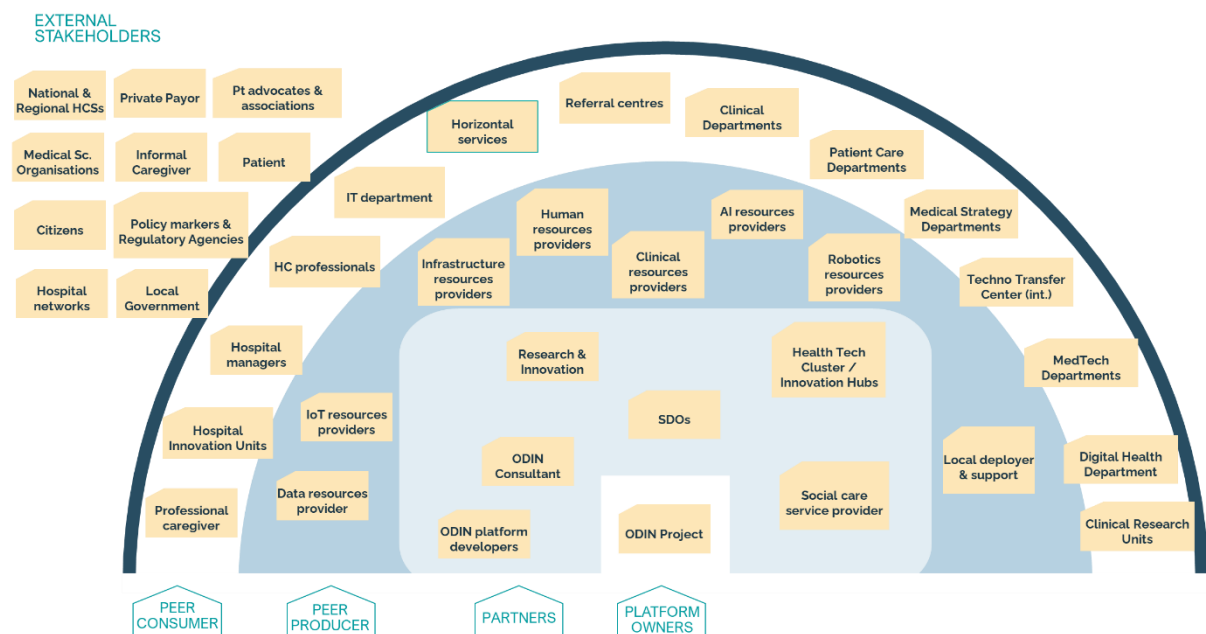


Figure 3 ODIN Stakeholder mapping

As showcased in Figure 3, as the project evolved to encompass additional layers of stakeholders, data was increasingly processed to ensure the successful completion of ODIN’s own dissemination, communication and exploitation activities. All these activities were performed in tight coordination with the Project Coordination team and as defined by the contractual framework defined by the project’s Grant Agreement and Consortium Agreement.

The project dataflows in this context can be characterized as multi-directional, encompassing upstream (data collection and acquisition), midstream (processing, model training, validation), and downstream (evaluation, dissemination and reuse) components. Data was gathered through

various methodologies in close alignment with ethical and regulatory frameworks (see WP8 deliverables), and included a wide-range of sources, from clinical research outputs, sensor recordings, robotic system logs, surveys, interviews and questionnaires.

Figure 4 below presents the overarching information flow found within the ODIN platform and its various enablers/resources.

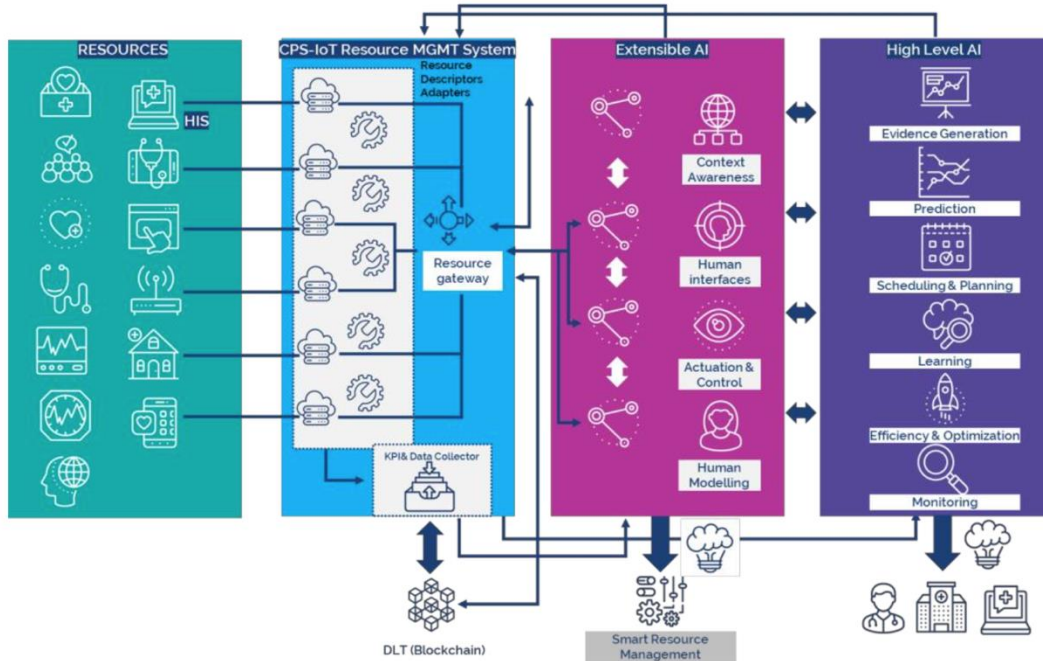


Figure 4: High-level representation of ODIN information flows

The figure below offers a simplified scheme of the data processing, storage, and retention flows followed across the project’s activities, including those related to communications and dissemination activities and ongoing exploitation and sustainability efforts.

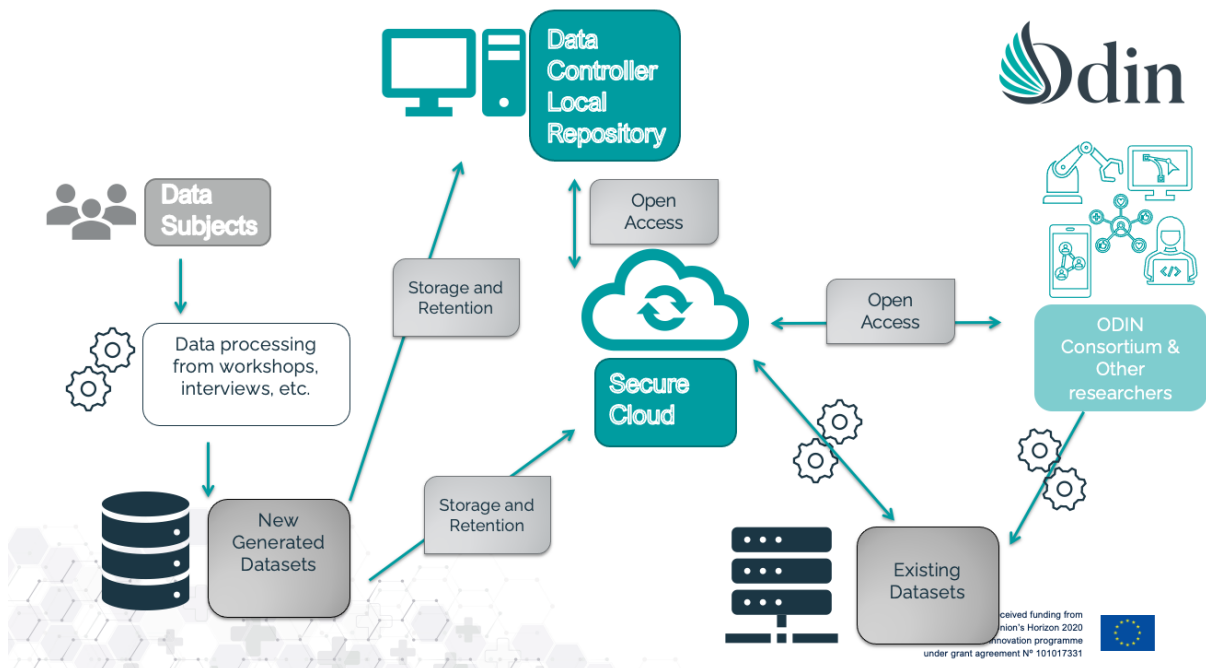


Figure 5: ODIN simplified data flow overview

As noted above, when addressing personal data (and the associated responsibilities pertaining data subject right compliance), ODIN pilot owners adopted the role of primary data controllers, with the capability and responsibility to define the means and purposes of processing at local level, as well as the potential dissemination avenues (and technical means) of collected data (in close collaboration with the consortium partners through dedicated monthly meetings). To meet the Grant Agreement’s objectives, consortium partners were granted with the opportunity to utilize anonymized or pseudonymized information (based on applicable ethical approval and contractual dispositions), to this end, data was stored in internal project repositories and secure institutional servers meeting relevant standards.

The project has sought to ensure interconnection through the integration of interoperable formats and semantic frameworks (like the ODIN ontology) which together ensure data exchange whilst maintaining privacy and contextual integrity. The project has adopted a comprehensive dissemination and communication strategy, which has led to the broad availability of its results whilst respecting scientific quality controls, and has sought to align with FAIR data principles as much as possible (and within the limitations of the sensitive data its partners have processed).

Lastly, the project has pursued various approaches to ensure the viability and sustainability of its results through the various exploitation-oriented actions performed by WP9. From a scientific point of view these efforts are reinforced through the specification of data retention strategies consistent with each partner’s legal and institutional framework (varying from short-term analytical periods to long term preservation strategies).

The harmonious way in which these efforts were achieved, and the close collaboration of the partners throughout this project have led to ongoing efforts to ensure the continuity of the project, its research objectives, and the associated data sharing and governance exercise it entails. These have been reflected in the proposal of a dedicated Memorandum of Understanding which considers data management priorities (and is reported in WP9’s deliverable on ODIN Project Legacy).

