



D1.2 Data Management Plan

Deliverable No.	D1.2	Due Date	31/December/2021
Description	The Data Management Plan provides the main principles, as well as ethical and data protection strategies to be 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 is a living document that will be constantly updated during the lifetime of the project according to the changes that might happen at a project level and at the pilots' level.		
Type	Report	Dissemination Level	PU
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	aqesada@udgalliance.org
Stea-Maria Miteva	UDGA	smiteva@udgalliance.org

History

Date	Version	Change
26/10/2021	0.1	Creation of ToC
30/11/2021	0.2	Circulation of the questionnaire for collection of relevant inputs from relevant partners
09/12/2021	0.3	Update of content according to received assessment forms
14/12/2021	0.4	Circulation of the draft for collection of relevant inputs from Policy, Legal and Gender Board Members
24/12/2021	0.5	Final Draft submitted to review
14/01/2022	0.6	FORTH Peer-Review
07/02/2022	0.7	CERTH Peer-Review
14/02/2022	0.8	Peer review comments addressed, submitted to quality review
22/02/2022	0.9	Quality review comments received
21/03/2022	0.91	Final version ready for submission
28/03/2022	1.0	Final review

Key data

Keywords	Data; Data Protection; Data Management;
Lead Editor	Adrian Quesada Rodriguez; Stea-Maria Miteva
Internal Reviewer(s)	Daphne Plati (FORTH); Dimitra Triantafyllou (CERTH)

Abstract

This document describes the Data Management Plan (DMP) and serves as a guide for the partners of the ODIN project. This deliverable is the first version of the DMP, which outlines a framework for proper management of data processing within the project. Further, this document identifies the data which will be generated during ODIN's execution, and the already existing data used within the tasks. The findings leverage on inputs provided by the consortium, as the partners and pilots' managers will continue to update this deliverable. A second version of this document will be prepared at the end of the second year, updating the data processing activities and including an initial plan for exploitation and preservation. A final version of the DMP will be presented at the very end of the project and will include conclusions on the data processing and ODIN consortium agreements.

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.....	4
TABLE OF CONTENTS	5
LIST OF TABLES	9
LIST OF FIGURES.....	10
EXECUTIVE SUMMARY	11
1 INTRODUCTION	12
1.1 THE ODIN PROJECT: OVERVIEW.....	12
1.2 ABOUT THIS DELIVERABLE.....	13
1.3 CONTEXT OF THE DELIVERABLE	13
1.4 METHODOLOGY	14
2 OVERVIEW OF RESPONSIBILITIES.....	16
2.1 TASK MANAGEMENT WITHIN THE PROJECT AND THE PILOTS	16
2.1.1 <i>ODIN Ecosystem of Partners</i>	17
2.1.2 <i>Data Protection Officers (DPOs)</i>	17
2.2 CONTROLLER IDENTIFICATION AND INITIAL INSTRUCTION DEFINITION	18
2.3 PROJECT ETHICAL RISK ASSESSMENT AND DATA PROTECTION IMPACT ASSESSMENT (DPIA)	22
2.3.1 <i>ODIN Ethical Risk Assessment:</i>	25
2.3.2 <i>ODIN Opinion regarding need to perform DPIA:</i>	28
2.4 CONSENT FORMS	29
2.5 FINDINGS	30
3 GENERATED DATA IN ODIN.....	31
3.1 PURPOSE OF DATA GENERATION AND RELATION TO OBJECTIVES	31
3.2 TYPE AND FORMAT OF GENERATED DATASETS FOR ODIN	31
3.3 FINDINGS	37
4 PROCESSING OF EXISTING DATA.....	38
5 DATA STORAGE MANAGEMENT & RETENTION POLICY	41
6 TECHNICAL AND ORGANIZATIONAL MEASURES (TOMS) FOR SAFEGUARDING THE RIGHTS AND FREEDOMS OF THE DATA SUBJECTS	45
7 FURTHER PROCESSING OF PREVIOUSLY COLLECTED DATA	49
8 MAIN PRINCIPLES AND CONCEPTS OF DATA MANAGEMENT	51
8.1 GUIDELINES FOR GDPR COMPLIANT DEPLOYMENT OF AI, IOT AND ROBOTICS IN PILOTS	51
8.2 DATA PROTECTION PRINCIPLES	54
8.2.1 <i>Lawfulness and Fairness</i>	54
8.2.2 <i>Transparency and Information to Data Subjects</i>	55
8.2.3 <i>Purpose Limitation and Presumption of Compatibility</i>	55
8.2.4 <i>Data Minimization and Storage Limitation</i>	56
8.2.5 <i>Accuracy</i>	56

8.2.6	<i>Integrity and Confidentiality</i>	57
8.2.7	<i>Accountability</i>	57
8.3	ETHICAL PRINCIPLES	58
8.3.1	<i>Informed Consent</i>	59
8.3.2	<i>Approval by Research Ethics Committees</i>	59
8.3.3	<i>Scientific and Social Value</i>	59
8.3.4	<i>Purpose Limitation</i>	59
8.3.5	<i>Data Minimization</i>	60
8.3.6	<i>Use of Data obtained from the Online Environment and Digital Tools in Health-related Research</i>	60
8.3.7	<i>Reimbursement and Compensation for Research Participants</i>	60
8.3.8	<i>Recruitment of Affiliated Participants</i>	60
8.3.9	<i>Privacy and Confidentiality</i>	60
8.3.10	<i>Data Sharing</i>	60
8.3.11	<i>Vulnerable Persons and Groups</i>	61
8.4	DATA SUBJECT RIGHTS	61
8.4.1	<i>Right to Access</i>	62
8.4.2	<i>Right to Information</i>	62
8.4.3	<i>Right to Rectification</i>	62
8.4.4	<i>Right to Object</i>	62
8.4.5	<i>Right to Erasure</i>	63
8.4.6	<i>Right to Restriction of Processing</i>	63
8.4.7	<i>Right to Data Portability</i>	63
8.4.8	<i>Rights related to Automated Individual Decision-making and Profiling</i>	63
8.5	FAIR GUIDELINES FOR DATA MANAGEMENT	63
8.5.1	<i>Findability of Data</i>	63
8.5.2	<i>Accessibility of Data</i>	64
8.5.3	<i>Interoperability of Data</i>	65
8.5.4	<i>Reuse of Data</i>	65
9	IPR MANAGEMENT	66
9.1	INTELLECTUAL PROPERTY RIGHTS	66
9.1.1	<i>Copyright</i>	66
9.1.2	<i>Patents</i>	66
9.1.3	<i>Trademarks</i>	67
9.1.4	<i>Trade Secrets</i>	67
9.2	IPR MANAGEMENT WITHIN ODIN	67
9.2.1	<i>Ownership of Background Knowledge</i>	67
9.2.2	<i>Open-Source Access</i>	68
9.2.3	<i>IPR Conflict Resolution</i>	68
9.3	ODIN SOFTWARE IPR DIRECTORY	68
10	CONCLUSION AND FUTURE PLANS	69

APPENDIX A	DEFINITIONS AND GENERAL RECOMMENDATIONS.....	70
	<i>Data Controller.....</i>	<i>70</i>
	<i>Accountability.....</i>	<i>70</i>
	<i>Automated individual decision.....</i>	<i>70</i>
	<i>Biometric data.....</i>	<i>70</i>
	<i>Confidentiality.....</i>	<i>71</i>
	<i>Consent.....</i>	<i>71</i>
	<i>Cookies.....</i>	<i>71</i>
	<i>Data concerning health.....</i>	<i>71</i>
	<i>Data minimization.....</i>	<i>71</i>
	<i>Data mining.....</i>	<i>71</i>
	<i>Data protection authority.....</i>	<i>72</i>
	<i>Data Protection Impact Assessment (DPIA).....</i>	<i>72</i>
	<i>Data protection officer (DPO).....</i>	<i>72</i>
	<i>Data quality.....</i>	<i>72</i>
	<i>Data retention.....</i>	<i>73</i>
	<i>Data subject.....</i>	<i>73</i>
	<i>Data transfer.....</i>	<i>73</i>
	<i>Personal data.....</i>	<i>73</i>
	<i>Personal data breach.....</i>	<i>73</i>
	<i>Privacy.....</i>	<i>73</i>
	<i>Privacy by design.....</i>	<i>74</i>
	<i>Processing (of personal data, including sensitive data).....</i>	<i>74</i>
	<i>Processor.....</i>	<i>77</i>
	<i>Processor agreement.....</i>	<i>77</i>
	<i>Pseudonymisation.....</i>	<i>78</i>
	<i>Retention periods.....</i>	<i>78</i>
	<i>Special categories of personal data.....</i>	<i>78</i>
	OTHER RELEVANT CONCEPTS.....	78
	<i>Processing for the Purpose of Scientific Research.....</i>	<i>78</i>
	<i>Further processing.....</i>	<i>79</i>
	<i>Joint Controllership.....</i>	<i>79</i>
APPENDIX B	DATA MANAGEMENT AND ETHICS QUESTIONNAIRES.....	82
	B.1 DATA MANAGEMENT PLAN QUESTIONNAIRE.....	82
	B.2 ETHICS MANAGEMENT QUESTIONNAIRES.....	85
APPENDIX C	INFORMED CONSENT.....	87
	C.1 ESSENTIAL INFORMATION FOR PROSPECTIVE RESEARCH PARTICIPANTS.....	87
	INFORMATION SHEET.....	87
	C.2 SAMPLE INFORMATION CONSENT FORM.....	91
	CONSENT SHEET.....	91

APPENDIX D	HOW TO DETERMINE THE ROLES OF DATA CONTROLLER, DATA PROCESSOR AND JOINT CONTROLLERS IN THE PRAXIS	96
D.1	DATA CONTROLLER OR DATA PROCESSOR	96
D.2	JOINT CONTROLLERSHIP FLOWCHART	98
APPENDIX E	DECLARATIONS OF COMPLIANCE WITH NATIONAL REGULATIONS	100

List of tables

TABLE 1: DELIVERABLE CONTEXT	13
TABLE 2: DATA GENERATED BY THE PARTNERS IN DIFFERENT WORK PACKAGES FOR THEIR DELIVERABLES	32
TABLE 3: <i>PROCESSING OF EXISTING DATA</i>	38
TABLE 4: <i>PROCESSING OF EXISTING DATA: CERTH</i>	39
TABLE 5: <i>PROCESSING OF EXISTING DATA: UMCU</i>	40
TABLE 6: <i>DATA STORAGE MANAGEMENT & RETENTION</i>	42
TABLE 7: <i>TECHNICAL AND ORGANIZATIONAL MEASURES FOR DATA SUBJECTS' RIGHTS</i>	46
TABLE 8: <i>FURTHER DATA PROCESSING</i>	49

List of figures

FIGURE 1: THE POSITION OF D1.2 IN ODIN MANAGEMENT	12
FIGURE 2: DMP METHODOLOGY	15
FIGURE 4: WORK PACKAGE GOVERNANCE	16
FIGURE 5: ODIN STAKEHOLDER ANALYSIS.....	17
FIGURE 6: INFORMATION FLOW IN ODIN	31
FIGURE 7: STORAGE AND FLOW OF DATA.....	42
FIGURE 3: ODIN PLATFORM BLUEPRINT (SOURCE: D2.2).....	52
FIGURE 8: INDICATIONS FOR DATA CONTROLLERS AND DATA PROCESSORS IN THE GDPR.....	96

Executive Summary

The current document presents the first 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). The plan specifies the Data Governance and handling of personal and sensitive data during the project activities; outlining what types of data are expected to be generated and used, if and how it will be shared and made accessible internally and, after the lifetime of the project, externally for verification and re-use. The plan guides the partners how to store and protect data, considering pertaining ethical, privacy, and security issues. The guidelines on collecting and characterizing datasets follow the ethics, privacy and legal framework delivered in D8.2. All findings are based on the answers provided by the partners to dedicated Data Management Questionnaires.

The DMP covers the entire research data life cycle and is consistent with exploitation and Intellectual Property Rights (IPR) requirements. Particularly, sensitive and personal data of patients and participants will be kept strictly confidential and either anonymized or pseudonymized, to maintain compliance with General Data Protection Regulation (GDPR). Since this is the first iteration of the DMP, identified best practises will be further identified and updated in the following iterations. To facilitate the compliance, in Appendix C the deliverable provides templates for information sheets and consent forms to be tailored by partners to their needs and ensure GDPR-compliant data collection. Furthermore, each partner has been requested to formally state the compliance of their organization with not only the European legislation on data protection but also with complementary national obligations. Lastly, the DMP aims at establishing a common understanding of the GDPR principles, its goals, and requirements to the obliged entities. For this, Appendix D presents a guide for identifying whether an entity is a data controller or a processor, and which responsibilities their role incorporates.

1 Introduction

1.1 The Odin Project: Overview

The ODIN project focuses on identified hospitals’ critical challenges which will be faced 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.

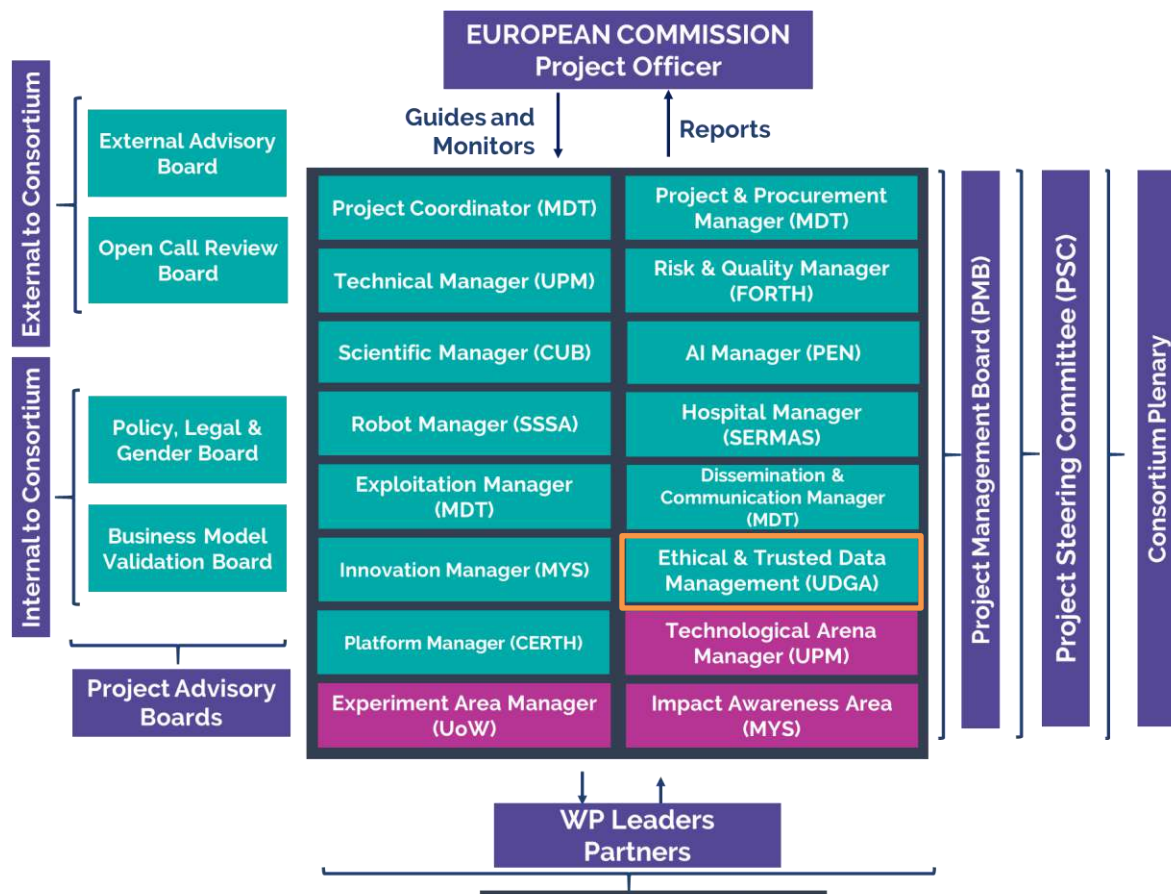


Figure 1: The position of D1.2 in ODIN Management

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).

Deliverable D1.2 is 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 aims at summarizing the data to be generated within the project and the envisioned data processing. The current deliverable is the first version of the plan and is produced at month 10. It is a recurrent live deliverable, which will be constantly updated according to partners’ inputs and will reflect on any changes regarding data generation, usage, processing, storage, and ethical management. A second version in month 24 will update the data processing activities and include the initial plan for exploitation and preservation. The deliverable’s final version, which will be produced in month 42, will include the final work done in terms of data processing in alignment with the ODIN consortium agreements.

1.3 Context of the Deliverable

Table 1. Deliverable context

PROJECT ITEM IN THE DOA	RELATIONSHIP
<p>Project Objectives</p>	<p>In providing a management plan for compliant handling of data in the scope of the ODIN project, the DMP contributes to the realization of the objectives, tightly dependent on a compliance with legal, ethical and security frameworks. In particular, the DMP suffices the requirements in O1 to support the interoperable and effective implementation of the decentralized ODIN platform; O2 to guarantee the delivery and scale-up of innovative services in accordance with national and European legal frameworks; and O4 to help set up an exploitation strategy for data, specifically in terms of delivery to European Data Space.</p>

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

Exploitable results	The deliverable presents a model for data management and will serve as a reference for the consortium. Exploitation strategy for open access data can be further explored outside the consortium.
Workplan	The deliverable will be constantly updated according to the DoA. Our partners will be encouraged to provide constant up-to-date inputs regarding their data processing activities. Pilots' progress in this regard will be monitored and documented.
Milestones	D1.2 is a key deliverable for the Preparation milestone.
Deliverables	D1.2 defines the Data Management plan of the project. It is also connected to other deliverables such as D8.2, D11.1, D11.2, and D11.3.
Risks	The constant update of information from the pilots will need to be monitored. Particular attention will need to be devoted to data sharing issues.