2.2 Types and formats of datasets

As part of the project activities, a diverse array of datasets has been gathered at project level by general partners and at the pilots’ level by pilot-owners. Diverse datasets were introduced to the project for production of deliverables, training AI algorithms (and, consequently, robots), initial analysis of requirements and use-case catalogue production, as well as for model validation. Within these contributed datasets, the following categories and formats can be generally identified:

- Clinical and health-related data: sleep records, patient monitoring information, diagnostic pathways, generally stored in formats like CSV, EDF and TXT.
- Multimedia and sensor outputs: photographs, video, and recordings of various monitoring and rehabilitation systems, commonly in JPEG and MP4 format.
- Operational and technical logs: including robot movement data, localization maps and platform usage metrics, found in structured formats like JSON, CSV and TXT.
- Survey and administrative data: such as consent forms, stakeholder questionnaires, legal self-assessments, usually stored in DOCX, XLSX and PDF.
- AI training datasets.

The table below presents a high-level overview of the partner-provided inputs to this section as defined in the answers to the Data Management Questionnaire (Appendix A) found in Appendix B to this deliverable.

Partner	Dataset Name	Description	Contains Personal Data	Purpose	Data Format	Storage Location
CERTH	Federated Learning Pilot Experiment data	Data used in federated learning pilot sent through blockchain	No	Pilot purposes only	Access request and federated component response formats	Initially on external hard disk, later uploaded to InfluxDB
CERTH	CUB DATASET	Health data and pseudoanonymized metadata from sleep recordings from patients	Yes (pseudonymized)	Research (sleep disorder diagnosis, sleep pattern analysis, visual analytics)	EDF (European Data Format)	Initially on external hard disk, later uploaded to InfluxDB

Partner	Dataset Name	Description	Contains Personal Data	Purpose	Data Format	Storage Location
CUB	ESADA Insomnia Ring data Robot and Camera data	Multiple datasets: ESADA (200-230 sleep apnea patients), Insomnia (64 patients), Ring data (~60 patients), Robot and Camera data	Yes (implied) re-identification risk analysis performed	Research (sleep disorder diagnosis, pattern analysis, visual analytics)	EDF and .txt for annotations, .CSV for Camera and Robot	Local at institute or with partners working on use cases
MedICT (UNIFI)	HTA-related KPIs dataset	Key Performance Indicators per RUC and pilot sites	No	HTA and Impact Assessment (WP7)	Tabular (.xlsx)	ODIN sharepoint repository
FORTH	Oxygen monitoring dataset created from Forth	Images of Forth employees wearing oxygen masks correctly or incorrectly	No	Develop AI-based models for Oxygen Monitoring UC	.jpeg images	Forth's server
FORTH	Oxygen monitoring dataset created from UCBM	Images from UCBM employees wearing oxygen masks correctly or incorrectly	No	Develop AI-based models for Oxygen Monitoring UC	.jpeg images	UCBM
FORTH	UCBM food image database	Food images with information (weight, calories, macronutrients)	No	Develop AI-based models for Malnutrition	.jpeg images, .xls file	UCBM and shared with Forth

Partner	Dataset Name	Description	Contains Personal Data	Purpose	Data Format	Storage Location
				Monitoring UC		
FORTH	UCBM rehabilitation videos	Videos of patients performing rehabilitation exercises	No	Develop AI-based models for Rehabilitation Monitoring UC	.mp4 videos	UCBM and shared with Forth
Robotnik (ROB)	Robot localization data	2D maps and associated software outputs	No (only sensitive: 2D maps of facilities)	Validate performance of developed KERS	CSV and TXT	Organized directories with consistent naming conventions
SAS	GetReady-ODIN	Patient monitoring data	Yes (PROMs, PREMs, demographic data, adherence data)	For the study	Electronic	Maela database and Metrics ODIN platform
INETUM	MS COCO	Multipurpose dataset with 125 classes	No	Training of AI algorithms	Images	N/A (uses open source data)
MINDS & SPARKS	Stakeholder collections	Contact data, email addresses	Yes	Targeted dissemination and communication activities	Spreadsheets (.xls/.xlsx, .csv)	Secured personal computers with password protection
MEDTRONIC	Get Ready ODIN PROJECT	Personal data processed through GetReady software	Yes (patient contact data, health info, HCP data)	Research project	Not specified (exported as CSV)	Software platform maintained by ATOS, hosted by OVH in France
MEDEA	HTA-related KPIs dataset	KPIs per RUC and pilot sites for	No	HTA and Impact Assessment	Tabular (.xlsx/.csv)	ODIN sharepoint repository

Partner	Dataset Name	Description	Contains Personal Data	Purpose	Data Format	Storage Location
		HTA assessment				
PHILLIPS	CUB Dataset	See CUB	See CUB	See CUB	See CUB	See CUB
SSSA	System Usability Questionnaire	Anonymous data from questionnaires	Yes (sex, birth date, professional role, but anonymous)	Assess system usability of HOSBOT	CSV	CBMLBox
SSSA	HOSBOT	Mapping of navigation environments, odometry data, state-machine statuses	No	Assess performance of HOSBOT	Environment maps (.pgm), odometry (.csv), others (.txt)	CBMLBox
SSSA	Human Modelling	Videos of environment at UPM	Yes (videos of people)	Assess performance of Human Modelling algorithm	mp4, csv, python scripts	CBMLBox, Google Drive
TWI Hellas	Robot Fleet Management Log	Metrics for Robot Fleet Management System	No	Measure performance of task allocation algorithm	CSV	ODIN Platform Server/Laptop, THL private Google Drive
UCBM	UCBM_pilot	Data from UCBM pilot activities	Yes	Meet inclusion criteria and study objectives	Not specified	Not specified
UCBM	UCBM_food_pictures	Pictures of food for Malnutrition Monitoring	No	Not explicitly stated	Not specified	Not specified

Partner	Dataset Name	Description	Contains Personal Data	Purpose	Data Format	Storage Location
UMCU	UCC CVRM – Informed Consent	Responses of patients	Yes (pseudonymised patient data)	Pilot (consent)	CSV	UMCU dataverse/archivemetica storage
UMCU	e-consent study	Responses of patients	Yes (pseudonymised patient data)	Pilot (e consent)	CSV	UMCU dataverse/archivemetica storage
UMCU	Trust Vignette study	Responses of patients	No	Pilot (Patient-Physician Trust)	CSV	the Utrecht University Yoda archive
UMCU	Odin UC3	diagnostic trajectories of patients undergoing CEA	Yes (pseudonymised)	Pilot (diagnostic trajectories)	CSV	Preferred Research Folder Structure of the UMCU
UMCU	Odin UC4	Data from first appointment of geriatrics patients	Yes (pseudonymised)	Pilot (Eligibility/check with CVRM learning healthcare system)	CSV	Preferred Research Folder Structure of the UMCU
UPM	Operational KPIs	Collection of operational KPIs to track pilot deployment	No	Pilot tracking	Excel	CBML Box
UPM	Metrics and Historic database	Collection of logs and system metrics	No	Platform and KER evaluation	Text and database	Google Drive
UPM	Consent Form IR Pilot	Collection of consent forms for IR Pilot participants	Yes (name and ID)	Collect consent for LL pilot	Paper	Local

Partner	Dataset Name	Description	Contains Personal Data	Purpose	Data Format	Storage Location
UPM	Consent Form Living Lab Pilot	Collection of consent forms for UPM-LL Pilot participants	Yes (name and ID)	Collect consent for LL pilot	Paper	Local
SERMA S	RUC B1 UC1 datasets	Multiple datasets including patient data, hospitalization data, and stent information	Yes (socio-demographic and clinical variables)	Produce datasets for RUC B1 UC1	Excel/CSV	Local computers, secure shared folder, dedicated server

Table 1 ODIN Dataset summary²

In addition to the previously described datasets, the following table presents the datasets which each partner has generated as part of their involvement in the diverse project work packages and tasks. Detailed information about the generated data by each partner is provided in the submitted Data Management Questionnaires (Appendix B).

Partner	Work Package/ Task	Asset	Type & Format
MDT	WP2, T2.1	Interviews 1:1 with hospitals	.docx, .pptx
MDT	WP2, T2.1	Requirements questionnaire	.xlsx
MDT	WP2, T2.1	Stakeholder mapping workshop	Miro board (online); .docx, .pptx
MDT	WP2, T2.5	Pilot Sites Legislation on Public Procurement	.docx
MDT	WP2, T2.5	Form to capture needs, requirements, and problems	.docx

² Some partners indicated that certain questions were not applicable to their role within the project, namely: MUL (Medical University of Lodz) MYS (Mysphera) & University of Warwick.

Partner	Work Package/ Task	Asset	Type & Format
		towards Public Procurement Processes	
MDT	WP2, T2.5	Public procurement form from suppliers	.docx
MDT	WP8, T8.2	A report summarising applicable standards to ODIN, and a standardisation and certification strategy, plus a sustainability plan, together with a general overview on the relevance of standardisation and certification to introduce the topic to Hospital partners	.docx, .ppt
MDT	WP9	Interviews 1:1 and workshops with hospitals and relevant partners to understand the needs for exploitation of project's results	Exploitation plan of each partner: .docx, .pdf, .xlsx
MDT	WP10, T10.	ODIN Community of Interest	ODIN Website, .pdf, .xlsx, .docx
MDT	WP10, T2.2	Focus Group on Public Procurement with hospitals	.docx, .pdf
MDT	WP10, T2.3	Focus Group on Public Procurement with suppliers	.docx, .pdf
MDT	WP10, T10.4	Open Call submission portal	ODIN Website, .pdf, .docx, .xlsx
CERTH	WP5, T5.2	Video format, RGB image format, Pointcloud format from depth sensors	either .mp4 or .avi, .png, and .pcd.
FORTH	WP6, T6.1, T6.2, T6.3	Pilot Data	JSON data types in either excel format, in SQL databases, in EHR systems, in xml format
UoW	WP3, WP6, WP7	Information referred to the pilots' representatives, their experiment definition and the procedure followed by each partner to obtain the ethical approval	.doc; .pdf; xcl

Partner	Work Package/ Task	Asset	Type & Format
SSSA	WP5	Data coming from cameras and used for human awareness, robot navigation, human detection and tracking, social interaction models, monitoring and security, human action and behavioural recognition, human-robot interaction, etc.	Data coming from sensors or HMLs (e.g., images); digital data
SSSA	WP5	Data coming from sensors for localization of devices and robots that could be transported by people or wearables for cognitive performance monitoring and user's state estimation (stress, cognitive load, sleep quality, etc.)	Data coming from sensors or HMLs (e.g., images); digital data
SSSA	WP5	Sensitive data of patients and workers that are transmitted/processed through robotic modules that come from human-machine interfaces installed in the robots (for accessing to services or registrations) or coming from the Hospital's ICT infrastructure (other WP's)	Data coming from sensors or HMLs (e.g., images); digital data
ROBOTNIK		Data related to the movement of the robot and its commands	JSON format
MYS	WP4	Technical requirements that are needed to achieve Use Case objectives from each Work Package. Opinions about the type of documentation and support service levels that partners can offer. Designs of the ODIN architecture.	Free text from datasheet surveys. Free text documentation and images of the designs.
THL	WP5, T5.3	Technical data related to robots' operation and status	Robotic data formats will be custom defined through the ROS

Partner	Work Package/ Task	Asset	Type & Format
			messaging and service interface (.msg and .srv file format)
PEN	WP6	Analytics and AI in specific clinical use cases to process de-identified patient data and relevant process and administrative data. The output of the work will be models.	Not defined yet.
UPM	WP2, T2.4	Participant data collected through interviews and workshops	Text documents
UPM	WP3, T3.3	User data collected for identity management (i.e., credentials)	JSON or another interoperable format
UPM	WP4, T4.6	Data related to metrics such as logs, usage stats of the platform	JSON or another interoperable format
UPM	WP5	Data related to interaction of users with social robots	JSON or another interoperable format
UPM	WP7, T7.1	Data from pilots collected through questionnaires	Text documents
UPM	WP10, T10.3	Data from open calls submissions (participant forms, project specification, etc.)	Digital format, not yet defined
UCBM	WP7	Robot data: robot data recorded during testing, debugging and verification of the developed software modules (e.g., positions, velocities, forces, torques, RGB-D camera data).	Possible format will include .csv or .txt.
UCBM	WP7	Physiological data: physiological data recorded during testing, debugging and verification of the developed software modules (e.g., electromyography, galvanic skin response, heart rate, respiration rate).	Possible format will include .csv or .txt.

Partner	Work Package/ Task	Asset	Type & Format
UCBM	WP5, WP7	Patient ID and HIS data: patient data (e.g., ID, pathologies, allergies, intolerances, diet) extracted from the HIS for testing, debugging and verification of the developed software modules.	Possible format will include: .xlsx or .json or .csv.
UMCU	WP7	UC3: Generation of patient data from patients using the Luscii app for monitoring	.cvs
SERMAS	WP7	UC1: Information concerning material and equipment consumptions and purchases for a yet to be defined medical procedure	CSV file
SERMAS	WP7	UC1: Data from patients who undergo the yet to be defined medical procedure	CSV file
SERMAS	WP7	UC2: Internal data from a robot used to transport materials from a storage room to an operation room	To be defined.
SERMAS	WP7	UC7: Video image of a hospital area (either the emergency service or a surgical area), geographical position of equipment and personnel/ patients (RFID)	Video files.
CUB	WP7, WP8, WP9	Questionnaires distributed to stakeholders, students, and pilot participants to collect medical data and economic data.	Text data on paper; .pdf, textual data from medical records; EDF format data from sleep recording equipment
MUL	WP7	Architectural data from the hospital administration	To be defined
MUL	WP7	IoT data from tagging devices	To be defined
MUL	WP7	Data related to clinical staff and patients, i.e., the final users of equipment and consumables	CSV Comma Separated Values, XLS Excel Spreadsheets

Partner	Work Package/ Task	Asset	Type & Format
MUL	WP7	EHR data, originating from the P1 EHR system, made available under nationwide P1 universal eHealth system, currently under implementation	SNOMED, ICD 10, ICD 9
M&S	WP9, T9.1 WP10, T10.1	Contact list	.xls/.xlsx, .csv
M&S	WP10, T10.1	Information on similar projects	.xls/.xlsx
M&S	WP10, T10.1	Data on supply and demand of ODIN related products	.xls/.xlsx
M&S	WP10, T10.1	Questionnaires for Trust building and Ecosystem enlargement	.xls/.xlsx
UDGA	WP1, T1.4	Questionnaires for information on partner data management activities	.docx; .pdf
UDGA	WP8, T8.3	Partner inputs on certification demand	.docx; .pdf
UDGA	WP8, T8.4	Partner inputs on data ethics for hospital procurement	.docx; .pdf
MEDEA	WP7, T7.2, T7.5, T7.7	Data referring to technological components provided by the partners; <ul style="list-style-type: none"> the viewpoints of top-managers, lead users (doctors, nurses, technical staff) and end-users (patients and relatives), including user experience, user acceptance, usability, ergonomics, safety and ethics aspects the impact on hospital management and cost effectiveness of the solutions according to specific identified KPIs 	.xlsx or .docx

Partner	Work Package/ Task	Asset	Type & Format
MEDEA	WP9, T9.2	Data for the PESTLE analysis to analyse events and trends in areas that commonly affect business operations and performance	.xlsx or .docx

Table 2 Overview of data generated by ODIN partners

2.3 Data Storage Management and Retention

As detailed in previous iterations of this deliverable, all datasets that contain personal or confidential information have been securely stored by responsible project partners, who were tasked with applying security updates and applicable technical and organizational measures required by data protection regulations. To support this action, at the beginning of the project (March 2021) a dedicated repository for project collaborative work was set up and best practices of data storage and handling were communicated to all project partners and team members.

Public-facing information was hosted on ODIN's public website (<https://www.odin-smarthospitals.eu>) where the following data and information has been made publicly available:

- General information about the project, its mission, objectives and impact;
- The participating consortium, including the ODIN ecosystem and information regarding its governance;
- Information on the Hospital Use Cases
- Project public deliverables;
- Webinars;
- Publications.

Non-public datasets, presentations, reports, scientific publications and other documentation containing sensitive or personal data were made accessible only by the consortium through its private repository (CBMLBox). Confidential deliverables have been made restricted to internal use and not available through public channels, as described in the Grant Agreement and Consortium Agreement.

Whenever a dataset was intended to be openly accessible, particularly the datasets containing personal information (e.g., interviews, pilots, focus groups), the DMP required anonymisation prior to release.

Project data was also stored in partners own facilities and servers. The storage time depends on the particular data but in general the rules are:

- **During the lifetime of the project:** the availability of and access to the data on the different servers has been ensured for as long as they are needed.
- **After the end of the project:** the project public website and CBMLBox will be maintained until the end of the project. Afterwards, whenever possible, the data from the ODIN platform will be anonymized and made available in accordance with the FAIR data principles. Dedicated discussions around how this process is to take place are ongoing

(particularly considering the MoU and project legacy activities) and are to consider, particularly, the sensitive nature of the data.

All project data, except for the public website, has been stored in password protected repositories and servers. The security strategy depends on the security policy of the partners in charge of these repositories and servers. Additional information on this point can be found in Appendix B.

Beyond the provisions outlined above, the table below presents the data storage, management and retention policy as declared by project partners.

Partner	Data Storage Management & Retention Policy
Robotnik	<p>Most of the data is stored inside the robot for internal algorithm optimization processes.</p> <p>There is data that is kept in only one work cycle of the robot and other data that will be kept during the pilot period.</p>
SERMAS	<p>The data was stored by SERMAS, in a server independent from the Hospital Clínico San Carlos network.</p> <p>The data will be kept for the complete duration of the ODIN project.</p>
MYSHERA	<p>MYSHERA stored the data in the Cloud available from ODIN project.</p> <p>The data will be stored “as long as it is needed for project purposes”.</p>
M&S	<p>Employees of MINDS & SPARKS GmbH stored the documents containing personal data locally on controlled secured, password protected personal computers, where only authorized access is allowed and to databases containing personal data, privacy by design techniques and encrypted file transfers.</p> <p>The data will be deleted three years after the end of the project.</p>
MEDTRONIC	<ul style="list-style-type: none"> • Data capture by ODIN’s website is stored in online servers • Miro board data in Miro tool’s servers • Documents were stored either in Medtronic’s internal servers/OneDrive folders or ODIN project’s repository (accessible to consortium). <p>The data will be kept during ODIN project’s duration and beyond, at least 5 years after the end of the project.</p>
CERTH	<p>Data was stored locally on at CERTH premises by responsible researchers assigned this task.</p> <p>In compliance with GDPR core principles of proportionality and minimization, data was processed and kept during the project.</p>
FORTH	<p>The data received from pilots was stored in their local repositories in order to ensure data privacy and protections. The current plan suggests that no data will be processed outside of the pilot site. Any data produced by FORTH will be stored in local repositories accessible only by FORTH personnel.</p>

Partner	Data Storage Management & Retention Policy
	Data was kept for the project period.
University of Warwick (UoW)	UoW stored data on the ODIN Project shared storage.
SSSA	<p>Data was centrally stored into the hospital's ICT infrastructure (mainly concerning WP3 and WP4).</p> <p>The aspect data retention does not concern WP5 and SSSA activities because data was not stored by SSSA, but was transmitted to the ODIN's ICT platform/infrastructure. Temporary dataset, used for local analysis, were frequently replaced with the new generated data flow.</p>
THL	The data was stored on a server or a laptop on-premise (TBDL) until the end of the project.
Philips Electronics Netherland BV (PEN)	<p>The data was stored at the pilot sites.</p> <p>PEN accessed data locally at pilot sites and nothing was transferred to PEN.</p>
UPM	<p>T2.4, T7.1, T10.3 stored the data using the cloud repository of the project (NextCloud).</p> <p>T3.3, T4.6 and WP5, data was stored at each pilot site of in a pilot cloud provider.</p> <p>Data will be kept for the time of the project.</p>
INETUM	There was no data collection, processing or sharing.
UCBM	<p>The data was available to the UCBM team for the development and clinical validation of the ODIN platform. It was strictly kept in closed archives and not connected to the network at UCBM.</p> <p>The data was collected, analysed and managed by UCBM for the entire duration of the ODIN project and only for its purposes. Once project tasks have been completed, the above mentioned repository will be managed as a long term data locker for project files and deliverables (duration to be defined).</p>
UMCU	<p>UMC Utrecht stored the study data on its secure servers protected by authorization.</p> <p>Data will be kept, according to Dutch law, for the period of 15 years.</p>
Charite (CUB)	The partner CHARITE stored the data on servers inside the hospital and inside the firewall protection of the hospital.