1.4 Methodology

The Data Management plan combines both data protection and ethical aspects of the compliant handling of data, lays down regulatory principles, and identifies best practises. For the purposes of the deliverable, a dedicated ethics and data protection questionnaire has been developed (Appendix B). The questionnaire leverages on GDPR principles, FAIR principles, and complementary data protection and ethical requirements (D11.1, D11.2, and D11.3). The questionnaire consists of two parts: 1) Part A, which asks questions on data generation, and 2) Part B, which demands inputs regarding the use of already existing datasets. The representatives of each partner organization within the ODIN consortium received the questionnaire in a digitalized form and were asked to provide their inputs.

These interactive activities are complemented by research on the GDPR and other applicable EU legislation (as comprehensively mapped in D8.2). The data management plan acknowledges and takes into account any complementary EU Member State legislation around the processing of special categories of data and demands declaration from partners that they abide by these rules and thus efficiently safeguard data subjects' rights.

The figure below describes the creation of the Data Management Plan. As outlined above, this is a living document, which incorporates best practices and main principles in the field of data protection and ethics; it offers mitigation strategies for various issues, including IPR management. Being a living document, the DMP presents the current state of partner's data management activities and anticipated actions. Identified issues and the effectiveness of applied mitigation measures will be further evaluated in the iterations of this deliverable. This is particularly relevant for partners, who have not yet fully identified and mapped their data processing activities at such an early stage of the project.

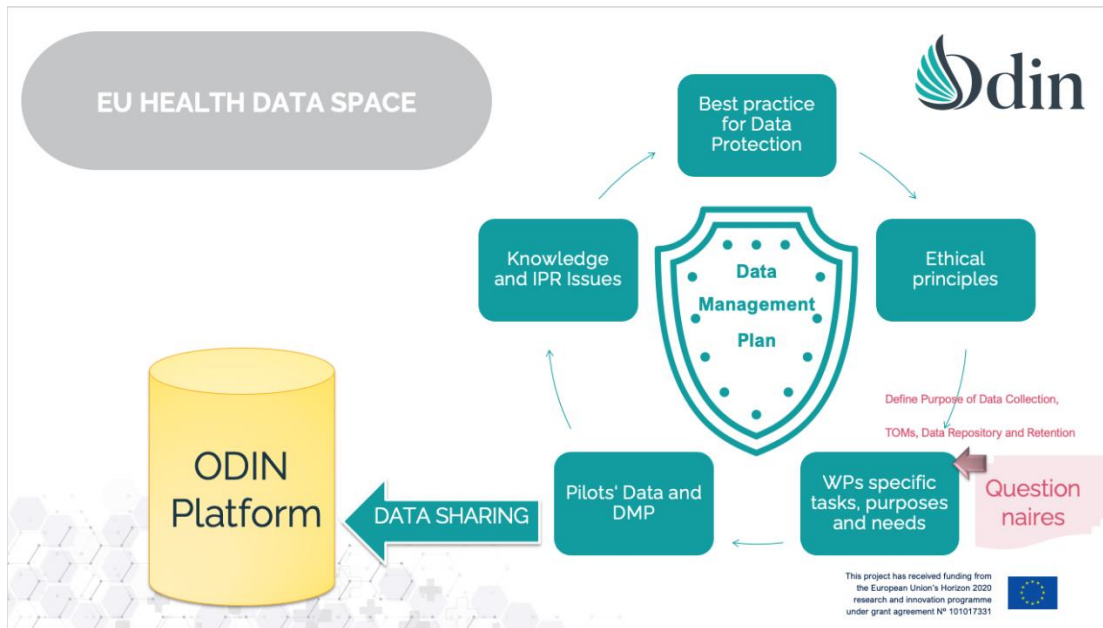


Figure 2: DMP Methodology

2 Overview of Responsibilities

2.1 Task Management within the Project and the Pilots

Firstly, each partner, including pilot owners, needs 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 need 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 dataflow mapping. In order to facilitate the identification of the roles of the partners, the current Data Management Plan has provided a guide (Appendix D) to help partners determine what their role in the personal data processing is, and what obligations follow.

For the definition of the data processing activities, partners have been provided with Data Management Questionnaires (Appendix B), which also provide explanations as to what is meant by “personal data”, “sensitive data”, etc. The understanding of the terminology and of the provisions of the Regulation is important in order to assure alignment in the communication within the consortium, but also to be able to correctly distinguish personal from non-personal data. As the work on local and general data management plans is understood as an ongoing work, the exercise in data mapping will continue over the course of the project. The figure below provides a high-level overview of the distribution of responsibilities and tasks among the different work packages.

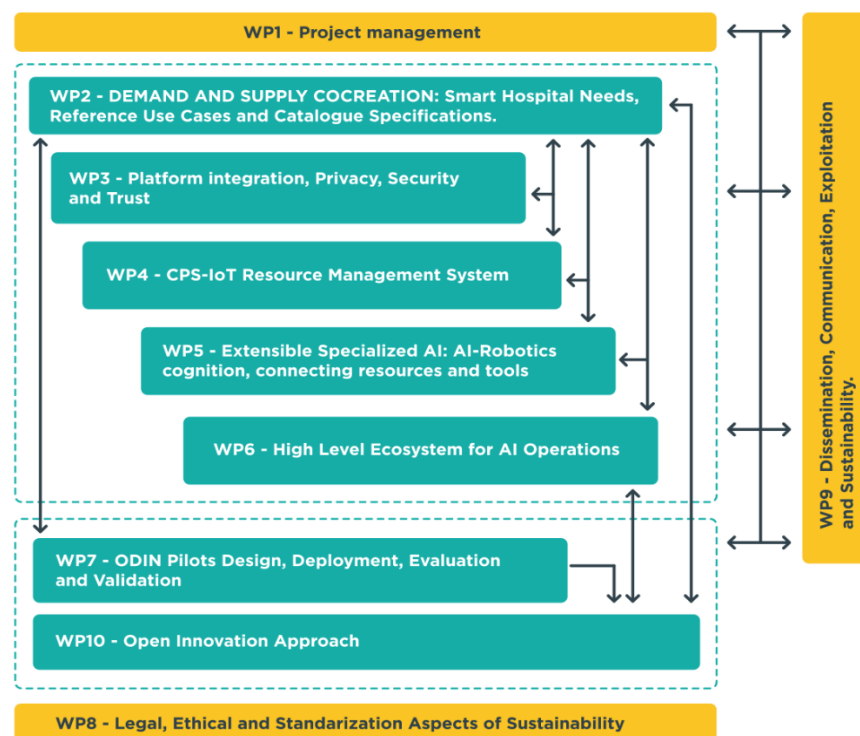
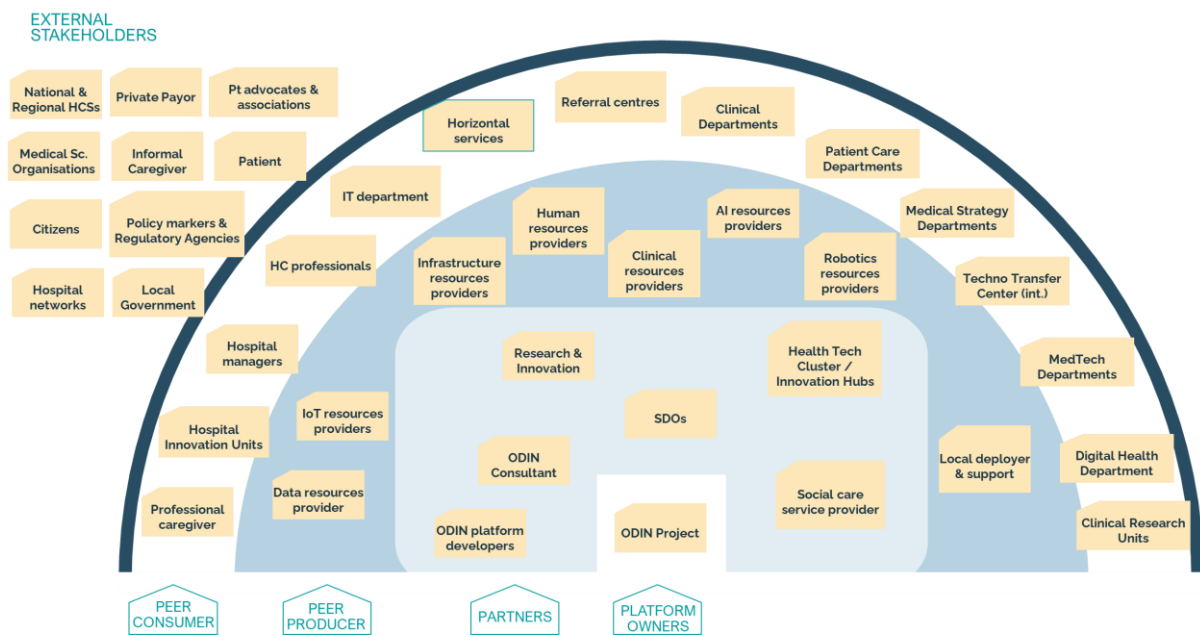


Figure 3: Work Package Governance

2.1.1 ODIN Ecosystem of Partners

The outcomes of T2.1 “Co-creation strategy, stakeholders’ definition and mapping” of Work Package 2 will complement 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 can 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.



Source: Medtronic, STAKEHOLDER MAPPING WORKSHOP (2nd Plenary Meeting)

Figure 4: ODIN Stakeholder Analysis

2.1.2 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 individuals’ rights. Each Data Controller (pilot) should have a clearly identified DPO. ODIN also has 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 and Ms. Stea Miteva, who are 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.

Local DPOs should report and work in close coordination with the researchers responsible of the different pilots and the project’s DPO. Thus, providing information about local DPOs in the data management questionnaires, and keeping it up to date, is of utmost importance.

2.2 Controller identification and initial instruction definition

The ODIN project’s implementation is divided into four phases, showcased in Figure 4 below.

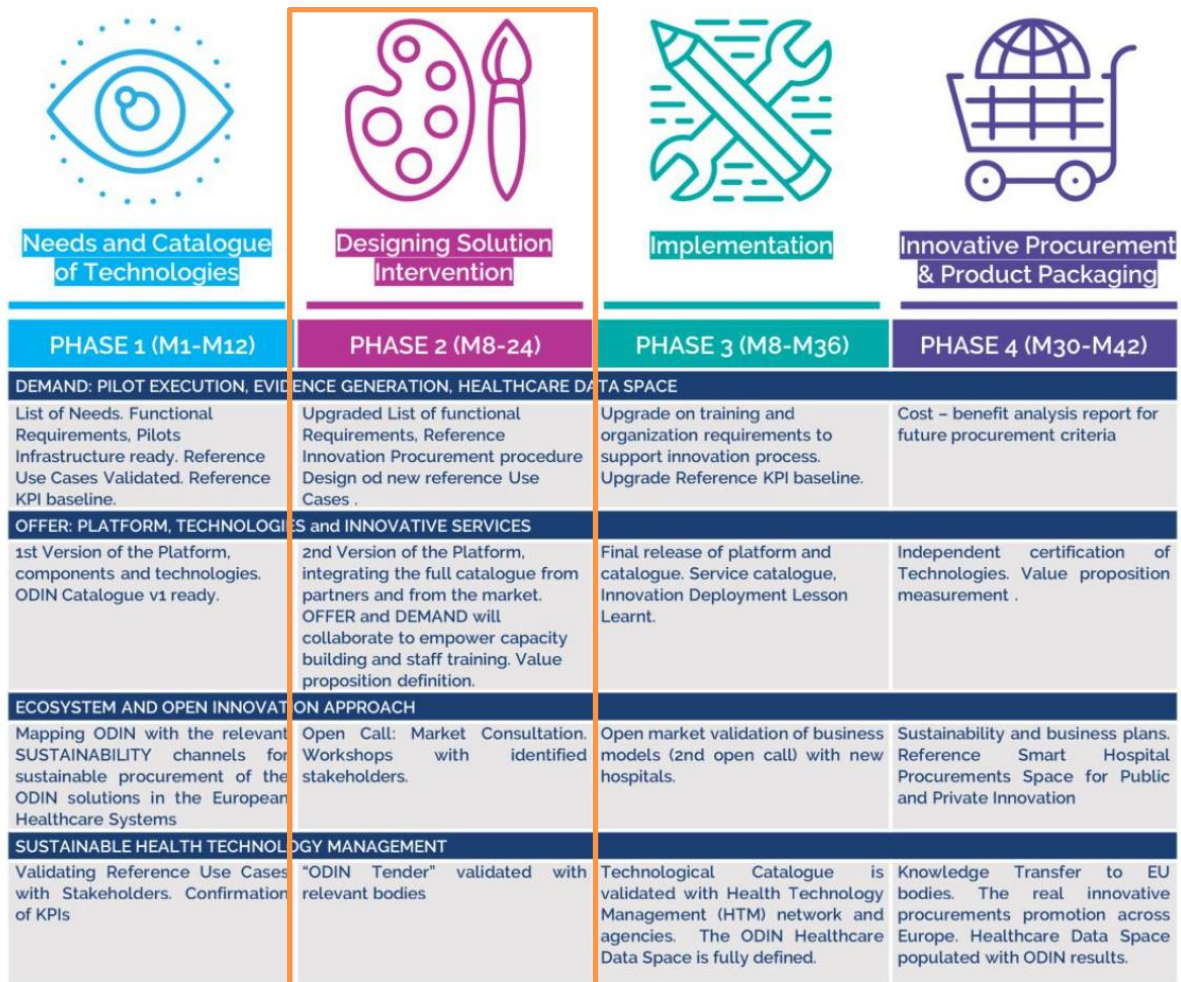


Figure 4: The ODIN Innovation Procurement Phases

During the first phase, the project identifies the demand in terms of pilots’ execution, evidence generation, and deployment of healthcare data space by compiling a list of needs, functional requirements, and preparing and validating reference use cases. An initial version of the platform, its compartments and technologies shall be prepared. The definition of the technology is a crucial step of the process, as it will allow to determine which privacy enhancing and safeguarding mechanisms need to be implemented, and how, i.e., deployment of an anonymization strategy. As the definition of technology is still ongoing, the document will be continuously updated, and identified risks and needs regarding the deployed technology will be described, and mitigation strategies will be proposed.

In a second phase of the project, new infrastructure/technology, according to the identified demand, will be integrated to the platform. Pilot solutions for eWorkers, eRobots, eLocation will be offered. The first round of open calls will ensure the necessary capacity building and training

through market consultation and workshops with identified stakeholders. For the carry-out of the workshops and interviews, which are related to collection of data, the current data management plan offers privacy-compliant approaches and mitigation strategies. The ethics management questionnaires, which shall be completed by pilot owners, should additionally provide details regarding the recruitment of participants.

The participating local responsible organizations are therefore to be understood as data controllers of the data (see figure below):

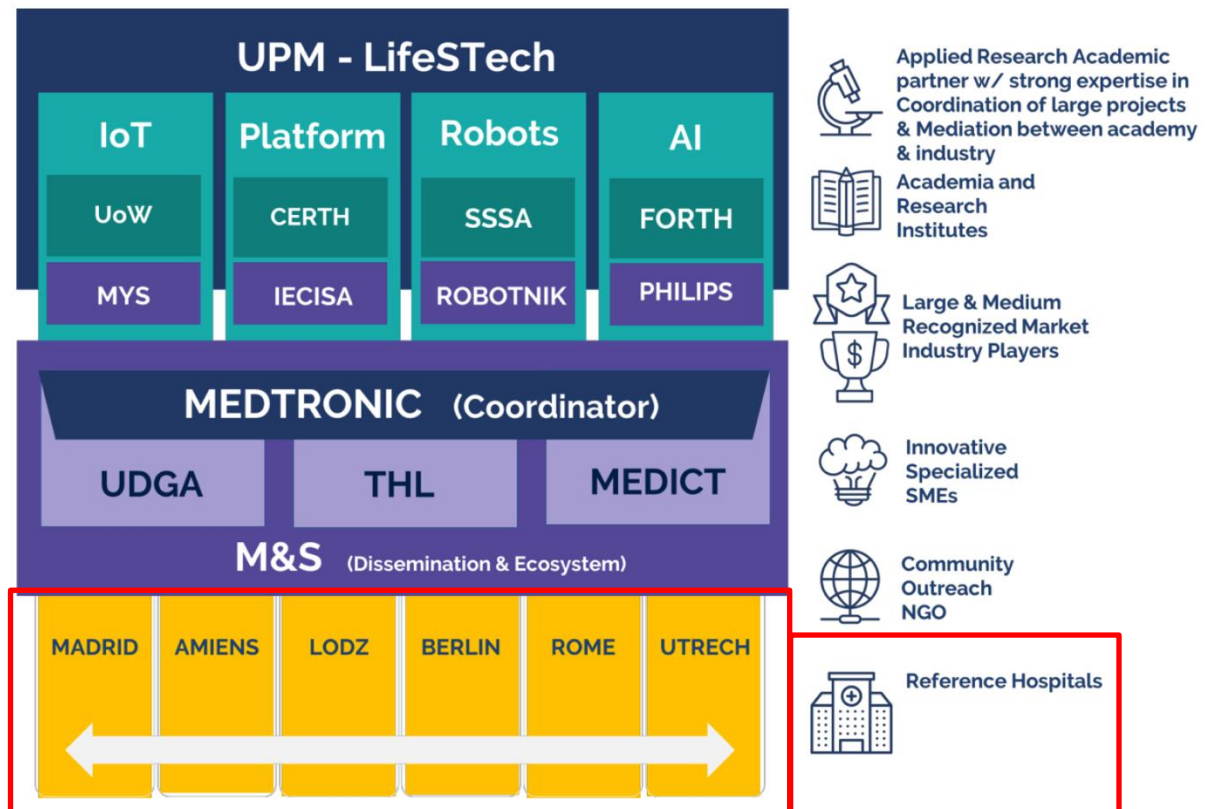


Figure 5: ODIN Consortium, represented by domain and organization

Health providers’ requirements and interests are two-fold: On one hand, there is a direct interest to ease access to data collected by healthcare providers to citizens and third parties, who could develop services out of it. On the other hand, there is a strict need to respect and preserve the privacy and the personal data of the participants. While the project will support the access to open data by third parties, it will abide to strict personal data protection policy in line with the EU General Data Protection Regulation (GDPR) and other applicable norms. Personal data protection compliance is part of the project’s requirements and will guide the architecture design. Personal data protection principles will determine and limit the data sharing. ODIN is committed to proactively ensure full compliance with the GDPR through a set of ad hoc policies, mechanisms, and tools.