Partner	Data Storage Management & Retention Policy
	<p>The data collected will be kept for 10 years unless other regulations in Germany require a longer storage. Clinical study data need to be stored for 15 years according to good clinical practice regulations.</p> <p>Data is provided to partners with data sharing agreements that contains provisions requiring due diligence and proper data management. The data is shared in a dedicated and cryptographed hard data disk.</p>
<p>MUL</p>	<p>MUL stored the data in a dedicated Research Folder Structure for which authorization is secured using personal logins. Only pseudonymised data was stored there. The key is stored at the separate drive.</p> <p>The MUL IT centre was responsible for security of data in the data centre.</p> <p>The data will be available for at least 10 years.</p>
<p>UDGA</p>	<p>Datasets were stored in the ODIN’s repository (CMBLBox) and kept for the duration of the project.</p>
<p>MEDICT MEDEA</p>	<p>Data was only collected by reference of MEDEA personnel and was stored in the internal server of the company for the extent of the project.</p>

Table 3 Data Storage Management & Retention

3 FAIR Principles

In its FAIR Data Management Horizon 2020 Guidelines, the European Commission notes that “Good research data management is not a goal in itself, but rather the key conduit leading to knowledge discovery and innovation, and to subsequent data and knowledge integration and reuse”. Therefore, beneficiaries are explicitly encouraged to make their research data findable, accessibly, interoperable and reusable (FAIR).

3.1 Findability

According to this principle, metadata and data should be easy to find for both humans and computers. Machine-readable metadata are essential for automatic discovery of datasets and services. For publicly available datasets, publications and reports (deliverables), the ODIN consortium is encouraged to attach or apply a DOI or any other unique identifier. Additionally, all communication and dissemination materials must include the following metadata:

- European Union’s Horizon 2020 research and innovation programme letterhead
- Grant agreement No 101017331

For this, and as part of ODIN’s communication and dissemination activities, a folder with templates has been uploaded to the common repository.

The table below presents a high-level overview of the partner-provided inputs to this section as defined in the answers to the Data Management Questionnaire (Appendix A) found in Appendix B to this deliverable.

Partner	Findability Approach	Metadata Standards	Persistent Identifiers	Metadata Registration
CERTH	Not applicable	Not applicable	Not applicable	Not specified
CUB	Provides dataset info in deliverables/publications	Not specified	DOIs linked to publications	ODIN deliverables (e.g., D7.7)
Firenze (MedICT)	Uses metadata standards for HTA-related KPIs dataset	Dublin Core, ISO 19115	DOIs	Institutional repositories, open-access platforms
FORTH	Not specified	Not specified	Not specified	Not specified
Robotnik	Organizes data with structured naming conventions and directories	Not specified	ODIN Platform	WP3
SAS	Data collected via a patient app and healthcare	Not specified	Not specified	Not specified

Partner	Findability Approach	Metadata Standards	Persistent Identifiers	Metadata Registration
	platform, stored in a database			
INETUM	Does not generate or collect data	Not applicable	Not applicable	Not applicable
M&S	Stakeholder collections (emails, contact data) but no specifics on findability provided	Not specified	Not specified	Not specified
MDT (Medtronic)	Uses a patient app and healthcare platform, adheres to ISO27001:2013 for security	Not specified	Not specified	Information Security Management System (ISMS) by ATOS, OVH
MEDEA	Uses metadata standards for HTA-related KPIs dataset	Dublin Core, ISO 19115	DOIs	Institutional repositories, open-access platforms
MUL	Does not generate or collect data	Not applicable	Not applicable	Not applicable
MYS	Does not generate or collect data	Not applicable	Not applicable	Not applicable
Phillips	Uses CUB's metadata policies	Refer to CUB	Refer to CUB	Refer to CUB
SERMAS	Uses unique patient/stent identifiers, timestamps for organization	No metadata standards planned	No persistent identifiers planned	Metadata will not be registered due to data sensitivity
SSSA	Organizes HOSBOT/Human Modelling datasets with structured naming conventions	WP3	ODIN Platform	ODIN Platform
THL	Saves Robot Fleet Log data with structured naming (UUID, ISO 8601 timestamps)	JSON metadata corresponding to CSV files	DOIs	One-to-one correspondence between data and metadata files
UCBM	Odin Ontology for Metadata	No specific standards, custom metadata	Custom format	Registered with data

Partner	Findability Approach	Metadata Standards	Persistent Identifiers	Metadata Registration
UMCU	ISO9001 certified workflow, and for dataverse and archivemetic have specific workflows	Futurely DCAT	DOIs	In the catalogue
UPM	Plans to use ODIN Ontology for metadata	ODIN Ontology	TBD	TBD
Warwick	Did not use, collect, or generate data	Not applicable	Not applicable	Not applicable

Table 4 Findability approach per project partner

3.2 Accessibility

Once research data have been found, they should be accessible to the user, possibly through mechanisms for access control, such as authentication and authorisation. As outlined in section 5.1.1.4 of the Grant Agreement, the ODIN project participates in the Open Research Data Pilot (ORDP) which aims to improve access to and re-use of research data generated by Horizon 2020 projects and applies primarily to the data needed to validate the results presented in scientific publications. Project datasets (presentations, reports, scientific publications etc.), intended for public level of dissemination, have been made openly accessible through:

- CBMLBox
- Project’s website (<https://www.odin-smarthospitals.eu>)
- Partners’ own distribution channels
- CORDIS

Most openly accessible data is accessible with a regular browser, with MS excel or a PDF reader.

In this respect, the data management in ODIN was directed to be carried out in accordance with the Grant Agreement (article 29.3), which states that:

Regarding the digital research data generated in the action (‘data’), the beneficiaries must:

(a) Deposit in a research data repository and take measures to make it possible for third parties to access, mine, exploit, reproduce and disseminate — free of charge for any user — the following:

(i) The data, including associated metadata, needed to validate the results presented in scientific publications, as soon as possible;

(ii) Not applicable;

(iii) Other data, including associated metadata, as specified and within the deadlines laid down in the ‘data management plan’ (see Annex 1);

(b) Provide information — via the repository — about tools and instruments at the disposal of the beneficiaries and necessary for validating the results (and — where possible — provide the tools and instruments themselves).

(...)

As an exception, the beneficiaries do not have to ensure open access to specific parts of their research data under Point (a)(i) and (iii), if the achievement of the action's main objective (...) would be jeopardised by making those specific parts of the research data openly accessible. In this case, the data management plan must contain the reasons for not giving access.

The table below presents a high-level overview of the partner-provided inputs to this section as defined in the answers to the Data Management Questionnaire (Appendix A) found in Appendix B to this deliverable.

Partner	Accessibility Approach	Repository/Storage	Access Protocols	Authentication/Authorization	Open/Public Access
CERTH	Not specified	Not specified	HTTPS, API (potentially)	Not specified	Not specified
CUB	Data sharing agreement required; data is not publicly available	Hard drive, sent via post	Password encryption	Requires data sharing agreement with data owners	No
Firenze (MedICT)	Uses a project repository for sharing and long-term preservation	Institutional repository	Secure HTTPS, API-based access	Requires authorization from institutional portal	Restricted
FORTH	Data shared only with FORTH and UCBM	UCBM distribution channels	Credentials provided to FORTH	Restricted to project partners	No
Robotnik	Shared internally among partners, public results available via publications	Odin standards	Not specified	Following open-access/copyright guidelines	Some data public (after embargo)

Partner	Accessibility Approach	Repository/Storage	Access Protocols	Authentication/Authorization	Open/Public Access
SAS	Data stored in a shared project folder, results shared in PDF reports	Shared project folder	Not specified	Patient removed access post-program	No
INETUM	Does not generate or collect data	Not applicable	Not applicable	Not applicable	Not applicable
M&S	No specific accessibility details provided	Not specified	Not specified	Not specified	Not specified
MDT (Medtronic)	Uses a shared project folder, results in Power BI reports	Shared project folder	Not specified	Security controlled by ATOS/OVH, access via GetReady	No
MEDEA	Uses institutional repository for data sharing and preservation	Institutional repository	Secure HTTPS, API-based access	Requires authorization from institutional portal	Restricted
MUL	Does not generate or collect data	Not applicable	Not applicable	Not applicable	Not applicable
MYS	Does not generate or collect data	Not applicable	Not applicable	Not applicable	Not applicable

Partner	Accessibility Approach	Repository/Storage	Access Protocols	Authentication/Authorization	Open/Public Access
Phillips	Follows CUB's policies	Refer to CUB	Refer to CUB	Refer to CUB	Refer to CUB
SERMAS	Stored on a secure server separate from hospital network	Secure shared folder (Madrid's Digital Dept)	Secure VPN	Access restricted to authorized project members	No
SSSA	Shared internally among partners, public results in publications	WP3 repository	Not specified	Following open-access/copyright guidelines	Some data public (after embargo)
THL	Initial storage in private Google Drive, then uploaded to Zenodo or CMLBox	Google Drive, later Zenodo/CMLBox	HTTPS	No authentication required	No
UCBM	Data acquired by robotic platforms	Stored in a local HD not connected to any network	anonymized and password protected databases	Accessible only by dedicated researchers	No
UMCU	Datasets in the catalogue	Dataverse and Archivermetica	API	Data access will require authorization, specific datasets are reviewed by a Data Access Committee.	No
UPM	Raw data publicatio	TBD	TBD	TBD	TBD

Partner	Accessibility Approach	Repository/Storage	Access Protocols	Authentication/Authorization	Open/Public Access
	n undecided repository TBD				
Warwick	Did not generate or collect data	Not applicable	Not applicable	Not applicable	Not applicable

Table 5 Accessibility approach per project partner

3.3 Interoperability

As data usually needs to be integrated with other data, they need to interoperate with applications or workflows for analysis, storage, and processing. ODIN's consortium is aware of this challenge, as the different WPs require interoperability of data in order to allow smooth dataflow between partners. Best practices for achieving interoperability are continuously sought by the partners.

Within this context, where appropriate, partners have established and shared data dictionaries regarding the variables they intend to share in order to facilitate interoperability. The project's ontology has been designed in accordance with standardized ontologies as further analysed in Deliverable D3.3.

The table below presents a high-level overview of the partner-provided inputs to this section as defined in the answers to the Data Management Questionnaire (Appendix A) found in Appendix B to this deliverable.

Partner	Data Formats	Metadata & Documentation Standards	Shared Vocabularies/Ontologies	Compatibility Measures
CERTH	EDF, CSV, TXT (Federated Learning Pilot)	Not specified	Not needed for Sleep Analysis Application	No external integration for Sleep Analysis Application
CUB	CSV, TXT, EDF	Controlled vocabularies (sleep recording channels & annotations)	European standards	Works across platforms, compatible with other datasets
Firenze (MedICT)	XLSX, CSV	Not specified	No shared vocabularies/ontologies adopted	Not specified

Partner	Data Formats	Metadata & Documentation Standards	Shared Vocabularies/Ontologies	Compatibility Measures
FORTH	JPEG, MP4, XLS	Not specified	Not specified	Not specified
Robotnik	CSV, TXT	Not specified (refer to WP3)	Not specified	Uses MQTT, Robot Operating System (ROS) for data communication
SAS	CSV	LOINC	No shared vocabularies	Confirmed compatibility with technical team
INETUM	Not applicable	Not applicable	Not applicable	Not applicable
M&S	XLS, XLSX, CSV	Not specified	Not specified	Not specified
MDT (Medtronic)	CSV	LOINC	No shared vocabularies	Confirmed compatibility with technical team
MEDEA	XLSX, CSV	Not specified	No shared vocabularies/ontologies adopted	Not specified
MUL	Not applicable	Not applicable	Not applicable	Not applicable
MYS	Not applicable	Not applicable	Not applicable	Not applicable
Phillips	EDF, TXT (from CUB)	Not specified	Aligned with CUB	Refers to CUB questionnaire
SERMAS	CSV, MP4, log files	ICD-10, ATC	ICD-10, ATC	Designed to integrate with FORTH, SSSA, INETUM; uses standardized vocabularies
SSSA	CSV, MP4, TXT	Not specified (refer to WP3)	Not specified	Uses MQTT, ROS for data communication
THL	CSV, JSON	Not specified	Not specified	Uses JSON for metadata

Partner	Data Formats	Metadata & Documentation Standards	Shared Vocabularies/Ontologies	Compatibility Measures
UCBM	CSV	Not specified	Not specified	Not specified
UMCU	CSV	Some of our EHR data contains ontologies (ICD-10, ATC coding)	Some of our EHR data contains ontologies (ICD-10, ATC coding)	Data Dictionary
UPM	CSV, Text, RDF (where applicable)	ODIN ontologies	ODIN ontologies (D3.3)	Aims for semantic interoperability
Warwick	Not applicable	Not applicable	Not applicable	Not applicable

Table 6 Interoperability approach per project partner

3.4 Reusability

The ultimate goal of FAIR is to optimise the reuse of data. This can be achieved, when metadata and data are well-described so that they can be replicated and/or combined in different settings.

Given the sensitive nature of the pilots’ datasets and privacy requirements as per the GDPR, partners have agreed to only make available data for reuse beyond the project’s duration where national legislation permits so and only if all adequate measures have been adopted. Such measures may include the full anonymization of the data, an Ethics approval by the respective Ethics Committees and the signature of a data sharing agreement, specifying the purposes, condition, rights and obligations regarding the reuse of the data. As described in the relevant deliverables of WP8 and in previous iterations of this DMP, discussions have already taken place within the consortium regarding compliance with relevant regulations requiring additional reusability of data, such as the European Health Data Space (EHDS) Regulation, and will continue to address these as part of the project legacy activities setup by WP9.

The table below presents a high-level overview of the partner-provided inputs to this section as defined in the answers to the Data Management Questionnaire (Appendix A) found in Appendix B to this deliverable.

Partner	Data Reusability Approach
CERTH	No data generated or preserved for reuse; no licensing, documentation, or quality control mechanisms; FAIR principles not applicable.
CUB	Data is highly reusable (.CSV, .TXT, .EDF formats); a data dictionary is available on request; anonymization required; no license on medical data; data sharing agreements required.
MedICT (Firenze)	Data tables with KPIs are reusable; no license; no restrictions on reuse; KPIs are public information with no personal data; targets verified via literature.
FORTH	Data kept only for the project duration.

Partner	Data Reusability Approach
Robotnik	README files and data dictionaries provided; no personal data collected; design and performance data shared publicly; quality control includes versioning and validation scripts.
SAS	Marked as "N/A"; protected health data with contractual usage restrictions.
INETUM	Does not produce, generate, or collect data.
MINDS & SPARKS	No explicit statement on reusability.
MEDTRONIC	Marked as "N/A"; protected health data with contractual usage restrictions.
MEDEA	Same as MedICT (Firenze): Data tables with KPIs are reusable, no license, no restrictions, public KPIs, literature-verified targets.
MUL	No datasets listed or reusability information provided.
MYS	No datasets used; no information provided.
Philips	Used data from CUB under a data sharing agreement; performed re-identification risk analysis; referred to CUB's questionnaire for details.
SERMAS	README file and data dictionary included; data quality ensured via validation and version control; reuse restricted to ODIN Consortium and subject to Ethics Committee approval; no open license.
SSSA	README files and data dictionaries included; no personal data collected; design and performance data shared publicly; quality control includes versioning and validation scripts.
THL	Dataset contains logs of FMS component; reusability uncertain; README file provided; data licensed under MIT License.
UCBM	README files included; reusable within ODIN project or related publications; version control applied.
UDGA	Standardized questionnaires and templates for compliance monitoring made available with publications
UMCU	UMCU is deploying a Data Catalogue. Most datasets contain personal data and won't be shared. Scripts are shared in GitHub.
UPM	README files included; data available under CC BY 4.0 license; no restrictions on reuse.
Warwick	Did not use, collect, or generate datasets; FAIR principles not applicable.

Table 7 Reusability approach per project partner

4 Ethics, Data Protection and Security Considerations

4.1 Ethical Principles

ODIN as a project, its consortium and the actions related to the project have complied with ethical and legal principles, standards and regulations. This includes undertaking activities in compliance with ethical principles and applicable international, EU and national law. The most important guiding principles are outlined in this section. The deliverable D8.2 “Policy, Legal and Ethics Framework” provides a comprehensive mapping of the most relevant initiatives, which should be drawn to support the current document, and which were fundamental to guide and align partner activities during the project (particularly as part of the monthly meetings).

As noted in previous iterations of this deliverable, various ethical requirements apply, such as the Good Clinical Practice guidelines³, and the Declaration of Helsinki, as well as those principles found in relevant EU legislation, such as:

- The Charter of Fundamental Rights of the EU (specially Art.3: right to the integrity of the person; and Art. 8: protection of personal data)
- 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 of clinical trials on medicinal products for human use;
- EU General Data Protection Regulation 2016/679;
- Treaty on the European Union (TEU): Article 6;
- EU Charter of Fundamental Rights of 7 December 2000;
- Medical Device Regulation (EU) 2017/745 for the implementation of the system in the public health environment in a secure setting.

Given its nature and scope, the most relevant ethical issues to prevent related to management and protection of personal. For this reason a commitment was made within ODIN to ensure that any research involving human subjects, data processing, and sensitive data processing would conform to applicable legislation and regulations both on European level, as well as to complementary obligations of the countries where the activities were carried out..

In order to protect the privacy rights of participants, a number of best practice principles has been strictly followed throughout the runtime of ODIN. There are two basic components to the ethical standards: (i) **informed consent** and (ii) **independent ethical oversight**.⁴ Leveraging on

³ COMMISSION DIRECTIVE 2005/28/EC of 8 April 2005 laying down principles and detailed guidelines for good clinical practice as regards investigational medicinal products for human use, as well as the requirements for authorisation of the manufacturing or importation of such products. Available here: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32005L0028&from=EN>.

⁴ EDPS A Preliminary Opinion on data protection and scientific research, p.14. Available here: https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf.

*International Ethical Guidelines for Health-related Research Involving Humans*⁵, ODIN's consortium has identified and implemented additional ones, in the light of the specific identified risks for the project, and its needs. These include:

- 1) **Informed Consent**, that is prior, freely given and specific. Researchers must provide all relevant information to the participants beforehand, as well as all clarification where required.
- 2) **Approval by Research Ethics Committees**, as reported in Deliverable D11.1.
- 3) **Scientific and Social Value**, conducting studies that are scientifically sound, build on an adequate prior knowledge base, and are likely to generate valuable information.
- 4) **Purpose Limitation**.
- 5) **Data minimization**, not retaining any ancillary data obtained and anonymizing all personal data when possible.
- 6) **Use of Data obtained from the Online Environment and Digital Tools in Health-related Research**, focusing on the adoption of privacy-protecting measures and the mitigation of risks that could result from combining data from multiple sources and their subsequent use and publication.
- 7) **Reimbursement and Compensation for Research Participants**, such as travel costs, and compensated reasonably for their inconvenience and time spent, whether monetary or non-monetary, following the approval of the local ethics committee.
- 8) **Recruitment of Affiliated Participants** and the protection of their privacy, confidentiality, ensuring their non-discrimination.
- 9) **Privacy and Confidentiality**, specifically with regards to the measures to prevent re-identification of the data subjects.
- 10) **Data Sharing**, in accordance with legal requirements.
- 11) **Vulnerable Persons and Groups**, placing additional safeguards for their protection.

Alignment with these commitments was ensured as part of the various WP activities, in particular WP2, WP7 and WP8.

4.2 Consent forms

Even though it is not only the explicit consent of participating individuals in medical research that should constitute a legal basis for a data processing (Art. 6(1)(b-d) GDPR, Art. 9(2) GDPR), the “ethical requirement” of an informed consent should be met either way.⁶ The statements according to the ethical standards and bio-ethics conventions primarily aim to protect individuals against being included in medical research activities against their will and/or without their

⁵ International Ethical Guidelines for Health-related Research Involving Humans, Prepared by the Council for International Organizations of Medical Sciences (CIOMS) in collaboration with the World Health Organization (WHO), Geneva 2016. Available here: <https://cioms.ch/wp-content/uploads/2017/01/WEB-CIOMS-EthicalGuidelines.pdf>.

⁶ EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research, paragraph 7, p.4. Available here: https://edpb.europa.eu/sites/default/files/files/file1/edpb_replyec_questionnairesearch_final.pdf.

knowledge. Hence, sufficiently informing participating individuals about their engagement in scientific (or medical) research activities is imperative and was provided in the scope of this project.

The provisions of the Oviedo Convention⁷, along with those of the Declaration of Helsinki⁸, outline the essential information for prospective research participants to obtain an informed consent, mainly focusing on maintaining the research subjects' privacy, while ensuring a free and informed consent, providing all required information to participants of age. In this context, during the ethical approval process and the implementation of WP7 activities, all participants' rights, especially with regards to information and access to the clinical study data, were of utmost importance, along with the protection of vulnerable individuals.