Moreover, the project commits 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.

In the context of the ODIN project, a number of consortium partners (Beneficiaries as described in the Grant Agreement) may provide datasets with the aim to enable other partners to perform the project's described activities. Whenever these datasets include personal data, it is important to ensure no sharing of personal data is performed unless covered by adequate data sharing agreements (joint data controller agreement or data processing agreements). In this context, three potential scenarios can be identified:

- 1) No need for Data Sharing Agreement (individual Controllers): Processing of personal data is performed unilaterally by the partner which provides it (sole data controller, determines the means and purposes of processing), and only shares non-identifiable, anonymized data with the consortium;
- 2) Joint-controller agreement (Controller to Controller transfer of Personal Data): Personal data is introduced by a project partner with the express aim to share it amongst (some) of the project partners who will process it independently (not following specific instructions by the provider with regarding the processing of personal data), thus acting as joint controllers in accordance to a data sharing agreement;
- 3) Data Processing Agreement (Data Controller to data processor transfer of Personal Data): personal data is introduced and shared with certain partner(s) (data processors) who will process the data in line with express instructions from the partner which introduces this data (data controller) in line with a data processing agreement.

The core providers of (sensitive) personal data in the framework of the project will be the Pilot owners, which will act as data controllers for any data to be provided to the consortium from their infrastructure and/or network and will be the key responsible organizations to ensure 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 design phase of the pilots will enable the controllers to determine the means and purposes of any processing to be performed and to identify whether any other partner should be granted access to the data (see Appendix D). Upon the finalization of the pilot designs, the project will support the adoption of the relevant Data Sharing Agreements, which will be reported on the upcoming iteration of this deliverable.

General instructions for Data Controllers under the individual Controllers and Controller to Controller data transfer scenarios:

The following instructions should be considered by all Data Controllers in the framework of the ODIN project, as applicable:

- 1) Personal Data shall be accessed only for the purpose of the project and in line with the project's associated agreements (Grant Agreement, Consortium Agreement). No further processing of personal data by the partners for own purposes or for purposes of third parties is permitted unless permitted under the Data Protection Legislation (including as expressly permitted in the informed consent forms).
- 2) All personal data introduced, transferred, or processed in the project must be adequate in relation to the purposes (purpose limitation) of the ODIN project. No personal data shall be transferred or processed unless necessary (data minimization). Any further processing for archiving purposes in the public interest, scientific or historical research purposes or

statistical purposes should ensure compliance with both European Data Protection Legislation and National Data Protection guidance and regulations.

- 3) Personal data shall only be retained in a form which permits the identification of data subject as long as this is absolutely necessary for the performance of the project's objectives and purposes. All personal data should be pseudonymized as soon as possible and anonymized if possible to carry out the project's objectives. No personal data shall be disclosed by the project partners unless anonymized.
- 4) Any Controller introducing or transferring personal data shall inform the data subjects about the transfer of their personal data to and the expected processing activity to be performed by the accessing Controller. The accessing Controller shall provide the introducing partner with all information about the accessing and Processing of the Personal Data which the introducing Controller requests to inform the Data Subjects according to applicable law.
- 5) Both introducing and accessing Controllers respectively are the responsible contact for any requests by the Data Subjects, e.g. for information, correction or deletion of the Personal Data or for an objection to the Processing, the case being.
- 6) The introducing and accessing Controller shall take all reasonable technical and organizational measures necessary to protect the introduced Personal Data against unauthorized or unlawful Processing and against accidental loss, destruction of or damage to such Personal Data.
- 7) The introducing Controller is entitled to perform an audit of the data processing performed by any accessing Controller during the term of the project. Any accessing Controller is obliged to perform internal audits to ensure compliance with its obligations.

General instructions for Data Processors under the Controller to Processor data transfer scenario:

- 1) The introducing Controller shall only use those Processors that provide sufficient guarantees to implement appropriate technical and organizational measures to ensure compliance with data protection legislation and protection of Data Subject rights.
- 2) The processor shall not engage any sub-processor without prior specific or general written authorisation of the Controller. In the case of general written authorisation, the Processor shall inform the Controller of any intended changes concerning the addition or replacement of other Processors, thereby giving the Controller the opportunity to object to such changes. Where the accessing Beneficiary/Third Party as Processor does engages another Processor for carrying out specific processing activities on behalf of the Controller, the same data protection obligations as set out in the contract or other legal act between the Controller and the Processor shall be imposed on that other processor by way of a contract or other legal act, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Data Protection Legislation. Where that other Processor fails to fulfil its data protection obligations, the initial Processor shall remain fully liable to the Controller for the performance of that other Processor's obligations.
- 3) The Processor shall process Personal Data exclusively in the name of and in accordance with the documented instructions of the Controller, including with regard to the transfer of Personal Data to a third country (i.e. a country outside the European Economic Area). The processing shall be governed by a contract or other legal act, that is binding on the Processor with regard to the Controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of Personal Data and categories of Data Subjects and the obligations and rights of the Controller.

- 4) The Processor will, by appropriate technical and organisational measures, assist the Controller insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights, taking into account the nature of the processing and will assist the Controller towards ensuring compliance with the obligations relating to security of processing, data breach notification, data protection impact assessment and prior consultation.
- 5) The Processor will report to the Controller any data breach without undue delay and at the latest within 24 hours after having become aware of it and provide the Controller with all relevant information in that regard.
- 6) The Processor shall return all the Personal Data to the Controller after the end of the provision of services relating to processing and delete existing copies (unless applicable law requires storage of the Personal Data).
- 7) The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations set forth in Data Protection Laws and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the Controller

2.3 Project ethical risk assessment and Data Protection Impact Assessment (DPIA)

A DPIA is a process designed to describe the data-processing, assess its necessity and proportionality, and help manage the risks to the rights and freedoms of natural persons by assessing them and determining the measures to address them.

The DPIA is required when the processing is “likely to result in a high risk to the rights and freedoms of natural persons”. “The rights and freedoms” of data subjects primarily concerns the rights to data protection and privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience, and religion.

The WP29's guidelines seek to promote the development of:

A) A common European Union list of processing operations for which a DPIA is mandatory

- Evaluation or scoring, including profiling, and predicting, in particular involving “aspects concerning the data subject's performance at work, economic situation, **health**, personal preferences or interests, behaviour, location or movements”.
- Automated decision-making with legal or similar significant effect, i.e. data processing leading to decisions on data subjects producing legal effects concerning the natural person or which similarly significantly affects them.
- **Sensitive data or data of a highly personal nature. This includes special categories of personal data as defined in Article 9 of the GDPR. For instance, a general hospital keeping patients' medical records would fall under this category.**
- Data processed on a large scale, as already defined.
- Matching or combining datasets, originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject.
- Data concerning vulnerable data subjects, such as minors.

- **Innovative use or applying new technological or organisational solutions**, like combining use of fingerprint and face recognition for improved access control, etc. For example, **certain “Internet of Things” applications** could have a significant impact on individuals’ daily lives and privacy, and, therefore, would require a DPIA.
- When the processing in itself “prevents data subjects from exercising a right or using a service or a contract”. This includes processing that aims at allowing, modifying or refusing data subjects’ access to a service or entry into a contract.
- A DPIA can also be useful for assessing the data protection impact of a technology product, for example a piece of hardware or software, where this is likely to be used by different data controllers to carry out different processing operations.

In most cases, a data controller can consider that a **processing meeting at least two criteria would require a DPIA** to be carried out. Nonetheless, that should be examined on an ad hoc basis, as in some cases, a data controller can consider that a processing meeting only one of these criteria requires a DPIA. Conversely, a processing operation may correspond to the above-mentioned cases and still be considered by the controller not to be “likely to result in a high risk”. In such cases the controller should justify and document the reasons for not carrying out a DPIA, as well as recording the views of the DPO.

The WP29 also focuses on providing examples of cases meeting the above criteria. For instance, storage for archiving purpose of pseudonymised personal sensitive data concerning vulnerable data subjects of research projects or clinical trials involves sensitive data, concerning vulnerable data subjects and prevents data subjects from exercising a right or using a service or a contract. Therefore, a DPIA would be required.

The mere fact that the conditions triggering the obligation to carry out a DPIA have not been met does not, however, diminish controllers’ general obligation to implement measures to appropriately manage risks for the rights and freedoms of data subjects.

B) A common EU list of processing operations for which a DPIA is not necessary

- Where the processing is not “likely to result in a high risk to the rights and freedoms of natural persons”.
- When the nature, scope, context and purposes of the processing are very similar to the processing for which DPIA have been carried out.
- When the processing operations have been checked by a supervisory authority before May 2018 and their specific conditions have not changed.
- Where a processing operation, pursuant to point (c) or (e) of Article 6 par. 1 GDPR, has a legal basis in EU or Member State law, where the law regulates the specific processing operation and where a DPIA has already been carried out as part of the establishment of that legal basis.
- Where the processing is included on the optional list, established by the supervisory authority, of processing operations for which no DPIA is required.

C) Common criteria on the methodology for carrying out a DPIA

- The DPIA should be carried out **“prior to the processing”**, starting as early as is possible even if some of the processing operations remain unknown. The fact that the DPIA may need to be updated once the processing has officially commenced does not constitute a valid reason for postponing or not carrying out a DPIA.

- **Updating the DPIA throughout the lifecycle project is required to maintain compliance.**
- **The controller is responsible for ensuring that the DPIA is carried out.** If the processing is wholly or partly performed by a data processor, the processor should assist the controller in carrying out the DPIA and provide any necessary information.
- The controller must also **seek the advice of the Data Protection Officer (DPO)**, where designated and this advice, along with the decisions taken by the controller, should be documented within the DPIA. The DPO should also monitor the performance of the DPIA.
- The controller must “seek the views of data subjects or their representatives”, “where appropriate”.
- A DPIA must at least include “a description of the envisaged processing operations and the purposes of the processing”, “an assessment of the necessity and proportionality of the processing”, “an assessment of the risks to the rights and freedoms of data subjects”, “the measures envisaged to address the risks and “to demonstrate compliance with the GDPR”.
- Compliance with a code of conduct must be taken into account when assessing the impact of a data processing operation. Certifications, seals and marks aiming at demonstrating compliance with the GDPR of such operations by controllers and processors, as well as Binding Corporate Rules, should also be considered.
- The DPIA implementation is scalable, in the sense that even a small data controller can design and implement a DPIA suitable for their processing operations.

D) Common criteria for specifying when the Supervisory Authority shall be consulted

- Where a DPIA reveals high residual risks, the data controller will be required to seek prior consultation for the processing from the supervisory authority.
- Whenever Member State law requires controllers to consult with, and/or obtain prior authorisation in relation to processing by a controller for in the public interest, including processing in relation to social protection and public health.

E) Recommendations, where possible, building on the experience gained in EU Member States

- Where it is not clear whether a DPIA is required, the WP29 recommends that it is carried out nonetheless as it is a useful tool in controllers’ path to compliance with data protection law.
- **Publishing a DPIA is not a legal requirement of the GDPR.** However, controllers should consider publishing at least parts, such as a summary or a conclusion of their DPIA, to help foster trust in the controller’s processing operations and demonstrate accountability and transparency.

The WP29 confirms that a **single DPIA could be used to assess multiple processing operations that are similar in terms of nature, scope, context, purpose, and risks**. This might be the case where similar technology is used to collect the same sort of data for the same purposes. This may also be applicable to similar processing operations implemented by various data controllers. In those cases, a reference DPIA should be shared or made publicly accessible, measures described in the DPIA must be implemented, and a justification for conducting a single DPIA must be provided. Moreover, the said DPIA should set out which party is responsible for the various measures mentioned, while each data controller should express their needs and share useful information without either compromising secrets or disclosing vulnerabilities.

Finally, the WP29 proposes a **list of criteria** in Annex 2, which data controllers can use to assess whether or not a DPIA, or a methodology to carry out a DPIA, is sufficiently comprehensive to comply with the GDPR, namely:

- a systematic description of the processing is provided (Article 35(7)(a)):
 - nature, scope, context and purposes of the processing are taken into account (recital 90);
 - personal data, recipients and period for which the personal data will be stored are recorded;
 - a functional description of the processing operation is provided;
 - the assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels) are identified;
 - compliance with approved codes of conduct is taken into account (Article 35(8));
- necessity and proportionality are assessed (Article 35(7)(b)):
 - measures envisaged to comply with the Regulation are determined (Article 35(7)(d) and recital 90), taking into account:
 - measures contributing to the proportionality and the necessity of the processing on the basis of:
 - specified, explicit and legitimate purpose(s) (Article 5(1)(b));
 - lawfulness of processing (Article 6);
 - adequate, relevant and limited to what is necessary data (Article 5(1)(c));
 - limited storage duration (Article 5(1)(e));
 - measures contributing to the rights of the data subjects:
 - information provided to the data subject (Articles 12, 13 and 14);
 - right of access and to data portability (Articles 15 and 20);
 - right to rectification and to erasure (Articles 16, 17 and 19);
 - right to object and to restriction of processing (Article 18, 19 and 21);
 - relationships with processors (Article 28);
 - safeguards surrounding international transfer(s) (Chapter V);
 - prior consultation (Article 36).
- risks to the rights and freedoms of data subjects are managed (Article 35(7)(c)):
 - origin, nature, particularity and severity of the risks are appreciated (cf. recital 84) or, more specifically, for each risk (illegitimate access, undesired modification, and disappearance of data) from the perspective of the data subjects:
 - risks sources are taken into account (recital 90);
 - potential impacts to the rights and freedoms of data subjects are identified in case of events including illegitimate access, undesired modification and disappearance of data;
 - threats that could lead to illegitimate access, undesired modification and disappearance of data are identified;
 - likelihood and severity are estimated (recital 90);
- measures envisaged to treat those risks are determined (Article 35(7)(d) and recital 90);
- interested parties are involved:
 - the advice of the DPO is sought (Article 35(2));
 - the views of data subjects or their representatives are sought, where appropriate (Article 35(9))

2.3.1 ODIN Ethical Risk Assessment:

The Grant Agreement (Page 142) requires the evaluation of the ethics risks associated with the ODIN project and the development of an opinion on whether a DPIA is required. In order to

determine the potential ethical impact of the ODIN project, the key ethical principles to be considered must be first identified²:

- 1) Respect for confidentiality and privacy: beyond legal compliance, the moral and ethical obligation to protect data subjects is a key guiding element to be considered by the project. Compliance with this principle is the core element to be secured through the performance of all data protection compliance activities, including a DPIA.
- 2) Beneficence: an overall commitment to protect the individuals from harm and ensure their well-being.
- 3) Justice: the fair and equal treatment of participants and data subjects, including the need to ensure inclusion, non-stigmatization and equality.
- 4) Respect for Persons: the respect of human autonomy and dignity, including respect of participant's will, information and self-determination.
- 5) Transparency: the need to provide open and transparent information to participants at all stages of the project.
- 6) Sustainability: a requirement to ensure the sustainability of the proposed solutions in order to ensure the continued viability of the benefits offered to participants while minimizing potential impacts the developed solutions might have on society and the environment.

When assessing the potential ethical impacts of the ODIN project, a number of questions should be considered, namely:

- 1) Does this platform threaten the freedom of individual humans? A: No
- 2) Does this platform alter an individual's freedom of movement? A: No
- 3) Does this platform interfere intentionally with the formation of expression of beliefs? A: No
- 4) Does this platform threaten the natural equality of persons? A: No
- 5) Does this platform restrict the exercise of a dignified human life? A: No
- 6) Will this platform reduce the chance of life choices of individuals in ways they are not fully aware of? A: No
- 7) Does this platform seek to change the way in which individuals reason? A: No
- 8) Will this platform restrict access to information? A: No
- 9) Will this platform promote specific decision-making schemes the users will not be aware of? A: No
- 10) Does this platform alter the exercise of human moral conscience? A: No
- 11) Will this platform promote specific visions of a good life? A: No
- 12) Is this platform explicitly designed to create or exacerbate inequalities between individuals or groups? A: No

² Based on the work of the PICASO project, D3.3. Ethical Guidelines.

- 13) Are the expected benefits divided between groups for reasons not associated with differences in use? A: No
- 14) Is this platform intended to create tiers of persons on the basis of social, international, or political factors? A: No
- 15) Does this limit the rights of any individuals or groups based upon race? A: No
- 16) Does this limit the rights of any individuals or groups based upon biological sex? A: No
- 17) Does this platform restrict the enjoyment of basic human rights? A: No
- 18) Does this limit the natural life of an individual? A: No
- 19) Is this designed to enhance or augment the natural life of an individual? A: No
- 20) Does this restrict an individual's opportunity to exercise liberties? A: No

As noted in the EDPB guidelines, in order to determine whether the ODIN Project's controllers should perform a DPIA, the project should consider whether the processing is likely to result in a high risk to the rights and freedoms of natural persons. In the context of this deliverable (and the associated requirement towards this action on D11.2 POPD requirement No. 2), this assessment will be simplified, as the performance of DPIAs by the data controllers is expressly required by the ODIN Grant Agreement (Section 5.1.1.1, Page 310).

Summary of personal data collected by ODIN Partners:

- Robotnik: no personal data collected
- SERMAS: Personal data: WP7 UC 1: information concerning material and equipment consumptions and purchases for a yet to be defined medical procedure, data from the patients who undergo that procedure (sociodemographic, hospital intake and leave dates, procedure outcomes, successive hospital intakes; WP7 UC7: Video image of a hospital area (either emergency service or a surgical area); geographical position of equipment and personnel/patients (RFID).
- M&S: WP9 contact list
- MySphera: no personal data collected nor processed
- THL: no personal data collected nor processed
- CERTH: WP5 T5.2, video (hospital areas), depth information (derived from video)
- FORTH: WP6 retrospective (data that have already been collected by patients from the clinical partners serving as data providers) or prospective patient data for generation of AI models to fulfill the pilots requirements (Prospective are new data from new patients of the clinical partners (i.e., patients for whom no data has been collected and thus provided as part of the retrospective data)).
- UMCU: UC3: patient data from patients that are using the Luscii app
- INETUM: No data provided
- UPM: T2.4: participant data through interviews and workshops; t7.1 pilot data from pilots (questionnaires); T10.3: data from open call submissions (participant forms); T3.3.: user data (credentials); T4.6: metric data (logs, IP address); WP5: interaction to users with social robots.
- CUB: WP7/WP8/WP9. Questionnaires including medical data and economic data, interviews

- PEN: de-identified patient data from WP6 and pilots for analytic and AI model generation.
- UoW: Pilot representative information
- UCBM: WP7: data collected by y clinical staff for registration of consent to participate in the experimental studies (name, surname, age, patient status, pathology, consent to participate, etc.) in accordance with the provisions of the UCBM Ethics Committee and the current laws about processing of personal data and conducting clinical studies (WP7). Furthermore, there will be other data collected automatically by robotic/AI systems during the carrying out of the validation activities foreseen in the ODIN project (i.e. WP7). They include, for example, trajectories traveled during navigation tasks and performed during grasping tasks by the robot, patient ID, face recognition data, annotation of the level of food intake by the patient, score obtained by the patient during the execution of tasks rehabilitation, compliance with oxygen intake prescriptions (WP5 and WP7).
- SSSA: WP5: data concerning robotics activities. Data will be generated into the WP5 also data coming from other technical WPs will be processed. Data will be used in real-time or wired/wireless transmitted for being stored into Hospital's ICT infrastructure. So far, Data to be considered into robotics activities regard: 1) 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.; 2) 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..); 3) 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).
- MEDEA: No personal data collected nor processed
- UDGA: Partner representative information
- MDT: Partner representative information (WP2, WP8, WP10) , interview results (WP2), data collected through workshops and open calls (WP10)
- MUL: IoT Data from tagging devices (WP7); Data related to clinical staff and patients (WP7); Electronic health record data (WP7) towards development and implementation of AI solutions (UC2, UC6; UC7)

Key outcomes:

Identified risk factors requiring the performance of a DPIA by the controllers include the collection and processing, by some of the ODIN project partners, of sensitive health data (EHR data). The project's nature and the technologies used to fulfil the DoA requirements intrinsically fall under the "innovative use or applying new technological or organizational solutions" mentioned by EDPB. This element is sufficient to form an informed opinion regarding the need to perform a DPIA.

2.3.2 ODIN Opinion regarding need to perform DPIA:

Based on the results of the ODIN Ethical Risk Assessment, the guidance from EDPB, and the express dispositions on this subject found in the Grant Agreement Section 5.1.1.1 (Page 310), every Data Controller in the ODIN project will be required to perform a DPIA. The results of the performed DPIAs will be shared with the project's Ethical and Trusted Data Manager and with the

Legal and Ethics Board for discussion, evaluation, and documentation. The results of this DPIA will be reported in the upcoming iterations of this DMP.

2.4 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.³ 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 knowledge. Hence, sufficiently informing participating individuals about their engagement in scientific (or medical) research activities is imperative. On a more theoretical note, the ethical requirement of “informed consent” is to be distinguished from the consent as a legal basis for lawful data processing in Art. 6(1)(a) GDPR.

The following principles, combining the provisions of the Oviedo Convention⁴, the Declaration of Helsinki⁵, outline the essential information for prospective research participants to obtain an informed consent:

1. Every precaution must be taken to **protect the privacy of research subjects** and the confidentiality of their personal information. Participants should be informed about the safeguards taken to ensure their privacy and confidentiality of records. They should be also informed about any limits to safeguard the confidentiality, and possible consequences of such breaches.
2. An intervention in the health field may only be carried out after the person concerned has given **free and informed consent** to it.⁶ Although it may be appropriate to consult family members or legal representatives, no individual capable of giving informed consent may be enrolled in a research study unless he, she or they freely agree.
3. For a potential adult research subject incapable of giving informed consent, the informed consent ought to be sought from the **legally authorised representative**. It should be ensured that the research study is solely intended to promote the health of the group represented by the potential subject; cannot instead be performed with persons capable of providing informed consent; and entails only a **minimal risk** or minimal burden for the participants.
4. According to the law, a **minor** does not have the capacity to consent to an intervention themselves, the intervention may only be carried out with the authorisation of their **legal guardian** or representative. The **opinion of the minor** shall be taken into consideration as an increasingly determining factor in proportion to his or her **age and degree of maturity**.

³ 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_questionnaire_research_final.pdf.

⁴ 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>.

⁵ 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/>.

⁶ Please note the differentiation between the ethical requirement of informed consent and the legal basis in Art. 6(1)(a) GDPR.

5. Some groups and individuals are **particularly vulnerable** and may have an increased likelihood of being wronged or of incurring additional harm. All vulnerable groups and individuals should receive specifically considered **protection**. Medical research with a vulnerable group is only justified if the research is responsive to the health needs or priorities of this group and the research cannot be carried out in a non-vulnerable group. In addition, this group should stand to benefit from the knowledge, practices or interventions that result from the research.
6. The participant shall **beforehand** be given appropriate information as to the **purpose and nature of the intervention as well as on its consequences and risks**, including the anticipated benefits and potential risks of the study and the discomfort it may entail, post-study provisions and any other relevant aspects of the study. Each potential subject must be adequately informed of the **aims, methods, sources of funding**, any possible **conflicts of interest**, institutional affiliations of the researcher.
7. The person concerned may freely **withdraw consent** at any time without penalty or loss of benefits to which he or she would otherwise be entitled.
8. The participant should be informed about the **expected duration** of their participation (including number and duration of visits to the research centre and the total time involved) and the possibility of early termination of the trial or of the individual's participation in it.
9. Participants have the right to be informed about the **outcomes of the study**.
10. The participants have the **right of access to their clinically relevant data** obtained during a study on demand (unless the research ethics committee has approved temporary or permanent non-disclosure of data, in which case the participating individual should be informed of and given the reasons for such non-disclosure).

Pilots and other partners in the role of data controllers need to prepare information sheets and consent forms to be filled out by participating individuals. Appendix B offers a sample information sheet as well as a sample consent form, which contain all the ethical and legal requirements for sufficiently informing data subjects regarding their data processing and allow them to provide an informed consent. The fields marked in yellow in the sample forms need to be tailored according to the concrete needs and goals of the activity. The ODIN data controllers are free to choose to use the sample form provided in this data management plan, or to use an own equivalent.

2.5 Findings

All the researchers involved in ODIN will comply with and follow the principles outlined by the GDPR, European and International Instruments in the fields of data protection, and ethical provision on protection of individuals with regard to the processing of personal data and on the free movement of such data. Medical data will be deposited in anonymised form which is allowed by the informed consent signed by study participants from the user groups. All participants are made aware if their collected will be shared with other research collaborators; nevertheless they are ensured that their personal data is kept confidential at all times. The databases that hold confidential data on participating subjects sit on a secure network and do not have an internet (HTTP) connection so as not to compromise the data. Furthermore, technical procedures are in place to monitor what data is entered and exported to ensure there is no breach of this. Measures will be taken to ensure data security at each pilot site.

The project invites the pilots and takes itself into consideration the best practices developed in the context of the other LSPs projects.

3 Generated Data in ODIN

3.1 Purpose of Data Generation and Relation to Objectives

In the context of the ODIN project, personal data are processed with the aim of working on solutions with technologies for the better quality of life and (health) care. The purpose of the treatment is to carry out the management of stakeholder participation in the project. Likewise, the data may be processed to develop ODIN's own dissemination activities or to send information about participation in the project-to-project users.

Personal data of participants will only be used for the development of the implementation in the region where the ODIN project is developed (please refer to figure 5 for the geographical regions), being stored with all the possible guarantees of confidentiality and privacy.

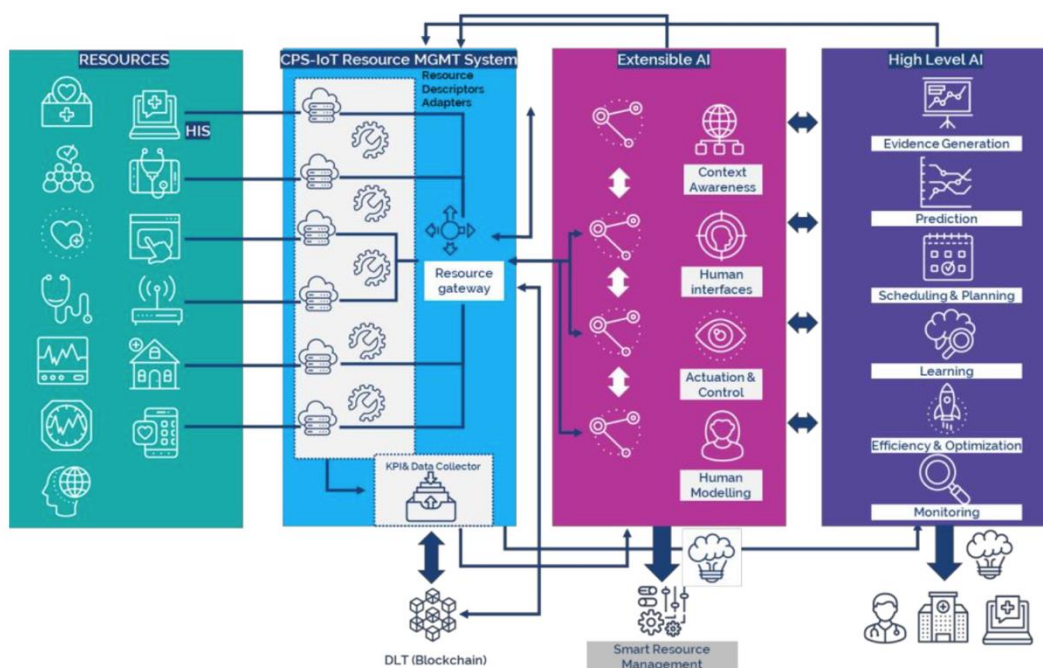


Figure 5: Information Flow in ODIN

3.2 Type and Format of Generated Datasets for ODIN

Data in the context of ODIN are collected at the project level by non-pilot owners and at the pilots' level by pilot-owners. In the context of ODIN, data is 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 table presents the datasets which each partner will generate, irrespective of their personal data protection relevance. 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.

Table 2: Data generated by the partners in different work packages for their deliverables

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 towards Public Procurement Processes	.docx
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;
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
ROBOTNIC		Data related to the movement of the robot and its commands	JSON format

MYS	WP4	<p>Technical requirements that are needed to achieve Use Case objectives from each Work Package.</p> <p>Opinions about the type of documentation and support service levels that partners can offer.</p> <p>Designs of the ODIN architecture.</p>	<p>Free text from datasheet surveys.</p> <p>Free text documentation and images of the designs.</p>
THL	WP5, T5.3	Technical data related to robots' operation and status	Robotic data formats will be custom defined through the ROS 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	Possible format will include .csv or .txt.

		modules (e.g., positions, velocities, forces, torques, RGB-D camera data).	
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.
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
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	To be defined
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 	.xlsx or .docx

		<ul style="list-style-type: none">the impact on hospital management and cost effectiveness of the solutions according to specific identified KPIs	
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 .docs

3.3 Findings

Data are a central component of the research project. At the project level WPs will mainly manage data related to the production of the different deliverables. As the project is still in an early stage, there is a notable difference in the preparation and clarify around required data to be collected and processed for the individual purposes set by each partner. Although there are several work packages and tasks, where the concrete data format and type is still to be identified, a positive commitment to ensuring anonymization, pseudonymization, purpose limitation and data minimization is visible from the provided responses to the questionnaires.

4 Processing of Existing Data

In order to determine, if and what previously available data will be processed by the consortium members, the following table has been provided to be filled out by all partners.

Table 3: Processing of Existing Data

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>
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>

In principle, as outlined in the previous sections of the current document, the processing of an already existing dataset for scientific research, is permitted under the GDPR. The processing activities and the already existing datasets are nevertheless subject to conditions such as appropriate safeguards, technical and organizational measures, pseudonymization, etc. A general good practice is, whenever possible, to share only anonymized or pseudonymized data when reusing already existing data sets, and, in case of pseudonymized data, the researcher should not receive the link file, which will possibly allow re-identification.

For the reuse of special categories of personal data (Art. 9(2)(j) GDPR) for the purposes of academic research, necessary and proportionate safeguarding measures should be undertaken in order to be compliant.

As per Art. 14 (5)(b) GDPR, the data subjects have the right to be informed immediately about the processing if personal data have not been received from the data subject unless this requires a disproportionate effort. In the latter case, the data subject must be informed either publicly or by means of a privacy statement.

The current analysis is carried-out on a per-partner basis. Two partners from ODIN's consortium, CERTH and UCBM, will process already existing datasets.

In the case of CERTH (see table below), the existing datasets containing personal data will be collected from the source YouTube, which grants public access. As the datasets are licensed under a Creative Common Attribution, no specific permission is required. The datasets will be processed for a specifically defined purpose to “*train baseline deep neural network models to perform human action recognition in hospital environments*”, in line with CERTH's obligations under WP5, Task 5.2. The datasets are stored at CERTH's specialized machines on their own premises, where technical and organizational measures for safeguarding of data subjects' rights and freedoms are implemented.

Table 4: Processing of Existing Data: CERTH

	Please provide your answers in this column:
Dataset(s) name	Kinetics (400/600/700)
Dataset(s) description	A collection of large-scale, high-quality datasets of URL links of up to 650,000 video clips that cover 400/600/700 human action classes, depending on the dataset version. The videos include human-object interactions such as playing instruments, as well as human-human interactions such as shaking hands and hugging. Each action class has at least 400/600/700 video clips. Each clip is human annotated with a single action class and lasts around 10 seconds.
Personal Data	Yes. The dataset is depicting humans performing actions in various situations during their daily life.
Purpose	Train baseline deep neural network models to perform human action recognition in hospital environments
Data format	Video format, either .mp4 or .avi.
Data Storage	At specialized machines on our premises.
Main Data Source	YouTube
Data Ownership	DeepMind
Country of Origin	Not defined
Restrictions on the use	Restrictions as defined in dataset licence
Access	CERTH (is publicly available so practically anyone)
Retention Period	For the duration of the project
Licence	The kinetics dataset is licensed by Google Inc. under a Creative Commons Attribution 4.0 International License.
WP and task	Task T5.2 of WP5

UCBM will re-use their own previously generated datasets, which will be fully pseudonymized (see table below) in order to provide sufficient measures for safeguarding the rights and freedoms of data subjects. Further technical and organizational measures, such as access restriction, and data minimization will be accordingly implemented.

Table 5: Processing of Existing Data: UMCU

	Please provide your answers in this column:
Dataset(s) name	<i>Utrecht Patient Oriented Database</i>
Dataset(s) description	<i>Routine care database consisting of all patients that ever visited the UMC Utrecht</i>
Personal Data	<i>Yes, although fully pseudonymized, these data are still considered personal data</i>
Purpose	<i>Research</i>
Data format	<i>Sasbdat files</i>
Data Storage	<i>According to the UMC Utrecht data management policy: within UPOD structures protected by authorization and outside UPOD structures in protected research folder structures protected by authorization</i>
Main Data Source	<i>The electronic health record system</i>
Data Ownership	<i>(Editor's note: To be clarified.)</i>
Country of Origin	<i>The Netherlands</i>
Restrictions on the use	<i>Yes, it cannot leave the hospital and users need to comply with Dutch data management and research guidelines before use</i>
Access	<i>Only UMC Utrecht</i>
Retention Period	<i>The full database is maintained indefinitely, the research subsets are kept for 15 years according to Dutch research guidelines</i>
Licence	<i>N/A</i>
WP and task	<i>For WP7 UC1/2/4</i>
Additional Comments	<i>It is our own dataset so we have easy access.</i>

5 Data Storage Management & Retention Policy

As indicated in Section 3 regarding General Security Instructions, datasets that contain personal or confidential information need to be securely stored, and the data controller needs to ensure that the latest security updates are in place. Personal data obtained by the project's partners will be securely stored on local data servers. Additionally, best practices of data storage and handling (see Section 2, 3, and 4) are communicated to all project partners and team members.

At the beginning of the project (March 2021) a dedicated repository for project collaborative work was set up.

On ODIN's public website (<https://www.odin-smarthospitals.eu>) the following data and information will be publicly available:

- General information about the project, its mission, and objectives;
- The participating consortium;
- Project public deliverables;
- Publications.