4.3 Data Protection Principles

The project agreed in previous DMPs to consider data management as an ongoing process and the current data management plan, as outlined above, is the final reflection (within the scope of the Grant Agreement) of this action. In view of this, the present deliverable builds upon the work already performed in its previous iterations and recognizes the ongoing need to respect the following principles, as were originally identified:

- A. **Lawfulness and Fairness**, focusing on the identification of a valid legal basis, as per Art. 6 (1) and 9 GDPR, and the processing of data in a way that is not unjustifiably detrimental, unlawfully discriminatory, unexpected or misleading to the data subject;
- B. **Transparency and provision of sufficient information** to data subjects;
- C. **Purpose Limitation and Presumption of Compatibility** of any Further Processing purposes;
- D. **Data Minimization and Storage Limitation**, also referring to national obligations and guidelines;
- E. **Accuracy** and, where required, updates of the data;
- F. **Integrity and Confidentiality**, ensuring appropriate security against unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organisational measures. Said security measures must be designed in accordance with the nature of the data as sensitive data related to the data subjects' health;
- G. **Accountability**, ensuring not only that adequate measures are adopted but also that compliance can be demonstrated.

The ODIN project demonstrated its commitment towards compliance with the data protection rules and GDPR regulations and commitment to promoting EU fundamental rights by dedicating a Work Package (WP8) to Legal, Ethical and Standardization Aspects for Sustainability. However,

⁷ Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine, Oviedo, 4.IV.1997. Available here: <https://rm.coe.int/168007cf98>.

⁸ WMA DECLARATION OF HELSINKI – ETHICAL PRINCIPLES FOR MEDICAL RESEARCH INVOLVING HUMAN SUBJECTS. Available here: <https://www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects/>.

as it was noted that each partner remained responsible for *its actions, for compliance with the GDPR and safeguarding EU fundamental rights, safekeeping documentation on compliance was requested from all parties involved in the project*. To ease this process, all partners were granted access to the Europrivacy Academy training, so as to align their self-assessment activities and documentation actions with the Europrivacy GDPR Certification Scheme, which has been officially adopted by EDPB as a Data Protection Seal to be used all across the EU. This action is also of relevance towards the sustainability of the project results (as defined by Task 8.2 and 8.3 and noted in the Project Legacy Deliverable of WP9), since an eventual certification of compliance for the platform, its enablers and the partners involved in their deployment and exploitation could greatly ease market access in the EU and beyond.

4.4 Controller identification and initial instruction definition

While the project supported the access to open data by third parties, it has always sought to abide with strict personal data protection policy in line with the EU General Data Protection Regulation (GDPR) and other applicable norms, including the European Health Data Space Regulation. Personal data protection compliance is part of the project's requirements and will guide the architecture design. Personal data protection principles determine and limit the data sharing. ODIN remains committed to proactively ensure full compliance with the GDPR through a set of ad hoc policies, mechanisms, and tools.

Moreover, the project committed to strictly stick to the principle of data minimization by avoiding the collection and processing of any unnecessary personal data. Personal data can be kept in a form which permits identification of data subjects for no longer than is reasonable, proportionate, and necessary for the purposes for which the personal data are processed.

As noted in Section 2, the core providers of (sensitive) personal data in the framework of the project were the Pilot owners, acting as data controllers for any data to be provided to the consortium from their infrastructure and/or network and the key responsible organizations ensuring compliance with ethical and data protection requirements throughout the design and implementation of the processing activities (e.g.: DPIA, data subject right protection, etc.). The implementation phase of the pilots enabled the controllers to validate the means and purposes of any processing performed and identified whether any other partner should be granted access to the data. The project has also adopted the relevant Data Sharing Agreements, reported on in detail above.

As was analysed in detail in the first version of the Data Management Plan, there is a set of general instructions that Data Controllers must take into consideration under the individual Controllers and Controller to Controller data transfer scenarios. Said guidelines mainly focus on purpose limitation, data minimization, the obligation to ensure data subjects are adequately informed and can effectively exercise their rights, as well as the adoption and implementation of adequate technical and organizational measures in order to ensure personal data remains protected at all times, which may also be accompanied by audits.

Similarly, data Processors under the Controller to Processor data transfer scenario are bound to follow additional guidelines adapted to this scenario. In this context, it is highly important that the Processors provide sufficient guarantees to implement technical and organizational measures, as well as to refrain from engaging sub-processors without the Controller's prior authorization. They shall additionally take all appropriate measures to assist the Controller to fulfil their obligations and shall act only in the name of and in accordance with the Controller's instructions. Finally, the Processor shall return all personal data to the Controller once the relevant task has been concluded and shall delete all copies.

Lastly, all Partners acting as data Controllers were requested to ensure compliance with national and regional requirements for personal data processing, and should consider both EDPB and national authority guidance when developing and deploying their respective research actions in the context of the ODIN project. In particular, all partners must consider the content of the following EDPB guidance whenever relevant to their actions:

- Article 29 Data Protection Working Party - Guidelines on Data Protection Officers ('DPOs') (wp243rev.01) (10/2017)
- Article 29 Data Protection Working Party - Data Protection impact assessments High risk processing (10/2017)
- Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01)
- Guidelines 3/2019 on processing of personal data through video devices
- EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default
- EDPB Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak
- Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak
- EDPB Guidelines 05/2020 on consent under Regulation 2016/679
- EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR
- EDPB Guidelines 01/2022 on data subject rights - Right of access
- EDPB Guidelines 02/2021 on virtual voice assistants
- EDPB Guidelines 08/2022 on identifying a controller or processor's lead supervisory authority

Within the scope of the ODIN project, WP7 partners involved in the piloting activities were particularly active in the performance of compliance activities denoted in this section, and prepared extensive documentation and impact assessments as part of the ethical approval process which is available upon request.

4.5 Technical and Organisational Measures

According to Art. 32(1) GDPR, the data controller and the data processor should implement appropriate technical and organisational measures (TOMs) to ensure a level of security appropriate to the risk, as well as to the state of the art, the costs of implementation and the nature, scope, context and purposes of processing. The Regulation deems, inter alia, the following TOMs appropriate⁹:

⁹ Art. 32 (1) GDPR.

- Pseudonymisation and encryption of personal data;
- Ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- Restoring the availability and access to personal data in the event of a physical or technical incident;
- Regularly testing, assessing and evaluating the effectiveness of the TOMs for ensuring the security of the processing.

As a general guiding element, project partners were required to implement and document appropriate technical and organizational measures towards ensuring the security of any data collected, processed, transmitted, disclosed or deleted during the scope of the project. All partners were also invited to consider relevant standards on both data protection and security, including (but not limited to):

- ISO/IEC 15408-1:2009 Information technology — Security techniques — Evaluation criteria for IT security;
- ISO/IEC TS 19608:2018 Guidance for developing security and privacy functional requirements based on ISO/IEC 15408;
- ISO/IEC 27001:2022 information security management;
- ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines
- ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls;
- ISO/IEC 27018:2019 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors;
- ISO/IEC TS 27110:2021 Information technology, cybersecurity and privacy protection — Cybersecurity framework development guidelines;
- ISO/IEC 29100:2011 Information technology — Security techniques — Privacy framework;
- ISO/IEC 27559:2022 Information security, cybersecurity and privacy protection – Privacy enhancing data de-identification framework
- ISO/IEC 29101:2018 Information technology — Security techniques — Privacy architecture framework;
- ISO/IEC 29134:2017 Information technology — Security techniques — Guidelines for privacy impact assessment;
- ISO/IEC 29151:2017 Information technology — Security techniques — Code of practice for personally identifiable information protection;
- ISO/IEC 29190:2015 Information technology — Security techniques — Privacy capability assessment model

The table below represents the TOMs each partner of the consortium has undertaken to secure their data processing and to safeguard the rights and freedoms of the data subjects, whose data are being processed.

Partner	TOMs
Robotnik	The robot is protected by different security layers regarding network, code, and access.
SERMAS	<ul style="list-style-type: none"> • Data back-ups. • The server will be located in a secure area of the hospital with restricted physical access. • Different users and user rights will be defined for the project members accessing the data remotely.
MYSHERA	<p>Secure access through role base permission.</p> <p>Data is stored with version management and data loss protection.</p>
M&S	<p>MINDS & SPARKS GmbH ensures that both physical and technical measures will be taken for the protection of the personal data which are going to be processed during the lifetime of ODIN.</p> <p>Internal policies and confidentiality agreements will safeguard the data as well as secured storage where only authorized access is allowed with controlled password-protected access (see above).</p>
MEDTRONIC	<ul style="list-style-type: none"> • Data stored in documents is regularly backed-up to Medtronic’s OneDrive servers • Miro boards data, although available through Miro website, is backed up in Medtronic’s internal servers • Website data also backed up and properly secured
CERTH	<p>In conformity with international (GDPR) and national law a number of technical and organizational measures (TOMs) will be initiated and implemented. For instance, among the technical measures that are defined to be implemented is to conduct regular back-ups in order to avoid unexpected data loss, enable physical and virtual secured storage and access to data. Particularly sensitive data will be stored in an anonymised form, explicitly stated in the consent form and in the context of the overall consent procedure. Access rights to this data will be clearly stated in relevant documentations.</p>
FORTH	<p>FORTH and the technology that is used is GDPR compliant for all data used. The private cloud facilities are ensuring data security and privacy.</p>
University of Warwick (UoW)	<p>UOW is not storing data on their premises but on the Cloud Services provided by FORTH.</p>
SSSA	<p>This aspect does not concern WP5 and SSSA activities because data will not be stored by SSSA, but will be transmitted to the ODIN’s ICT platform/infrastructure.</p>

Partner	TOMs
THL	Equipment used in the project’s data processing activities (including laptops etc) is password protected. Regular weekly back-ups are conducted.
Philips Electronics Netherland BV (PEN)	PEN will not store data in their infrastructure based on initial discussions with pilot sites. Data will be accessed at the clinical sites.
UPM	Security measures are going to be defined but in principle it is foreseen high availability of data services that implies backups, data redundancy, as well secure storage with encryption at rest and access control are expected for securely accessing the data only by authorized users.
INETUM	At this stage, there is no data collection, processing or sharing envisioned on behalf of INETUM.
UCBM	<p>Thanks to its previous experience, UCBM will adopt several good practices to ensure data management in complete safety. In particular, the data will be password protected and access will be allowed only to a small group of the UCBM team. Anyone who works with confidential electronic data should identify themselves when they log on to the PC or laptop computer that gives them access to the data and the list of users will be kept up to date. Furthermore, only secure methods of data transfer will be used and systems for the secure destruction of the same will be adopted. Furthermore, all UCBM personnel are constantly trained and updated on the best practices to be adopted for data management.</p> <p>PCs and laptops will be used for short-term storage and data processing. In no case should these be relied upon for storing master copies, unless backed-up regularly. A private back-up area will be identified for research data collection, and it will be set and configured to act as the only backup area for any relevant project file. The file repository will be duly sized. Moreover, all data will be backed up and securely encrypted with a cadence to be defined.</p>
UMCU	UMCU is ISO27001 certified (IT dept) and 9001 certified (lab).
Charite (CUB)	The hospital firewall is maintained by the IT department of the Charite university hospital. All computers in use are protected and administered by the university hospital IT department. One of our IT department members is member of the Charite group involved in ODIN.
MUL	Data access is available for researchers at the Department of Family Medicine, Medical University of Lodz based on the MUL data management policy and binding national regulations. Backups are made on the continuous basis by MUL IT department for all study-related data.