Project datasets (presentations, reports, scientific publications etc.), which are not intended for public dissemination will be shared only within the consortium on its private repository (CBMLBox). The following deliverables are confidential:

- D1.1: Quality Management Plan;
- D1.5, D1.6, D1.7, D1.8: Annual Report v1, 2, 3, 4;
- D2.2: Hospital requirements report;
- D2.3: ODIN platform catalogue;
- D2.4: Acceptance, Trust and Change Management;
- D3.4, D3.5, D3.6: Privacy, Security and Trust report v1, 2, 3;
- D3.7, D3.8, D3.9: Technical Support Plan and Operations v1, 2, 3;
- All WP5 deliverables;
- D6.2, D6.3: Data results interpretation and data integration services v1, 2;
- D6.6, D6.7: Development of the High-Level AI-based models of planning, scheduling, and workflow modelling v1, 2;
- D7.1: Pilot Studies Use Case Definition and Key Performance;
- D7.8: New use case demonstrations conclusion (I to IX);
- D7.9: Pilot Studies Evaluation Results and sustainability;
- D8.3: Certification scheme strategy and sustainability plan;
- D8.4: Data ethics in public procurement for hospitals v1;
- All WP 9 deliverables;
- D10.3: Supply Open Innovation;
- D10.4-6: Open Calls Report v1, 2, 3;
- All WP11 deliverables.

Of the datasets intended to be openly accessible, particularly the datasets containing personal information (e.g., interviews, pilots, focus groups) require anonymisation prior to release.

Project data will also be 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 will be maintained 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, the data from the ODIN platform will be anonymized and uploaded on in an open source. Dedicated discussions will be held around how this process will take place.

The figure below offers a simplified scheme of the data processing, storage, and retention.

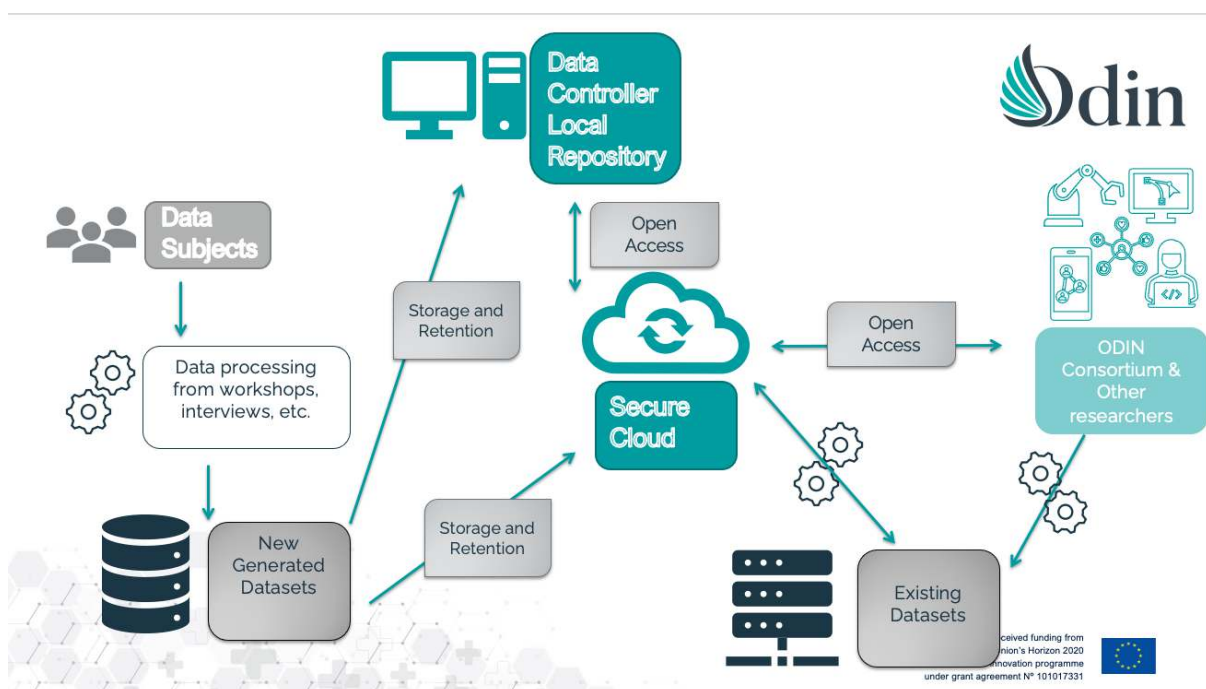


Figure 6: Storage and Flow of Data

All project data, except for the public website, is 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.

Beyond the provisions outlined, the table below presents the data storage management and retention policy on a per-partner basis.

Table 6: Data Storage Management & Retention

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 will be 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 will store 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 will store 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 will be 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 lifetime and beyond, at least 5 years after the end of the project.</p>
CERTH	<p>Data will be 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 will be processed and kept during the project's lifetime.</p>
FORTH	<p>The data received from pilots will be 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.</p> <p>Data will be kept exactly for the project period.</p>
University of Warwick (UoW)	<p>UoW Team is collecting and they will be stored on the ODIN Project shared storage.</p> <p>No data will be stored locally.</p>
SSSA	<p>Data will be centrally stored (if needed) 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 will not be stored by SSSA, but will be transmitted to the ODIN's ICT platform/infrastructure. Temporary dataset, used for local analysis, will be frequently replaced with the new generated data flow.</p>
THL	<p>The data will be stored on a server or a laptop on-premise (TBDL) until the end of the project.</p>
Philips Electronics Netherland BV (PEN)	<p>The data would be stored at the pilot sites. Only a limited amount of data (if allowed and needed) will be shared to develop base models.</p>

	PEN will access data locally at pilot sites and nothing will be transferred to PEN.
UPM	T2.4, T7.1, T10.3 will store the data using the cloud repository of the project (NextCloud). T3.3, T4.6 and WP5, data will be stored at each pilot site of in a pilot cloud provider. Data will be kept for the time of the project.
INETUM	No information about data storage and retention period could be provided at this stage.
UCBM	The data will be available to the UCBM team for the development and clinical validation of the ODIN platform. They will be strictly kept in closed archives and not connected to the network at UCBM. The data will be 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).
UMCU	UMC Utrecht will store the study data on its secure servers protected by authorization. Data will be kept, according to Dutch law, for the period of 15 years.
Charite (CUB)	The partner CHARITE will store the data on servers inside the hospital and inside the firewall protection of the hospital. 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.
AMIS	No information provided.
MUL	We store our data in a dedicated Research Folder Structure for which authorization is secured using personal logins. We only store pseudonymised data there. The key is stored at the separate drive. We will not transfer sensitive data outside the hospital. The MUL IT centre will be responsible for security of data in the data centre. The data will be available at least 10 years.
UDGA	Datasets will be stored in the ODIN's repository (CMBLBox) and kept for the duration of the project.
MEDICT MEDEA	MEDEA - Data will be only collected by reference MEDEA personnel and will be stored in the internal server of the company for the lifetime of the project.

6 Technical and Organizational Measures (TOMs) for Safeguarding the Rights and Freedoms of the Data Subjects

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 appropriate⁷:

- 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 are 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. The following sections present an initial set of recommendations for partners to consider alongside those security practices implemented by their organizations. All partners are 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 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines;
- ISO/IEC 27001 information security management;
- 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 29101:2018 Information technology — Security techniques — Privacy architecture framework;

⁷ Art. 32 (1) GDPR.

- 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

Furthermore, all Partners acting as data Controllers should 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 BEAMER 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

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.

Table 7: Technical and Organizational Measures for Data Subjects' Rights

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	Secure access through role base permission. Data is stored with version management and data loss protection.

M&S	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. 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).
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
CERTH	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.
FORTH	FORTH and the technology that is used is GDPR compliant for all data used. The private cloud facilities are ensuring data security and privacy.
University of Warwick (UoW)	UOW is not storing data on their premises but on the Cloud Services provided by FORTH.
SSSA	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.
THL	The laptop 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	No information about implemented TOMs could be provided at this stage.
UCBM	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,

	<p>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.
AMIS	No information provided.
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.
UDGA	Access to the data processed for UDGA's activity is secured with password, 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.

7 Further Processing of Previously Collected Data

Recital 50 GDPR provides that “*the processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected*”. The purposes of processing must be specified prior to, and in any event, not later than, the time when the collection of personal data occurs.⁸ As outlined in section 9.2.3 of the current Data Management Plan, in order to conduct a “compatibility assessment”, the following aspects should be considered⁹:

- The **link** between the original purpose and the new/upcoming purpose;
- The **context** in which the data was collected (i.e., What is the relationship between your company/organisation and the individual?);
- The **type and nature** of the data (i.e., Is the data sensitive?);
- The possible **consequences** of the intended further processing (i.e., How will the further processing impact the individual?);
- The existence of appropriate **safeguards** (i.e., encryption or pseudonymisation).

The compatibility assessment is, however, not necessary if the data should be used for archiving purposes in the public interest, statistical or scientific research purposes.

The table below outlines if further data processing is being conducted within ODIN.

Table 8: Further Data Processing

Partner	Further Data Processing
Robotnik	No further data processing.
SERMAS	No further data processing.
MYSOPHERA	No further data processing.
M&S	No further data processing.

⁸ ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 03/2013 on purpose limitation. Available here: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

⁹ https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/purpose-data-processing/can-we-use-data-another-purpose_en.

MEDTRONIC	No further data processing.
CERTH	No further data processing.
FORTH	Further processing for scientific reasons.
University of Warwick (UoW)	No further data processing.
SSSA	No further data processing.
THL	No further data processing.
Philips Electronics Netherland BV (PEN)	No further data processing.
UPM	No further data processing.
INETUM	No information regarding further data processing could be provided at this stage.
UCBM	No further data processing.
UMCU	No further data processing.
Charite (CUB)	The patient data will be processed further for patient diagnostic purposes. The result of the diagnosis will be part of the electronic patient record as used in clinical work in the hospital.
AMIS	No information provided.
MUL	No further data processing.
UDGA	No further data processing.
MEDICT MEDEA	MEDEA – No further data processing

8 Main Principles and Concepts of Data Management

All partners are invited to consider the following information throughout their project-related activities. Relevant definitions and further information about the fundamental concepts can be found in Annex A of this deliverable.

8.1 Guidelines for GDPR Compliant Deployment of AI, IoT and Robotics in Pilots

The management and exchange of information within ODIN pilots, the hospitals, has been recognized to be deeply heterogeneous, due to the implementation of various functionalities, different data representations, user interfaces, terminologies, etc. The interoperability, which enables the heterogeneous structures to interfere, is achieved through health data exchange standards and protocols, common middlewares, and specific standards for the management of domains and servers.¹⁰ With this respect, the ODIN project aims at developing and/or integrating technologies to reconstruct the surrounding environment and retrieve useful information to monitor the quality of the environment, model the human behavior, enhance human-robot collaboration and increase cognition capabilities from ODIN platform technologies.¹¹ As showcased in the figure below, there will be 3 types of communication architectures: Robotics, AI and IoT.

¹⁰ ODIN_D2.2_Hospital_Requirements_Report_v.1.1_revTHL: section 2.2.4.

¹¹ ODIN_D5.1 - Context_awareness_human_modelling_v05; Section 4.1.

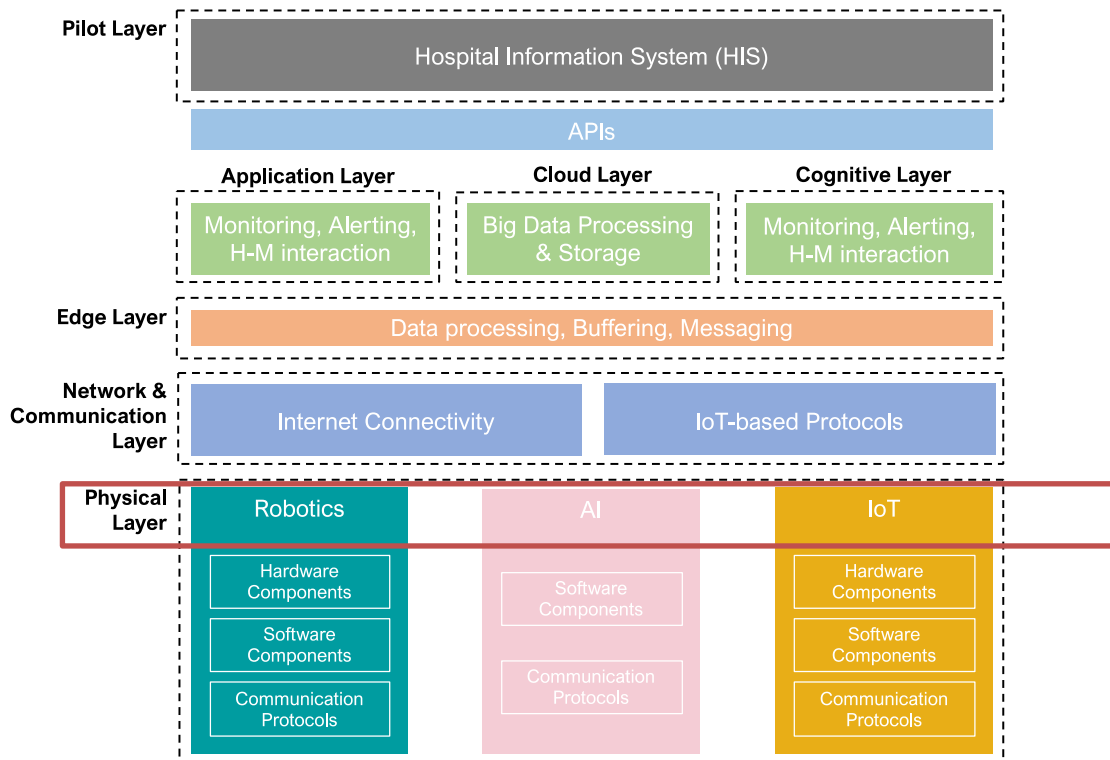


Figure 7: ODIN Platform blueprint (Source: D2.2)

The architecture of all of the physical layer is multi-layer and, partially, very complex. On top, the architectures are not strictly distinct and can merge, creating for example an Internet of Robotics Things (IoRT) infrastructure, combining IoT and Cloud Robotics technology. Its accelerated development is enabled by Artificial Intelligence of Things (AIoT) to improve humans-machines interactions and enhance data management and analytics. Such human-robot collaborative environments need to ensure the safety of human beings, but also to guarantee their rights and freedoms. This could prove particularly challenging considering the multitude of sensors deployed in a pilot environment, collecting data from various sources, and exploiting it into the complex technological architecture of the project.

Such Large-Scale-Pilots (LSPs) have been long examined, tested and validated in diverse application domains by the research community. The following guidelines have been established as best practice to guide the consortium and the pilots in deploying different solutions. As ODIN aims at being compliant with the standards identified by the research community, the guidelines have been communicated with pilots, who are invited to comply with these principles¹²:

1. **Perform a preliminary data protection impact assessment** before collecting any data with new technologies. Ensure that you address and mitigate the identified risks.
2. **Minimize personal data collection**, by adapting the granularity of the data and processing the data at the edge. Consider data minimization and data protection by design as an

¹² The list of principles is taken by S. Ziegler and others, *Personal Data Protection for Internet of Things deployment: Lessons learned from the European Large-Scale Pilots of Internet of Things*, February 2020, pp. 30-31.

opportunity to save costs and to increase the scalability of the system to be deployed. This is a way to leverage the approach to build trust within the organization and towards the different stakeholders.

3. **Minimize personal data transfers** by prioritizing onsite pre-processing, edge computing and local storage. Decentralized data processing can contribute to enhance both data protection and scalability of the system.
4. **Minimize data storage and retention time**, which will also save infrastructure costs.
5. **Maximize the use of anonymization¹³ and pseudonymization techniques.**
6. **Ensure that data processing is lawful** and that the amount of personal data collected is proportionate to the legitimate purpose.
7. **Identify the data controllers and data processors** involved in the deployment as well as their respective Data Protection Officers. Establish adequate coordination mechanisms and regular communication among the DPOs and clarify their respective responsibilities.
8. **Designate a Data Protection Officer.**
9. **Ensure that the Data Protection Officer can be easily contacted.**
10. **Formalize your data protection policy** in a clear document and communicate it to all involved stakeholders.
11. **Organize regular communication and training activities on data protection and data management** for all those involved in the processing of personal data.
12. **Write a Data Management Plan** that specifies what data are collected for what purpose, who can access them, how long they are stored, etc.
13. **Secure your IoT network** physically and logically.
14. **Each IoT mote should be protected by a unique and distinct password** and never use the default password provided by the manufacturer.
15. **Define and implement a clear access rights policy** that minimizes access to the processed personal data. The personal data should be accessible only to those who have a legitimate need to access them.
16. **Adopt and enforce a strict policy and procedures for updating the firmware** of the IoT motes whenever vulnerabilities are identified.
17. **Establish procedures to comply with the data subjects' rights.**
18. **Exchange and collaborate with other DPOs.**
19. **Use external certification of compliance** with data protection regulation as a mean to reduce liability and to increase trust and transparency with end-users.
20. **Identify any cross-border data transfer** of personal data and check if they are lawful.

¹³ ODIN partners are welcome to use open-source H2020 funded solutions, such as Amnesia (<https://amnesia.openaire.eu/>), a key result of the OpenAIRE project.

21. **Clearly inform and communicate the purpose for data collection**, the categories of data processed, who has access and how long the data will be stored online through online applications (i.e., [privacyapp.info](#)).
22. **Take advantage of online commitment tools** to ensure that all partners located in other jurisdictions are committed to respect the same level of data protection (i.e., [privacypact.com](#)).

Importantly, the recent developments around the COVID-19 crisis have brought new guidelines into play. On April 21st, 2020, the European Data Protection Board (EDPB) approved the Guidelines 3/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID 19 outbreak.¹⁴

8.2 Data Protection Principles

Data management is an ongoing process and the current data management plan, as outlined above, is meant to be a live document. Although Data Management Questionnaires were handed out and partially collected from the consortium members, due to the nature of the research and the early stage of the project, it cannot yet be stated with complete certainty what the exact specifications and modalities of the data, which are going to be gathered, processed and stored throughout the project, are going to be. Therefore, the current DMP adopts the following basic guidelines, as per EDPB's guidelines¹⁵ and best practices, in order to ensure that all researchers will keep up the principles of lawful and ethical data management. The following principles are binding to all data controllers in the framework of the ODIN project.

8.2.1 Lawfulness and Fairness

In order for the processing of personal data to be lawful, the controller must identify a valid legal basis for it and should abide by the relevant local laws and regulations. Valid legal basis are presented in GDPR Art. 6(1). Furthermore, the data should not be processed in a way that is unjustifiably detrimental, unlawfully discriminatory, unexpected or misleading to the data subject (principle of fairness). The researcher in the ODIN project, who are involved in data collection and processing activities, will follow procedures around determining not only how to process the data according to the reasonable expectations of the data subject, but also how they should obtain them and whether the data needs to be obtained at all. A Quality Management Plan has been established by the consortium already in Month 3, which describes QA procedures and reports relevant checkpoints, guidance and responsibilities for risk management related to each project activity. Furthermore, each of the pilot owner should have methodology in place to assess how the data processing affects the interests of the people concerned, both as a group and

¹⁴ https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf.

¹⁵ Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0. Available here: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf .; Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak.

individually. If the information is obtained and used fairly in relation to most of the people but unfairly in relation to one individual, there will still be a breach of this principle.¹⁶

8.2.2 Transparency and Information to Data Subjects

The principle of transparency constitutes that personal data shall be processed fairly and in a transparent manner in relation to the data subject. These provisions are strongly connected with the information obligations as in GDPR Art. 13 and Art. 14. Particularly in regard to health data processing for scientific purposes, each individual (participant) should be explicitly informed that their health data is going to be processed for the said purpose. This information leaflet should be aligned with the requirements in Art. 13, 14 of the GDPR, i.e., there should be information about the data controller(s), their contact details, purpose of processing, recipients, etc.

As it is not uncommon to occur that processed health data have not been obtained directly from the data subject, i.e., processing data from patient records or data from patients in other countries, the provisions of Art. 14(3)(a) stipulates that the controller shall provide the required information “*within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed*”.

GDPR Art. 14(4) notes that if “*the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose*”. This means that in the case of further processing of the health data for scientific purposes, the data controller should deliver the information to the data subject within a reasonable period of time before the implementation of the new research project to allow the data subject to become aware of the research project and enables the possibility to exercise its rights effectively beforehand.

The data controller is exempt from the information obligation, if it “*proves impossible or would involve a disproportionate effort*” (Art. 14(5)(b)) or if “*obtaining or disclosure is expressly laid down by Union or Member*” (Art. 14(5)(c)).

8.2.3 Purpose Limitation and Presumption of Compatibility

According to the principle of purpose limitation (GDPR Art. 5(1)(b)), the data controller must collect data for specified, explicit, and legitimate purposes, and not further process the data in a manner that is incompatible with the purposes for which they were collected. When it comes to data processed for research purposes, the compatibility presumption states that “*further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes*”. Art. 89(1) GDPR stipulates that the data processing for

¹⁶<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/#fairness>.

the aforementioned purposes “*shall be subject to appropriate safeguards (...) for the rights and freedoms of the data subject*”. The safeguards require technical and organisational measures to be in place to ensure data minimization.

The principle of purpose limitation is adhered to, when the purpose for the data processing has been clearly identified, documented and communicated in a plain understandable manner to the individuals (research participants).

8.2.4 Data Minimization and Storage Limitation

The data should be adequate, relevant and limited to what is necessary for the processing purpose (Art. 5(1) (c)). As a result, the data controller needs to predetermine whether they even need to process personal data for their relevant purposes, as well as which features, and parameters of processing systems and their supporting functions are permissible. Especially for scientific research, data minimisation can be achieved through specifying the research questions and assessing the type and amount of data necessary to properly answer these research questions. It should be verified whether the relevant purposes can be achieved by processing less personal data or having less detailed or aggregated personal data or without having to process personal data at all.¹⁷ Wherever it is possible to perform the research with anonymized datasets, then the data must be anonymized.¹⁸ Furthermore, the controller should periodically consider whether processed personal data is still adequate, relevant and necessary, or if the data shall be deleted or anonymized. This approach is closely linked with storage limitation.

In addition, proportionate storage periods for data retention shall be set. Article 5 (1) (e) GDPR stipulates that “*personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving (...) scientific purposes (...) in accordance with Article 89 (1) subject to implementation of the appropriate technical and organisational measures (...) to safeguard the rights and freedoms of the data subject*”. In order to define storage periods, criteria such as the length and the purpose of the research should be taken into account. National provisions may additionally stipulate rules regarding the storage period. Therefore, ODIN’s consortium involved data processing activities provides a signed declaration of compliance with GDPR provision and National Regulations.

8.2.5 Accuracy

Article 5(d) GDPR provides that personal data should be “*accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')*”. From this principle follows an obligation to the controllers to ensure that personal data are accurate and, keep them up to date, and erasing or rectifying inaccurate data without delay. In particular, controllers should accurately record information they collect or receive and the source of that information.

¹⁷ GDPR Recital 39: “*Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means*”.

¹⁸ 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.

8.2.6 Integrity and Confidentiality

This principle requires protection that ensures appropriate security against unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organisational measures.¹⁹ Security of personal data requires appropriate measures, designed to prevent and manage data breach incidents, as well as measures to guarantee the proper execution of data processing tasks, compliance with other principles, and facilitating the effective exercise of individuals' rights. Sensitive data, such as health data, merit higher protection as their processing is more likely to cause negative impacts for data subjects. This holds especially true for further processing of health data for scientific purposes by an increased number and types of processing entities.²⁰ Therefore, the principle of integrity and confidentiality must not only be read in conjunction with the requirements of Art. 32 (1) GDPR and Art. 89(1) GDPR, but also fully complied. This means that the required technical and organizational security measures should *at least* consist of pseudonymization, encryption, non-disclosure agreements and strict access role distribution, restrictions and logs. Lastly, pursuant to Art. 35(1) GDPR, Data Protection Impact Assessment (DPIA) should be performed to data processing "*likely to result in a high risk to the rights and freedoms of natural persons*". Additionally, as per EDPB's emphasis, data protection officers (DPOs) should be consulted on processing of health data for the purpose of scientific research.

8.2.7 Accountability

The data controller shall be responsible for compliance with all the aforementioned principles, and able to demonstrate its compliance, the measures taken to protect the subjects' data rights as well as their appropriateness and effectiveness. For example, the data controller should be able to demonstrate the reason that a certain implemented measure is appropriate to ensure the principle of storage limitation in an effective manner. In order to process personal data responsibly, the data controller needs to have the knowledge and ability to implement data protection measures, therefore they must understand their obligations under the GDPR, and complementary national obligations, and how to comply with them.

The ODIN project demonstrates 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, each partner remains responsible for *its actions, for compliance with the GDPR and safeguarding EU fundamental rights*.

¹⁹ Art. 5(1)(f) GDPR.

²⁰ 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, p.9-10.

8.3 Ethical Principles

ODIN as a project, its consortium and the actions related to the project will comply with ethical and legal principles, standards and regulation. 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.

Potential ethical issues will mainly concern data protection. Within ODIN, any research involving human subjects, data processing, and sensitive data processing will conform to applicable legislation and regulations both on European level, as well as to complementary obligations of the countries where the activities will be carried out.

The Good Clinical Practice guidelines²¹ are in agreement with the Declaration of Helsinki. Work done by partners and its beneficiaries will also conform to 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.

In order to protect the privacy rights of participants, a number of best practice principles will be followed. There are two basic components to the ethical standards: (i) **informed consent** and (ii) **independent ethical oversight**.²² Leveraging on *International Ethical Guidelines for Health-related Research Involving Humans*²³, 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:

²¹ 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>.

²² 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.

²³ 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>.

8.3.1 Informed Consent

The participation of individuals capable of giving informed consent is voluntary. No data will be collected without the explicit prior informed consent of participants. Researchers are expected to disclose information about a study's purpose, risks, procedures as well as measures in the case of harms resulting from participation. Participants should be able to fully understand and agree to the procedures/research being undertaken by giving their explicit consent (through consent forms, Appendix C). The project's consortium acknowledges that the process of obtaining informed consent begins when initial contact is made with a prospective subject and continues throughout the entire course of the study. By informing the prospective subjects, by repetition and explanation, by answering their questions as they arise, and by ensuring that each individual understands each procedure, investigators elicit their informed consent and in so doing manifest respect for their dignity and autonomy.

8.3.2 Approval by Research Ethics Committees

Research protocols must be submitted for consideration, comment, guidance and approval to the concerned research ethics committee before the study begins. Independent ethics committees or Institutional Review Boards should review and consider whether the research is ethical, lawful and provides appropriate safeguards. Alignment with national approaches will be sought through collaboration and exchange of good practices with local ethics committees, as well as via larger networks, such as the European Network of Research Ethics Committees.²⁴ A data minimisation approach is suggested at all levels of the project and will be supervised by each Pilot Demonstration responsible (one per each country involved and managed by the central Ethical Board (T1.4) of the project). Alignment with national approaches will be sought through collaboration and exchange of good practices with local ethics committees, as well as via larger networks, such as the European Network of Research Ethics Committees.²⁵

8.3.3 Scientific and Social Value

The ethical justification for undertaking health-related research involving humans is its scientific and social contribution and value for gaining knowledge for means on protecting and promoting peoples' health.²⁶ Researchers, research ethics committees, and health authorities must ensure that the studies are scientifically sound, build on an adequate prior knowledge base, and are likely to generate valuable information. All research activities conducted by the ODIN project have scientific validity and add social and scientific value. The activities use accepted scientific methods and follow scientific principles.

8.3.4 Purpose Limitation

No data collected will be sold or used for any purposes other than the ODIN project.

²⁴ <http://www.eurecnet.org/index.html>.

²⁵ <http://www.eurecnet.org/index.html>.

²⁶ INTERNATIONAL ETHICAL GUIDELINES FOR HEALTH-RELATED RESEARCH INVOLVING HUMANS, Guideline 1, p. 1. Available here: <https://cioms.ch/wp-content/uploads/2017/01/WEB-CIOMS-EthicalGuidelines.pdf>.

8.3.5 Data Minimization

Any shadow (ancillary) personal data obtained during the course of the pilots will be immediately cancelled. Only relevant personal data will be collected and processed, and it will be anonymized as soon as viable.

8.3.6 Use of Data obtained from the Online Environment and Digital Tools in Health-related Research

When researched utilize online and digital tools to obtain data for health-related research, privacy-protective measures should be set in place to protect the individuals from the possibility of their personal information being directly revealed or otherwise inferred when datasets are published, shared, combined or linked. Generally, information posted online voluntarily is public and hence not subject to the usual consent and protection requirements as other research data. However, it is important to acknowledge that in most cases users rarely completely understand and anticipate how their data are stored and used. Even though information may be collected from a public source, researchers should acknowledge that data subjects may be unwilling to have their data obtained for studies and may feel violated when their information is used in a context they did not anticipate. The existence of data and information online does not relieve the researcher from the obligation to respect privacy and mitigate risks that could result from combining data from multiple sources and their subsequent use and publication. The risk of unauthorized or inadvertent disclosure, in combination with technological capabilities are particular risk factors for re-identification of data.

8.3.7 Reimbursement and Compensation for Research Participants

If and when provided, compensation for participation will correspond to a simple reimbursement. Reimbursed can be provided for costs directly incurred during the research, such as travel costs, and compensated reasonably for their inconvenience and time spent. It can be of non-monetary nature, such as free health services unrelated to the research, medical insurance, educational materials, or other benefits. Compensation should not lead to inducement of potential participants to consent to participate in the research against their better judgment (“undue inducement”). Any compensation is therefore to be approved by local research ethics committee.

8.3.8 Recruitment of Affiliated Participants

If employees of partner organizations, are to be recruited, specific measures will be in place in order to protect them from a breach of privacy/confidentiality and any potential discrimination. In particular their names will not be made public, and their participation will not be communicated to their managers.

8.3.9 Privacy and Confidentiality

Every precaution must be taken to protect the privacy of research subjects and the confidentiality of their personal information. Any data or information that is disclosed or otherwise made available between ODIN Parties during the implementation of the projector for any exploitation activities (“Shared Information”), shall not include personal data as defined by the GDPR (Art. 4(1)). Accordingly, each Party agrees that it will take all necessary steps to ensure that all Personal Data is removed from the Shared Information, made illegible, otherwise made inaccessible (i.e. re-identifiable) to the other Parties prior to providing the Shared Information to such other Parties.

8.3.10 Data Sharing

Each Party who provides or otherwise makes available to any other Party Shared Information will represent that: (i) it has **the authority** to disclose the Shared Information, which it provides to the

Parties; (ii) where legally required and relevant, it has obtained appropriate **informed consents** from all the individuals involved, or from any other applicable institution, all in compliance with applicable regulations; and (iii) there is **no restriction in place** that would prevent any such other Party from using the Shared Information for the purpose of this Action and the exploitation thereof.

8.3.11 Vulnerable Persons and Groups

If vulnerable persons or groups are to be recruited for the research purposes, researchers and local research ethics committees must ensure that specific protections are in place to safeguard the rights and welfare of these individuals and groups.

According to the Declaration of Helsinki, vulnerable groups and individuals are such that “*may have an increased likelihood of being wronged or of incurring additional harm.*” Vulnerability involves judgments about both the probability and degree of physical, psychological, or social harm, as well as a greater susceptibility to deception or having confidentiality breached. Vulnerability is not considered only at the stage of giving informed consent, but also in the subsequent stages of the research, as vulnerable individuals are considered also those, incapable of protecting their own interests due to relative or absolute impairments in decisional capacity, education, resources, strength, or other attributes.²⁷

Special protections for these groups can include allowing no more than minimal risks for procedures; and supplementing the participant’s informed consent by the permission of family members, legal guardians, or other legal representatives. Safeguards can be designed to promote voluntary decision-making, limit the potential for confidentiality breaches, and otherwise work to protect the interests of those at increased risk of harm. Research ethics committees need to be sensitive to not overly excluding people and allow them to participate by requiring that special protections be put in place.

8.4 Data Subject Rights

Recital 59 GDPR provides that 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. Further, 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.

All participants will be 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 (see Appendix C). Withdrawal can be also expressed orally.

²⁷ CIOMS, International Ethical Guidelines, Guideline 15. Available here: <https://cioms.ch/wp-content/uploads/2017/01/WEB-CIOMS-EthicalGuidelines.pdf>, p.58.

Following, these are the data subjects' rights, as per the provisions of the GDPR, which the ODIN's consortium commits to respect and guarantee.

8.4.1 Right to Access

The right of access is the right for any data subject to obtain from the controller of a processing operation the confirmation that data related to him/her are being processed, the purpose(s) for which they are processed, as well as the logic involved in any automated decision process concerning him or her.

The right of access also allows the data subject to receive communication in an intelligible form of the data undergoing processing and information regarding the processing.

8.4.2 Right to Information

Everyone has the right to know that their personal data are processed and for which purpose. The right to be informed is essential because it determines the exercise of other rights. The right of information refers to the information which shall be provided to a data subject whether or not the data have been obtained from the data subject.

Under Art. 13 GDPR, where data are collected from an individual, they should be informed as to who is collecting their data, how to contact the controller and its data protection officer, for which purpose and on which legal grounds the data is processed, who will also receive the data, for how long it will be kept and how this period is determined, and whether automated decision-making is involved. This also includes receiving information on the rights available to them as well as the right to lodge a complaint with a supervisory authority.

Where data have not been obtained directly from the data subjects, patients and/ or research participants, in principle, they still have right to be fully informed that a data concerning them is being processed. Art. 14 GDPR sets out the data subject's right to information – what information should be provided and how. The information provided should also include the categories of personal data which are processed, the source from which the data comes and whether it came from publicly accessible sources. However, under Art. 14(5)(b) GDPR, the obligation to provide information does not apply 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*".

Additionally, the right of information for the person concerned is limited in some cases, such as for public safety considerations for the prevention, investigation, identification and prosecution of criminal offences, including the fight against money laundering.

8.4.3 Right to Rectification

The right of rectification is the right to obtain from the controller the rectification without delay of inaccurate or incomplete personal data. The right of rectification is an essential complement to the right of access and is important to maintain a high level of data quality.

To exercise the right of rectification, the data subject usually has to write to the controller of the processing operation.

8.4.4 Right to Object

Art. 21 GDPR grants individuals the right to object to the processing of their personal data at any time. This allows individuals to stop or prevent processing of their personal data. An objection may be in relation to all of the personal data of an individual or only to certain information. It may also only relate to a particular purpose for which data are being processed.

8.4.5 Right to Erasure

Art. 17 (1) GDPR provides data subjects with the right to have their personal data erased. This links with personal data being removed from datasets where individuals withdraw their consent. Partners will endeavour to comply with requests of erasure but note that data processors are exempt from doing so where erasure would endanger the fulfilment of research activities (which includes safeguards to protect personal data), Art. 17(3)(d) GDPR.

8.4.6 Right to Restriction of Processing

Art. 18 GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way in which an organisation uses their data. This is an alternative to requesting the erasure of their data.

8.4.7 Right to Data Portability

Art. 20 (1) provides data subjects with a right to request personal data which is held about them in a “*structured, commonly used and machine-readable format*” which can be used to transfer data from one data controller to another. Data subjects can only request such data where the data is processed on the basis of consent, or a contract, and the processing is done by automated means.