Partner	TOMs
UDGA	Access to the data processed for UDGA’s activities was thoroughly secured, access granted through an authentication mechanism only to participants in the consortium.
MEDICT MEDEA	MEDEA - Conduction of regular back-ups to avoid unexpected data loss; physical and virtual secured access to data.

Table 8 Technical and Organizational Measures for compliances

4.6 Data Subject Rights

Recital 59 GDPR defines modalities for facilitating the exercise of the data subject’s rights, such as mechanisms to request and obtain free of charge access to, request rectification or erasure of personal data shall be set. Furthermore it requires that the data controller should also make such exercise of data subjects’ rights possible electronically and should be obliged to respond to requests from the data subject without undue delay.

As reported in the context of WP7 & 8 deliverables, all ODIN participants were made aware of their right to withdraw from the research activities without providing any reason for their withdrawal and that they retain this right at all times. If any of the research activities they are participating in involves audio recording or electronic note taking, they will be notified that they can ask the interviewer to stop or delete all or a portion of the recorded material at any time. Participants can also request that content is erased retrospectively. Invited individual participants are briefed about this right through the informed consent process. Withdrawal can be also expressed orally.

Following, below are the data subjects’ rights, as per the provisions of the GDPR, which the ODIN’s consortium committed to respect and guarantee, as were previously analysed:

- a. **Right to access** their personal data that is collected and/or processed;
- b. **Right to information** about all relevant aspects surrounding the collection and processing of their personal data, unless the data was not collected directly by the data subjects and if it “proves impossible or would involve a disproportionate effort, in particular for processing for scientific research purposes when the conditions of Article 89 are satisfied or when this is likely to render impossible or seriously impair the achievement of the objective of that processing” .;
- c. **Right to rectification** of their personal data;
- d. **Right to object** to the processing of their personal data;
- e. **Right to erasure** of their personal data;
- f. **Right to restriction** of processing of their personal data;
- g. **Right to data portability** of their personal data in a “structured, commonly used and machine-readable format”;
- h. **Rights related to Automated Individual Decision-making and Profiling**, focusing in particular to the data subjects’ right to not be subject to automated Individual Decision-making and Profiling where that may have a legal or similar effect for them.

4.7 Data Protection Officers (DPOs)

The GDPR defines the role and responsibility of a Data Protection Officer (DPO), Art. 37 GDPR. The DPO is in charge of monitoring the application of the GDPR within an organization and providing strategic advice to it on how to process personal data while respecting and executing individuals' rights and the requests noted in the previous section.

As requested, all project partners took active and coordinated steps to ensure compliance and to maximize communication across the project. The following table presents the DPOs and relevant contact persons identified by project partners during the project to support this action:

Organisation	Contact Person(s)	Data Protection Officer (DPO)	DPO Email
CERTH	Vasileios Lolis	Stella Papastergiou	dpo@certh.gr
CUB	Matthew Salanitro	Behördliche Datenschutzbeauftragte der Charité	datenschutz@charite.de
MedICT (Firenze)	Lorenzo Mucchi	<i>No DPO info</i>	N/A
FORTH	Daphne Plati	Stavroula Stathara	dpo@uoi.gr
Robotnik	Raquel Juliá Ros, Víctor Solaz Estevan	Nuria Pla Plaza	npla@robotnik.es
SAS	Paula Algarín Sánchez	Cristina Suárez Mejías	cristina.suarez.mejias.sspa@juntadeandalucia.es
INETUM	Andres Iborra Martin	Susana Gonzalez Garcia de Consuegra	susana.gonzalez@inetum.com
MINDS & SPARKS	Gisela Hagmair	<i>No DPO info</i>	N/A
MEDTRONIC	Paula Currás, Alba Hernández	Luca Staffa	rs.europeanDPO@medtronic.com
MEDEA	Francesco Agnoloni	Nicola Fernando Fratea	n.fratea@orthokey.eu
MUL	Joanna Orłowska	Katarzyna Kawczyńska	iod@umed.lodz.pl
MYS	Pilar Sala	<i>(Not named)</i>	gdpr@mysphera.com
Philips	Stephan Nijssen	Oleksandr Tomashchuk	oleksandr.tomashchuk@philips.com
SERMAS	María Luaces, Jorge Nieto, Laura Llorente	<i>No DPO info</i>	delegadoprotecciondatos@sanidad.gob.es

Organisation	Contact Person(s)	Data Protection Officer (DPO)	DPO Email
SSSA	Gastone Ciuti	Rosa Medaglia	dpo@santannapisa.it
THL	Lampis Papakostas	Dr. Panagiotis Chatzakos	panagiotis.chatzakos@twi.gr
UCBM	Nevio Tagliamonte Luigi	Vincenza Del Prete	areaprivacy@unicampus.it
UMCU	Saskia Haitjema	Jaap van Minnen	j.g.vanminnen-2@umcutrecht.nl
UPM	Giuseppe Fico	LUIS CANCELA DE LA VIUDA	proteccion.datos@upm.es
Warwick	Leandro Pecchia	University Information and Data Compliance Team	infocompliance@warwick.ac.uk
UDGA	Adrian Quesada Rodriguez	Adrian Quesada Rodriguez	aqesada@udgalliance.org

Table 9 Contact person and DPO identification per partner

Alongside with their usual compliance activities, both local representatives and local DPOs were tasked with the alignment of the compliance approach for the project in close coordination with the researchers responsible of the different pilots. Their participation in the monthly meetings performed by the project to discuss legal, ethics and gender issues was fundamental to ensure proper risk mitigation took place.

As noted in the GA and the Consortium Agreement, ODIN appointed a DPO for the project, represented by the Ethical and Trusted Data Manager (ETDM) (UDGA) position currently held by MA. M.Sc. Adrian Quesada Rodriguez, in charge of:

- Establishing common rules and requirements for the consortium data protection policy;
- Coordinating the action and information among the various DPOs and organize, when needed, regular calls among the DPOs of the different data controllers;
- Serving as an entry point to answer questions and complaints from third parties when addressed to the project as a whole;
- Providing guidance on how to implement the privacy by design and by default principles.
- Organizing monthly calls, workshops, and relevant webinars on compliance with the support of the consortium partners and in alignment with WP8 activities.

5 Intellectual Property Rights

5.1 Intellectual Property Rights within ODIN

In line with contractual and legal requirements, all project partners have acknowledged the necessity of effectively managing Intellectual Property Rights (IPR) to safeguard the outputs, datasets, tools, methodologies, and frameworks generated during the lifecycle of the project. To this end, the Consortium Agreement has established a standardized framework for governing these discussions, upon which intellectual property of beneficiaries and third parties alike are respected while facilitating collaboration and information transfer.

As noted in this agreement, results from experiments are owned by the beneficiaries or third parties that generate them. In instances of joint ownership, partners have generated protocols (as part of WP9 sustainability actions) for shared right administration and preventing and/or managing eventual conflicts. Tools generated and used within the scope of the project to meet the dispositions of the Grant Agreement have been disseminated internally as necessary and permitted under applicable data sharing and utilization agreements (including those found in the Consortium Agreement).

The table below presents a high-level overview of the partner-provided inputs to this section as defined in the answers to the Data Management Questionnaire (Appendix A) found in Appendix B to this deliverable. It is important to note however that the information found in this deliverable only seeks to provide an inkling of the IPR approach followed by the project, and that a more thorough examination of the IPR considerations and needs for sustainability has been performed by WP9 (exploitation and innovation management), including the identification of exploitable assets, protection methodologies, prospective licensing or commercialization pathways and overall coordination approaches. These efforts have also been continued by the project legacy activities and the MoU which includes specific dispositions on this direction.

Organization	Background (Consortium Agreement)	Foreground: Aligned with Key Exploitable Results
CERTH	Human motion analysis toolkit Object detector module SLAM/mobile platform navigation toolkit Shared human-robot workspace toolkit IoT monitoring platform Data analytics and visualization platform Blockchain-based WoT certification CERTHbot endorsed with functionalities such as social navigation, human detection, tracking and action recognition. Data analytics platform for analyzing sleep monitoring data, and any machine learning methods developed within the project in this context.	Extension of: CERTHbot endorsed with functionalities such as social navigation, human detection, tracking and action recognition. - CERTH’s data analytics platform for analyzing sleep monitoring data, and any machine learning methods developed within the project in this context. Foreground, Licence, Access and dissemination will be defined by the end of the project.

Organization	Background (Consortium Agreement)	Foreground: Aligned with Key Exploitable Results
CHARITE	Database of sleep recordings from healthy subjects and patients with sleep disorders	The database is being used by CERTH to develop a sleep analysis application, which will then be used by CUB
FORTH	None	None identified in Questionnaire
INETUM	None	None identified in Questionnaire
M&S	None	None identified in Questionnaire
MDT	None	None identified in Questionnaire
MEDEA	None	None identified in Questionnaire
MUL	None	None identified in Questionnaire
MYS	ORVital IoT – Real Time location System ATLAS	Connector RTLS to Kafka to integrate in ODIN Resource choreographer connector and several workflow code and definition
PHILLIPS	None	None identified in Questionnaire
ROBOTNIK	None	None identified in Questionnaire
SERMAS	Clinical data lake of Hospital Clinico San Carlos (ECR, Clinical images, Drug Information)	None identified in Questionnaire
SSSA	Sensitive system for increased proximity detection Two patents on the capacitive technology employed by SSSA. Another patent for HOSBOT robotic platform.	Scuola Superiore Sant’Anna (SSSA) has generated a patent on one technology developed during the ODIN project, in collaboration with Universidad Politécnica de Madrid (UPM). This patent is national (Italy), has been submitted and is currently under review by the patent office. The patent regards the HOSBOT platform, generally called “dispositivo di movimentazione” (transportation device), and describes an invention. This invention is HOSBOT, which is a modular robotic device for hospital logistics, interfaced with compatible autonomous mobile robots as driving unit, and carrying boxes. The focus of the patent is the modular approach to robotics-aided logistics in hospitals and other industrial/service environments.