8.4.8 Rights related to Automated Individual Decision-making and Profiling

Art. 22(1) GDPR provides data subjects with the right not to be subject to decisions based solely on automated decision-making or profiling which creates legal or similar effects for such persons. However, such processing can be lawful, where this necessary for entering into, or performance of, a contract between the data subject and a data controller (Art. 22(2)(a) GDPR); if authorised by Union or Member State law and provided with suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests (Art. 22(2)(b) GDPR); and if data subject consents to this process (Art. 22(2)(c) GDPR).

8.5 FAIR Guidelines for Data Management

In its FAIR Data Management Horizon 2020 Guidelines²⁸, 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).

8.5.1 Findability of Data

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:

²⁸ EC H2020 Programme Guidelines on FAIR Data Management in Horizon 2020, p.3. Available here: https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf.

- 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.

8.5.2 Accessibility of Data

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. In addition, the project is largely based on open data principles, as defined by the Open Knowledge Foundation²⁹, which define a set of policies and technical specifications for being compliant.

Project datasets (presentations, reports, scientific publications etc.), intended for public level of dissemination, will be openly accessible through:

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

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

With this respect, the data management in ODIN will 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).

(...)

²⁹ <https://okfn.org/opendata/>.

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.

8.5.3 Interoperability of Data

As data usually need 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.

8.5.4 Reuse of Data

The ultimate goal of FAIR is to optimise the reuse of data.³⁰ This can be achieved, when metadata and data are well-described so that they can be replicated and/or combined in different settings.

³⁰ <https://www.go-fair.org/fair-principles/>.

9 IPR Management

Standard contracts will regulate the management of IPR (Intellectual Property Rights) in ODIN and protect the intellectual property of third parties and beneficiaries involved. The Consortium Agreement contains provisions regarding access rights.

Results from experiments are owned by the beneficiaries or third parties that generate them. Specifically, the product resulting from an experiment will be owned by third parties. Detailed IPR terms and conditions will be stated in the Consortium Agreement.

9.1 Intellectual Property Rights

IPR is a generic term that encompasses several different issues that are covered by different laws and practices. Generally, all issues related to copyright, patents, trademarks, trade secrets and sui generis database rights are collectively indicated as IPR.

IPR management is of fundamental importance in ODIN, because the main software artefacts that the project will release, will be distributed with the intent that Parties, either internal or external to ODIN, can use it freely. In order to grant Parties these rights, it should be carefully managed about the IPR distribution terms.

In the following paragraphs, we will discuss three basic issues about the knowledge the project are producing:

- Access rights: who will own the basic rights?
- Licences: under which conditions is the project going to exchange it?
- Use and dissemination: how will the project exploit it?

9.1.1 Copyright

Copyright is a corpus of laws that are harmonised in most nations in the world thanks to the Berne copyright convention. Copyright laws establish the rights that the authors have over their work. Copyright applies to most original and non-trivial works, be it writings, painting, music, most works of art and even software, both source and machine-readable code.

Copyright concerns the rights of copying, displaying, performing, printing, publishing, extending, modifying, translating a work. Application of copyright to software involves the rights to copy, modify or distribute the program. It does not involve the right to independently write a program performing the same actions as an original one. Generally speaking, the programmer who writes the program owns the rights. Where there is more than one programmer, the Directive (Directive 2009/24/EC) provides for co-ownership.

9.1.2 Patents

A patent is a set of exclusive rights granted by a national or international body to an inventor for a limited period of time in exchange for a public disclosure of an invention.

The procedure for granting patents, the requirements placed on the patentee, and the extent of the exclusive rights vary widely between countries according to national laws and international agreements. A patent application must include one or more *claims* defining the invention which must be new, non-obvious, and useful or industrially applicable. The exclusive right granted to a

patentee in most countries is the right to prevent others from making, using, selling, or distributing the patented invention without permission.

Software patents are an important issue, because they can pose a real danger to Free/Libre and Open Source Software (FLOSS) software. When a software method or algorithm is covered by a patent, the patent office has recognised the inventor's claim that the software method is original (never invented before), and non-trivial (a knowledgeable person in the field would not be able to reproduce it from state of the art). The inventors have a 20-years monopoly on the exploitation of the software method, and no one can lawfully use it without their permission.

In Europe the law disallows patents on software per se. The legal status of the European software patents is unclear, though. Application of these recommendations depending a big extent on national laws, which are not harmonized.

FLOSS communities are particularly sensible to this risk, and in fact they avoid as much as possible to use software on which patent claims are known or suspected to exist. Modern FLOSS software licences often contain provisions against the most blatant abuses of software patents. The Apache licence, for example, contains some clauses that protect the software against the use of submarine patents: if a contributor's software is covered by a patent, and that contributor makes legal attacks against users of the software, that contributor loses all rights to using the software. The Mozilla, Eclipse and GPL licences all have some sort of protection against software patents.

9.1.3 Trademarks

A trademark is a distinctive sign, usually a word or a logo. Its usefulness is to give a brand to something and avoid that someone else takes credit for the product using the trademark or distributes a different version of it with the same name.

9.1.4 Trade Secrets

The most generic way of protecting IPR is to just not let slip the knowledge outside of the boundaries of your organization. For its very nature, this practice is utterly incompatible with FLOSS, which is based on openness. Keeping the development secret is a risky choice, because it can easily give the impression to outsiders that the openness of the developers is just a facade, rather than a real overall policy.

In ODIN, trade secrets would be kept to a minimum, and development should be organised around publicly available repositories as early as practically feasible.

9.2 IPR Management within ODIN

The management of IPR component in ODIN will be handled per the provisions of the DESCA 2020 Model Grant Agreement, as well as per the clauses defined within the ODIN Consortium Agreement.

9.2.1 Ownership of Background Knowledge

Ownership of background IP will not be affected by participation in this project, and it will remain the property of the corresponding participant during and after the project execution. The following principles apply to the use of background knowledge:

- 1) Access rights will be free of any administrative transfer costs.
- 2) Access rights are granted on a non-exclusive basis.
- 3) Background will be used only for the purposes for which access rights have been granted.
- 4) All requests for access rights will be made in writing.
- 5) Access rights to results and foreground needed for the performance of the own work of a party under the project will be granted on a royalty-free basis.

9.2.2 Open-Source Access

As part of its commitment to open science, ODIN promotes the development of an Open Access Software. Some of the project's innovations will be evaluated and made openly available for reuse and further development to ensure a level playing field in the market, targeting the production of new open-source software solutions. Hence, open data must be technologically neutral, licensed for reuse at low constraints and documented. Access rights may be granted for research purposes only, as this granting access rights would not include any rights to sublicense or to commercialize the information. The aim of the exploitation will be to ensure the optimal use of ODIN's outcomes and results after the project's completion, speed up the potential of their wider use within the ecosystem, and support in building and expanding the open-source community.

9.2.3 IPR Conflict Resolution

In order to handle IPR issues, which may occur during the project, the following procedures will be undertaken:

1. All project members themselves immediately notify the Project Management Board (PMB) as soon as they are aware of any issue that could be related to ODIN.
2. As soon as an issue of any kind is noticed, the coordinator will nominate one person to be responsible to solve the issue. This person may nominate a task force of persons within ODIN and, discretionally, outside the project, to help in the analysis of the problem and the finding an efficient solution in a timely manner. The nominated person will be responsible for notifying on the progress of the task force.

9.3 ODIN Software IPR Directory

The Software IPR Directory is the document where we store intellectual property information about software. From the exploitation and future business perspectives, it is considered of paramount importance that any piece of software used and produced in ODIN is registered in the Directory.

A respective entry should be created both background, and foreground work at the start or as soon as possible from the start date. The terms foreground knowledge and background knowledge are defined in Appendix A. Entries in the database contain critical information about copyright holders, patents pending, software licence to be used, distribution terms and willingness to contribute it to further possible initiatives that continues the exploitation of the ODIN assets. Consequently, the IPR directory contains important information from the partners. It is therefore critical that the data entered is reliable and non-refutable.

10 Conclusion and Future Plans

The current deliverable includes the best available information on data processes at the project level and at the pilot level in the current stage of development of the ODIN project. It is the result of a collaborative work with representatives of the different WPs and of the different pilot sites. It is to be understood as a living document that will be constantly updated during the next steps of the project and thanks to the contribution of the different participants to the project. Particular attention will be also devoted to the issues arising from data sharing in the context of multisite research. The data management plan of the different pilots will also be constantly monitored and updated. The updated versions of the deliverable will be made available according to what has been agreed in the DoA. Important implications from the work done can be already highlighted:

- Data (personal and non-personal) play an increasingly important role in the medical research domain and e-health;
- Data controllers are responsible for guaranteeing compliance with legal norms and ethical standards for the treatment of personal data and should therefore produce their own DMPs;
- The pilots, as data controllers, also have to guarantee the flow of data to the platform. Further work will be required to define and design the Data Sharing Agreements (DSA);
- Non-personal data have also to be taken into consideration especially as far as IPR and licensing are concerned;
- This document is understood by the Consortium as a living document; it will be constantly updated through the involvement of the pilots.

Appendix A Definitions and general recommendations

In order to facilitate the understanding of fundamental concepts for the researchers as well as people who do not have a legal background, core concepts of the European Data Protection Framework are introduced and defined in this section. For some of the provided concepts, general information regarding their practical application is also provided:

Data Controller

Under the GDPR Article 4(7): “controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided by Union or Member State law”. The actual processing may be delegated to another party, called the data processor (see 2.1.25). The controller is responsible for the lawfulness of the processing, for the protection of the data, and respecting the rights of the data subject. The controller is also the entity that receives requests from data subjects to exercise their rights.

Accountability

Principle intended to ensure that data controllers are more generally in control and in the position to ensure and demonstrate compliance with data protection principles in practice. Accountability requires that controllers put in place internal mechanisms and control systems that ensure compliance and provide evidence—such as audit reports—to demonstrate compliance with external stakeholders, including supervisory authorities.

Automated individual decision

An “automated individual decision” is a decision which significantly affects a person, and which is based solely on automated processing of personal data in order to evaluate this person. Such an evaluation may relate to different personal aspects, such as performance at work, creditworthiness, reliability, conduct, etc.

Article 22 of the GDPR lays down the right for individuals to object to decisions about them and solely based on automated means, unless certain conditions are fulfilled or appropriate safeguards are put in place.

Biometric data

According to article 4(14) of the GDPR “biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data”.

Confidentiality

Confidentiality in general refers to the duty not to share information with persons who are not qualified to receive that information. In a more specific sense, it refers to the confidentiality of communications provided for in Article 5 of the E-Privacy Directive 2009/136/EC.

Consent

In data protection terminology, consent refers to any freely given, specific and informed indication of the wishes of a data subject, by which he/she agrees to personal data relating to him/her being processed (see Article 4 sub 11 of Regulation (EU) 2016/679).

Consent is an important element in data protection legislation, as it is one of the conditions that can legitimise processing of personal data. If it is relied upon, the data subject must unambiguously have given his/her (written or verbal) consent to a specific processing operation, of which he /she shall have been properly informed. The obtained consent can only be used for the specific processing operation for which it was collected, and may in principle be withdrawn without retroactive effect.

Cookies

Short text files stored on a user's device by a web site. Cookies are normally used to provide a more personalised experience and to remember user profiles without the need of a specific login. Also, it can be placed by third parties (such as advertising networks) in end users' devices and may be used to track users when surfing across different websites associated to that third party.

Data concerning health

According to article 4(15) of the GDPR "data concerning health means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status".

Data minimization

The principle of "data minimization" means that a data controller should limit the collection of personal information to the data that is directly relevant and necessary to accomplish a specific purpose. They should also retain the data only for as long as is necessary to fulfil that purpose. In other words, data controllers should collect only the personal data they really needed, and should keep it only for as long as they need it.

The data minimisation principle is expressed in Article 5(1)(c) of the GDPR.

Data mining

Data mining is the process of analysing data from different perspectives and summarising it into useful information. Data mining software is one of a number of tools for interrogating data. It allows users to analyse data from many different dimensions or angles, categorise it, and summarise the relationships identified. Technically, data mining is the process of finding correlations or patterns among dozens of fields in large relational databases. It is commonly used in a wide range of

profiling practices, such as marketing, surveillance, fraud detection and scientific discovery. Obviously, for data mining to be effective it is necessary to analyse large amounts of previously collected data.

Data protection authority

A Data protection authority (DPA) is an independent body which is in charge of:

- monitoring the processing of personal data within its jurisdiction (country, region or international organization);
- providing advice to the competent bodies with regard to legislative and administrative measures relating to the processing of personal data;
- hearing complaints lodged by citizens with regard to the protection of their data protection rights.

According to Article 51 of the GDPR, each Member State shall establish in its territory at least one data protection authority, which shall be endowed with investigative powers (such as access to data, collection of information, etc.), corrective powers (power to order the erasure of data, to impose a fine or a ban on processing, etc.), and authorisation or advisory powers (issuance of opinions, power to accredit certification bodies, etc..).

National data protection authorities have been established in all European countries, as well as in many other countries worldwide.

Data Protection Impact Assessment (DPIA)

The data controller shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data when a type of processing is likely to result in a high risk to the rights and freedoms of natural persons.

This assessment must generally be performed prior to the processing and, in particular if using new technologies, has to consider the nature, scope, context and purposes of the processing.

Data protection officer (DPO)

The DPO is an expert on data protection laws and practices and has to be in the position to operate independently within the organization. The DPO needs to ensure the internal application of the Regulation and that the rights and freedoms of the data subjects are not likely to be adversely affected by the processing operation.

Data quality

Data quality refers to a set of principles distinguished in Article 5 of the GDPR namely:

- Lawfulness, Fairness and Transparency (see sections 2.4.1 and 2.4.2);
- Purpose limitation (see section 2.4.3);
- Data minimisation (see section 2.4.4);
- Accuracy (see section 2.4.5);
- Storage limitation (see section 2.4.4);

- Integrity and confidentiality (see section 2.4.6).

Data retention

Data retention refers to all obligations on the part of controllers to retain personal data for certain purposes.

Data subject

The data subject is the person whose personal data are collected, held and processed.

Data transfer

Transfers are subject to specific safeguards when the recipient is located in a country outside of the EU/European Economic Area (EEA) according to Chapter V of the GDPR.

Personal data

According to Article 4(1) of the GDPR ‘personal data’ means “any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”.

The name and the social security number are two examples of personal data which relate directly to a person. But the definition also extends further and also encompasses for instance e-mail addresses and the office phone number of an employee. Other examples of personal data can be found in information on physical disabilities, in medical records and in an employee’s evaluation.

Personal data which is processed in relation to the work of the data subject remain personal/individual in the sense that they continue to be protected by the relevant data protection legislation, which strives to protect the privacy and integrity of natural persons. As a consequence, data protection legislation does not address the situation of legal persons (apart from the exceptional case where information on a legal person also is related to a physical person).

Personal data breach

According to article 4(12) of the GDPR “personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”.

Privacy

Privacy is the ability of an individual to be left alone, out of public view, and in control of information about oneself. One can distinguish the ability to prevent intrusion in one’s physical space (“physical privacy”, for example with regard to the protection of the private home) and the ability to control the collection and sharing of information about oneself (“informational privacy”).

The concept of privacy therefore overlaps, but does not coincide, with the concept of data protection.

The right to privacy is enshrined in the Universal Declaration of Human Rights (Article 12) as well as in the European Convention of Human Rights (Article 8).

Privacy by design

Privacy by design aims at building privacy and data protection up front, into the design specifications and architecture of information and communication systems and technologies, in order to facilitate compliance with privacy and data protection principles.

Processing (of personal data, including sensitive data)

According to Article 4(2) of the GDPR, processing of personal data “means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction”

Personal data may be processed in many activities which relates to the professional life of a data subject and of course in the case of health treatments.

General Instructions for all data processing and methods

Personal data must be processed in a lawful, appropriate and transparent manner, and be correct and up to date. Beyond this provision, there are some general principles for any data processing activities within the ODIN project, which the consortium is committed to following:

1. **Data minimization:** In the context of ODIN pilots work, data processing, pursuant to articles 5 and 25 of the GDPR, must comply with the principle of “data minimization” by taking into account the restriction of the quantity of personal data processed, the processing operations, the disclosure time window, the conservation of data, the purposes of processing.
2. **Access to personal data:** Access will be provided only to those datasets that are strictly necessary to complete the task assigned.

The **person authorized for the processing** when performing processing operations is required to:

- Ascertain that relevant data protection information are delivered to the party concerned pursuant to Art. 13, 14 GDPR and verify that each particular processing operation contained therein (for example sharing, disclosing or profiling) is true and complies with the provisions of law and regulations;
- Enable and work toward facilitation of the exercise of the rights and powers provided for in Chapter III of the GDPR (*right to access, right to rectification, right to erasure, right to restriction, right to object, right to human intervention and appeal case of decision based exclusively on automated processing*), also specified in Section 2.6 of the current Data Management Plan;
- Not transmit to third parties information about personal data processed; communication and disclosure is allowed only if it is functional to the performance of the task assigned or

in compliance with regulatory obligations, and with the authorization of the internal data processor;

- Validate the identity of the data subject before providing information about their personal data or the related processing performed (limited to verifying the identification document without having to keep a copy);
- Store in physically safeguarded spaces (i.e., locked cabinets) any storage devices or document and drafts, containing personal data at the end of the processing period;
- Not to leave prints of documents containing personal data unattended at the photocopiers; this also includes following the “*clean desk*” policy by not leaving any important tabs/ documents open on an unattended laptop/computer/ device; only storing passwords in secure locations, etc.;
- Use appropriate paper shredders to destroy documents containing personal data. When such tools are not available, tear or cut into strips the documents so that they cannot be recreated;
- Keep the processed personal data for a period of time not exceeding that necessary for the purposes for which they were collected and processed, in compliance with the terms provided for by the law;
- Lower the tone of voice in the conversations and adopt an adequate distance (so-called “*courtesy distance*”) in order to avoid that third parties can, even involuntarily, process personal data and/or professional information;
- For any concerns regarding the processing of personal data, contact the pilot’s data protection officer, or the project’s DPO;
- Immediately report anomalies, incidents, thefts, accidental losses of data affecting the processing of personal data to the data protection officer in order to initiate the procedure for the communication of the data breach to the data protection authority and the parties concerned;
- Fulfil the confidentiality obligation in the period following the termination, if applicable, of the activities carried out in the context of the project;

It is recalled hereby that the consultation of the data contained in the databases does not allow any form of data sharing, disclosing and further processing that is not strictly necessary and functional to the fulfilment of the tasks and functions assigned.