Organization	Background (Consortium Agreement)	Foreground: Aligned with Key Exploitable Results
TWI	None	A system and a methodology that enables a centralized control and orchestration throughout the operation of multiple robotic platforms within a hospital environment, optimizing their deployment and allocation for efficient logistics management and the utilization of robotic resources. The present system permits the seamless integration with multiple robots and offers a unified interface that simplifies communication, coordination, and control of robotic systems using a modular and scalable architecture.
UCBM	Systems and approaches for low-level interaction control algorithms, high level interaction planners, approaches for human-robot interaction and manipulation, high-level software packages for interconnection of sensors, actuators and control units, mechanical tools and interfaces	UCBM background knowledge was used to support all project activities. UCBM grants access rights to its background for research purposes only within the scope of the ODIN project and retains exclusive exploitation rights
UDGA	None	Certification-related criteria & Questionnaires and/or templates for compliance monitoring
UMCU	None	None
UOW	None	None
UPM	Know-how from R/D and previous research projects (See Consortium Agreement)	UPM's Software-type IPR: operational dashboard, metrics dashboard, ontology, metrics management, opensearch integration and configurations, platform designs, ODIN Innovation Hub, Change. MGMT, Streaming Server; and their respective associated documentation.

Table 10 Partners Background and Foreground IPR

6 Conclusion

This last iteration of ODIN's Data Management Plan showcases the activities undertaken by all project partners towards the definition, integration and implementation of a mature data governance strategy. Guided by living feedback from partners and informed by the evolving requirements of the pilots, technical activities and regulatory and ethical guidance, ODIN prioritized compliance while embracing transparency, scientific integrity and alignment with best practices and international standards.

The consortium adopted the FAIR data principles as a framework to ease the joint implementation of coordinated data practices with the long-term research and innovation goals in mind. By balancing openness and transparency requirements with a close monitoring of privacy requirements, the project has successfully generated impactful results. This is bolstered by the project-wide examination of IPR, sustainability and exploitation pathways that finally led to the Project Legacy activities planned for ODIN, and in which this task directly contributed.

As ODIN meets its culmination, this deliverable presents readers and consortium partners alike with the foundations for what will be a sustainable data management approach down the road. Indeed, the consortium has set in place all necessary data retention strategies, contractual, technical and organizational measures to preserve the project's impact beyond its original timeline. It is now up to the partners and stakeholders to carry this legacy forward, ensuring that the knowledge, tools and data governance practices developed with ODIN continue to support responsible innovation, open science, and international collaboration well beyond the project's completion.

Appendix A Data Management Questionnaire

Data Management Questionnaire

Deadline: 15/12/2024

Partner: [Organization + Contact person]

Instructions

This questionnaire aims at collecting final information on data management, ethics and IPR of partners in the present research project.

The current survey needs to be completed **by all partners**.

Please fill in the relevant (contact) information for your organization on the first page of this questionnaire.

Should you not process any personal data in the framework of your involvement in the project, you should at least complete the sections on (FAIR) Data Management, IPR management and AI use.

Please return the completed survey to us as soon as possible.

Partner Organization

Name:

Address:

Country:

Website:

Privacy policy webpage:

Contact Person

Name:

Email:

Phone Number:

Data Protection Officer

Name:

Email:

Phone Number:

Data Processing Activities

1. Indicate what categories of data you collect(ed) or process(ed) in the context of the project:
 - non personal data** (i.e. environmental data). *Note: All aspects are related to Research Data Management and FAIR compliance.*
 - personal data** (any information relating to identified or identifiable individuals, including for instance email or IP addresses)
 - special categories of data** (personal data revealing sensitive information such as sexual orientation, racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as any health, genetic or biometric data related to the data subjects)

2. Describe the categories of personal data you will be collecting and/or processing: How did you collect these personal data?
 - directly from data subjects who belong to your research team
 - directly from data subjects outside your research team (i.e. early adopters, beta testers, etc.)
 - indirectly through partners of the project
 - indirectly through other organizations external to the project
 - Other
 - N/A (*you can skip the last section of this document*)

Data Management

3. Please list all datasets which your organization currently uses or has obtained in the context of the ODIN project (*Feel free to duplicate this table if multiple datasets will or have been used*)?

	Please provide your answers in this column:
Dataset(s) name	<i>What is the name of the used dataset(s)?</i>
Dataset(s) description	<i>Please provide a short description of the dataset(s).</i>
Personal Data	<i>Does the dataset include personal data? If yes, please specify the type of personal data.</i>
Purpose	<i>What is the purpose for which you use/ process the dataset(s)?</i>
Data format	<i>What format(s) are your dataset(s)?</i>
Data Storage	<i>Where will you store the dataset(s)?</i>
Main Data Source	<i>What is the main source of the dataset(s)?</i>
Data Ownership	<i>Who owns the dataset(s)?</i>
Country of Origin	<i>Where does the dataset come from?</i>
Restrictions on the use	<i>Are there any restrictions for the use of the datasets?</i>

FAIR DATA

Access	<i>Who has access to the datasets? Please include other work packages which will also access the datasets.</i>
Retention Period	<i>How long will you keep the datasets?</i>
Licence	<i>Under which licence did you obtain access to the datasets?</i>
WP and task	<i>For which work package and which task do you need to use the datasets?</i>
Additional Comments	<i>Please add here any additional comments.</i>

1. Did you or will you be taking measures in order to comply with the FAIR data principles (making data Findable, Accessible, Interoperable and Reusable)? If so, kindly provide additional information on how each of these principles are being met:

	Please provide your answers in this column:
Findable	<p><i>Please explain in detail and with as much technical information as possible how you ensure findability of your research data.</i></p> <p><i>What types of data will you collect, generate, or reuse (e.g., datasets, images, software)?</i></p> <p><i>What metadata standards will you use to ensure discoverability (e.g., Dublin Core, ISO 19115)?</i></p> <p><i>What persistent identifiers will you use for your datasets (e.g., DOIs, PURLs)?</i></p> <p><i>How and where will your metadata be registered or indexed?</i></p>
Accessible	<p><i>Please explain in detail and with as much technical information as possible how you ensure accessibility of your research data.</i></p> <p><i>When and how will the data be made publicly available (e.g., embargo period, open access)?</i></p> <p><i>Which repository will you use for data sharing and long-term preservation (e.g., Zenodo, institutional repository)?</i></p> <p><i>What protocols or mechanisms will be used to ensure secure and open access to the data (e.g., HTTPS, API access)?</i></p> <p><i>Will access to any data require authentication or authorization?</i></p>
Interoperable	<p><i>Please explain in detail and with as much technical information as possible how you ensure interoperability of your research data.</i></p> <p><i>In what formats will your data be stored to ensure machine-readability (e.g., CSV, JSON, RDF)?</i></p> <p><i>What metadata and documentation standards will you adopt to ensure interoperability (e.g., controlled vocabularies, ontologies)?</i></p> <p><i>Will you use or adopt shared vocabularies or ontologies? If so, which ones?</i></p> <p><i>How will you ensure compatibility with other datasets or systems?</i></p>
Reusable	<p><i>Please explain in detail and with as much technical information as possible how you ensure reusability of your research data.</i></p>

What documentation will accompany your data to support reuse (e.g., README files, data dictionaries)?

Under which license will the data be made available (e.g., CC BY 4.0, MIT)?

Are there any restrictions on data reuse (e.g., personal data, third-party IP)?

How will you ensure data quality and provenance (e.g., versioning, quality control processes)?

Intellectual Property Rights

1. Did your organization generate or plan to generate any foreground IPR as part of the project? If so, please describe it's type (patents, copyrights, trademarks, know-how, trade secrets, etc.) and provide a brief description.

2. Please fill in this table to provide further information on IPR practices for your solutions/enablers.

	Please provide your answers in this column:
Ownership and Rights	<i>Who owns the overall IPR for the foreground code/solutions, and how will rights be shared or managed among project partners?</i>
Background Licences	<i>Please state any pre-existing code/solutions that were incorporated into the project-generated code/solutions. What licences govern these background assets, are there restrictions or obligations? (e.g. attribution, non-commercial use)</i>
Foreground Licences	<i>Please state those licences that have been applied to the new code/solutions (foreground) that were generated during the project.</i>
Licence Compatibility	<i>Are there conflicts or compatibility issues between the background and foreground licences? How should they be addresses?</i>
Access and Dissemination	<i>Will the foreground code/solutions be made publicly available after the project conclusion? If yes, under what conditions? (e.g. repositories, timing, usage restrictions)</i>

AI use Practices

	Please provide your answers in this column:
AI use practices	<i>Did your organization use or plan to use any Artificial Intelligence (AI) technologies or methodologies as part of the project? If so, please describe the specific AI tools or algorithms employed, the purpose and application of AI in your research activities, the types of data processed by these AI systems, and measures taken to ensure ethical use and compliance with relevant data protection regulations.</i>

Ethics and Personal Data Protection

	Please provide your answers in this column:
Purpose of Personal Data Collection	<i>For what purpose(s) did you collect the aforementioned personal data?</i>
Data Processing Activities	<i>List the main data processing activities your organization has or will perform in the context of the project</i>
Further Processing Purposes	<i>Did you or will you process the generated data for any further purposes than the ones it was originally collected for? Please indicate YES or NO If you answered YES, then please describe the purpose of this additional processing.</i>
Information Rights	<i>How did you inform the individuals (the data subjects) about the purpose of the data processing of their personal data in the project?</i>
Consent	<i>How did you plan to collect and document the consent of the data subjects whose personal data will be processed by you?</i>
Data Storage	<i>How and where did you or will you store the data?</i>
Data Retention	<i>For how long did you or will you keep the data?</i>
Ethical Approval	<i>Did you or will you obtain an ethical approval as part of your project-related activities? Please elaborate.</i>

Appendix B Questionnaire responses from the partners

Given the sensitive nature of the responses obtained from all project partners, answers to the questionnaire have been compiled in a confidential annex available upon request.