Regarding document flows between the different WPs of the project, it is recalled that suitable organizational measures must be adapted to protect the confidentiality of personal data. These are to be thoroughly identified in the provided Data Management Questionnaires, discussed and, if needed, improved.

For data searches and other processing steps performed by means of IT tools, the authorized processor shall have a strictly **personal login credential** to access data.

Within the ODIN project, the authorized processor commits to:

- Not share their personal credentials with other users, except for the cases expressly allowed;
- Not access services that are not permitted;
- Not attempt to obtain system administrator privileges;
- Verify that the used devices are virus-free;

- Not connect devices that allow uncontrollable access to the institution's network devices as well as not to connect to insecure or insufficiently secured (i.e., public) networks;
- Erase all personal data from any storage devices (disk, USB flash drives, etc.) before reusing them; if this is not possible, the latter must be destroyed;
- Lock all tools or protected them with a password, if left unattended. Whether using online storage, a laptop, or some other technology, it is important for any data processor to make their password hard to guess. A good password system should make it as difficult as possible for attackers to access stored passwords, as well as from using force or guesses. It should not, however, place an undue burden on individuals either to remember the password or to make sure the account is secure.³¹ To mitigate the risk of easily guessed passwords, we recommend introducing additional authentication controls (i.e. two-factor authentication) or introducing a *strong password policy* that ensures the password's length, complexity, reuse and aging;³²
- Back up information; Data processors should keep a separate copy of any important information to avoid losing either the access to it, or the information itself permanently. One way to do a back-up is an online storage or to keep a copy on a separate hard drive or USB stick. It is imperative to set a strong password to protect the information and lock it away when not in use (see upper bullet point on password management).

Additional advisable measures³³ to protect ICT communication, include:

- Keeping the firmware, operating system and application software on the servers, client machines, active network components, and any other machines on the same LAN (including Wi-Fi devices) up to date. Ensuring that all reasonable IT security measures are in place, and regularly updated includes also keeping detailed logs of which patches are applied at which timestamp – this is important for the data controller in order to demonstrate compliance with Art. 5(2) GDPR;
- Designing and organizing processing systems and infrastructures to segment or isolate data systems and networks to avoid propagation of malware within the organization and to external systems;
- Having/ obtaining an appropriated, up-to-date, effective and integrated anti-malware software;
- Having/ obtaining an appropriated, up-to-date, effective and integrated anti-malware firewall, as well as an intrusion detection and prevention system. Directing network traffic through the firewall/ intrusion detection, even in the event of home office or mobile work (e.g., by using VPN connections to organizational security mechanisms when accessing the internet);

³¹ <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/passwords-in-online-services/>.

³² https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/04-Authentication_Testing/07-Testing_for_Weak_Password_Policy.

³³ EDPB Guidelines 01/2021 on Examples regarding Data Breach Notification, Sections 2.5, 3.4. Available here: https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf.

- Training employees on the methods of recognizing and preventing IT attacks. The data controller should provide means to establish whether emails and messages obtained by other means of communication are authentic and trustworthy. For example, employees should be advised to never open an email attachment from an unknown source, or download/ install programs from the internet;
- Conduct a vulnerability and penetration testing on a regular basis;
- Establish a Computer Security Incident Response Team (CSIRT) or Computer Emergency Response Team (CERT) within the organization and create an Incident Response Plan, a Disaster Recovery Plan and a Business Continuity Plan, and make sure the plans are thoroughly tested.

Specific Instructions for processing of special categories of data (GDPR Art. 9)

Without prejudice to the foregoing, for the processing of personal data referred to in this paragraph the following additional instructions are prescribed:

- Do not provide special categories of data (i.e., health data) by telephone when not absolutely certain about the identity of the recipient;
- Avoid sharing or disclosing documents containing special categories of data when other identifying information is present; in this case it is preferable to send the documentation without explicit reference to the party concerned (for example, by simply marking the documents with a code);
- Replace the name of the data subject with a code and keep the “name-code” association in a separate archive, which access is limited to a small number of authorized processors (so-called “*pseudonymization*”);
- Do not leave documents, including drafts, or any devices containing such data unattended and keep them in furniture fitted with a lock, whose keys must be properly stored;
- Keep documents containing data on health, sex life and sexual orientation in the aforementioned lockable containers, separately from any other documents;
- Apply all the necessary organization and security measures to guarantee the security of the datasets collected.

Processor

According to article 4 (8) of the GDPR “processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Processor agreement

Transfer of personal data from a data controller to a data processor must be secured by a data processor agreement. It must meet certain minimum requirements, as set forth by Article 28 of the GDPR.

The contract must stipulate, amongst other elements that the data processor shall act only on instructions from the data controller. The data processor must provide sufficient guarantees in respect of the technical security measures and organisational measure governing the processing to be carried out, and must ensure compliance with such measures.

Pseudonymisation

According to article 4(5) of the GDPR: “pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person”.

Retention periods

Data retention refers to all obligations on the part of controllers to retain personal data for certain purposes.

To limit how long you keep personal data is part of data minimisation. The rule of thumb is “as long as necessary, as short as possible”, although sometimes legal rules may impose fixed periods. Data that is no longer retained cannot fall into the wrong hands, nor be abused, meaning that defining and enforcing limited conservation periods helps to protect the people whose data are processed.

Special categories of personal data

Special categories of personal data include data that reveals: “racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural’s sex life or sexual orientation (Article 9 of the GDPR).

Processing of such information is in principle prohibited, except in specific circumstances. It is possible to process sensitive data for instance if the processing is necessary for the purpose of medical diagnosis, or with specific safeguards in the field of employment law, or with the explicit consent of the data subject.

Other Relevant Concepts

To facilitate the understanding of complementary concepts and issues, which concern pilot owners, but also the consortium as a whole, a number of other relevant concepts has been identified and offered for consulting purposes. As the current DMP is a live document, the definitions and concepts will be extended and furthered according to the demand and needs of the partners.

Processing for the Purpose of Scientific Research

The GDPR Art. 4 does not explicitly define what is a “processing for the purpose of scientific research”. Recital 159 suggest that *“the term processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. (...) Scientific research purposes should also include studies conducted in the public interest in the area of public health.”* Despite the Recital’s wording *“in a broad manner”*, the former Article 29 Working Party considers that this notion may not be stretched beyond its common meaning and understands that ‘scientific research’ in this context means *“a research project set*

up in accordance with relevant sector-related methodological and ethical standards, in conformity with good practice”³⁴

This definition is even so more important for identifying the legal basis for the conduct of the scientific research, and in particular when the legal basis is consent.

Further processing

EDPB’s guidelines divide the processing of health data for the purpose of scientific research into two types of data usages:

1. “Primary use”: the research on personal (health) data consists in using data, directly collected for the purpose of scientific studies.
2. “Secondary use”: the research on personal (health) data consists in further processing of the data, initially collected for another purpose.

For example, if a data subject (patient) provides their data and fills out questionnaires regarding their health condition or, in case of a disease research – their symptoms, and the information is used to research and document on said disease, then this is a primary use.

If a data subject (patient) provides their health records and health data to healthcare professionals to treat the disease, and the information is later on used by scientists to research on the disease, this is a secondary use.

The distinction between those types of data use is important in regard to the data protection principles coded in GDPR Art. 5.

Joint Controllership

GDPR Art. 26(1) provides that *“Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers”*.

Obligations of Joint Controllers

Joint controllership entails specific obligations for the parties involved. GDPR Art. 28(1) provides that joint controllers *“shall in a **transparent manner determine** their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. (...)”*

EDPB identifies³⁵ that the objective of these rules is to ensure that responsibilities for compliance with data protection obligations are clearly allocated in order for personal data to be sufficiently

³⁴ Guidelines on Consent under Regulation 2016/679 of the former Article 29 Working-Party from 6.7.2018, WP259 rev.01, 17EN, page 27 (endorsed by the EDPB). Available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

³⁵ EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Section 2, point 160. Available here: https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf.

protected, and to avoid loopholes whereby some obligations are not complied with by any of the parties involved in the processing in situations where multiple actors are involved.

Responsibilities of Joint Controllers

Following the provision in GDPR Art. 26(1) joint controllers are obliged to define their responsibilities for compliance with data protection obligations, similarly to the approach followed for determining data controller's responsibilities. Importantly, the joint controllers do not have to share equal responsibilities. In the Case C-210/16 (*Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein vs Wirtschaftskademie Schleswig-Holstein*), the Court of Justice of the European Union (CJEU) has ruled that *"the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case."*³⁶ Therefore, EDPS identifies that the parties involved in the processing operations should assess their roles and responsibilities taking into account the different stages in which they operate.³⁷ This could be determined by case-by-case assessment, as, for example, some of the joint controllers will interact with data subjects, while others will not, and in such situations it would make more sense to assign responsibilities for informing data subjects and dealing with request to the former.

Lastly, should one of the joint controllers wish to engage with a data processor, this does not affect their responsibilities in the joint controllership in any way. In practice, if a joint controller wants to create specific procedures for using processors in the joint controllership arrangement, they should consult the other controller(s) on the part of the processing to be entrusted to a processor and on the aspects of the contract to be put in place with a processor. When agreement on the aforementioned points has been reached, the controller and the processor may enter into an agreement.

Exercising Data Subjects' Rights

Pursuant to GDPR Art. 26(2) *"The essence of the arrangement shall be made available to the data subject."* The identification of the roles of the different controllers in a joint controllership is very important for the data subjects in order for them to understand who is responsible for what, and whom to address first when exercising their data subjects' rights. It is sufficient that the information is provided to the data subjects through the data protection notice, as in GDPR Art. 13.

Furthermore, according to GDPR Art. 26(3) data subject may exercise their rights under the GDPR in respect of and against each of the controllers, irrespective of the terms of the arrangement.

³⁶ Case C-210/16 *Wirtschaftskademie Schleswig-Holstein*, para. 43.

³⁷ EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725.

However, the practical side of the joint controllership agreement may result in complications for the exercise of the data subjects' rights, if the set roles and responsibilities may not allow the joint controllers the same means of granting data subjects the exercise of their rights as provided under the GDPR (such as the right of access, erasure or restriction, etc.). In relation to this, the arrangement between joint controllers should also include cooperation obligations, for example, in a form of a set contact point, an email address or an online contact form to which data subjects could address their requests.

Liability

GDPR Art. 82(4) provides that *“Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are (...) responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.”* This means that in joint controllership there is also a joint liability, and the full amount of compensation may be recovered from either of the joint controllers. Yet, this GDPR provision does not prevent a separate contractual allocation of liability and risk between joint controllers. Furthermore, GDPR Art. 82(5) allows the controller, who paid full compensation for the damage suffered, is entitled to *“claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage”*.

Appendix B Data management and ethics questionnaires

B.1 Data Management Plan Questionnaire



Data Management Questionnaire

The survey consists of two parts, according to the data, which you will be using in your research:

Part A – please complete this part, if your research generates data, i.e., technical data, patient data, forms of informed consent, participant data from interviews and workshops.

Part B – please complete this part, if you are using open database or publicly available datasets, i.e., public statistic data from NSI, etc.

Should you both generate data and use open-source data, please complete both parts (**Part A + Part B**) of the questionnaire.

Should you not process any data in the framework of your research, please do not fill out this survey.

Part A

1. **What type of data will be collected, processed, and stored in the framework of your ODIN tasks?** *Please identify the respective WP and task next to the type of data.*

2. **Would the collected data include personal* or sensitive* data?**

Yes

No

** Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. (GDPR Art. 4(1))*

** Sensitive data is data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. (GDPR Art. 9(1))*

3. **How will you collect the data?** *(i.e., directly from pilots, indirectly form technical systems; What research methods will be used: observations, interviews, workshops, participations in simulations, etc)*

4. **What will be the format of the collected data?** *Please specify the format to each of the datatypes identified in Question 1.*
5. **Data storage: Who will store the data and where?**
6. **What technical and organizational measures (TOMs) have you undertaken to securely store the data?** *(i.e., conducting regular back-ups to avoid unexpected data loss; physical and virtual secured access to data; documenting access rights; migrating data to best formats and media, etc.)*
7. **Retention period: how long will you keep the data?**
8. **How will you process and analyse the generated data?** *(i.e., digitalizing data, transcribing and translating data, validating, anonymizing data, deriving data, describing and documenting data, producing research outputs, etc.)*
9. **Will you process the generated data for any further purposes than the ones it was originally collected for?**
 - Yes (please specify for which purposes)
 - No
10. **How do you ensure secure processing of the generated data and mitigate potential risks for data subjects, such as de-anonymization?** *(i.e., anonymization techniques, pseudonymization, tokenization, etc.)*
11. **Will you share data with other partners inside the project? If yes, would there be data transfer to third countries?** *Please explain the measures you have undertaken to ensure a secured data transfer (i.e., transferring to third countries with confirmed level of data protection on the basis of an adequacy decision; encryption, etc.)*
12. **Would your generated data be openly accessible beyond the lifetime of the project?**
 - Yes (please explain how it will be shared)
 - No (please explain why you will not share the data)
13. **Will your data be re-usable? If yes, how and what measures will you undertake to protect it?**
14. **How do you recruit participants for the activities in your tasks/ WP?** *(i.e., existing contact lists, social media, general public, academics, etc.)*
15. **How do you ensure fairness and avoid any discrimination during the recruitment process?**

16. Does your organization have a Data Protection Officer (DPO)?

- Yes (please provide their name and contact information)
- No

17. Complementary to the GDPR, the EU Member States have laid down own rules for data processing (i.e., additional requirements for processing of special categories of data).

Please submit a signed declaration of compliance to complementary national regulations (of the country which legislation applies to your organization) regarding the rights of the data subjects and, if applicable, the processing of biometric, genetic, or health data.

18. Do your research activities include profiling*? If so, please explain how you inform the data subjects about the profiling, its possible consequences and how you will safeguard their fundamental human rights and attach the consent forms you are using.

**Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. (GDPR Art. 4(4))*

Part B: Existing open database or publicly available datasets

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>
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

Please add here any additional comments.

B.2 Ethics Management Questionnaires



Ethics Management Questionnaire

The current questionnaire is mandatory to be filled out **by each pilot owner**. Please attach any required forms either to this document, or as a separate attachment to the email with the returned completed questionnaire.

The European Commission has identified that for all activities funded by the European Union, ethics is an integral part of research from beginning to end, and ethical compliance is pivotal to achieve real research excellence. Regardless of the discipline, research involving human participants, and especially such involving personal data processing, requires an ethical review assessment and an ethical approval. To comply with these obligations, researchers and organization representatives need apply for ethical approval at their local Ethics Committees (i.e., University, Research Institute, Hospital, etc.) and follow their local guidance and procedures for the application.

General

1. What is your procedure for identification of participants? *(i.e., existing contact lists, social media, general public, academics, etc.)*

.....
.....
.....

2. What is your procedure for recruitment of participants?

.....
.....
.....

3. Do you have an informed consent procedure in place?

Yes (Please describe it below and attach a copy to the questionnaire of the consent form used in the context of your pilot)

No (A template will be provided in D11.1. Please utilize it and tailor it to the needs of your pilot)

.....
.....
.....

Ethical Approval (EA) Procedure

1. Do you need to submit an EA?

Yes

No (*Please describe below why, what is your alternative strategy, and what kind of EA do you need*)

.....
.....
.....

If you have answered "YES" to the question above:

2. What type of EA do you have?

.....
.....
.....

3. Please explain the procedure you have followed in order to obtain EA.

.....
.....
.....

Documents for the Ethical Approval

Please attach the following documents, if applicable:

- a) **Main document** (*i.e., summary of the clinical study, study design, methodology & data analysis, recruitment, etc.*)
- b) **Participant Information sheet**
- c) **Informed consent form**
- d) **Ethical Approval** (if already obtained)

Others

Please specify in this section if you have already provided any temporary documents and if these have been submitted to the reference body. When do you foresee obtaining and send a final document?

.....
.....
.....

Appendix C Informed Consent

C.1 Essential Information for Prospective Research Participants



INFORMATION SHEET

You have been invited to take part in the European Commission funded ODIN project coordinated by MEDTRONIC IBERICA SA (MDT). The project is funded by the EU's Horizon 2020 programme and will be conducted by the ODIN consortium of 20 (twenty) partners. The current sheet provides information about the project and the role of participants.

Your participation is voluntary, and you are free to withdraw from participation at any time, without needing to provide any reason for that; your withdrawal can be also expressed orally and will not have any retroactive consequences. Before you consent to participating, please read carefully the current information sheet about why the research is being done and what it will involve. Please do not hesitate to ask questions and make sure that you have a complete understanding of the activities you are participating in.

Purpose of the ODIN Project:

ODIN will address critical hospital challenges with the use of robotics, Internet of Things (IoT) and Artificial Intelligence (AI) in order to empower workers, enhance medical locations, and introduce autonomous and collaborative robots. The areas of intervention will be piloted in six hospitals (Spain, France, Italy, Poland, The Netherland, Germany). ODIN pilot will be a federation of multicenter longitudinal cohort studies, demonstrating the safety, effectiveness and cost-effectiveness of ODIN technologies for the enhancement of hospital safety, productivity and quality. Our vision is that data-driven management (enabled by Industry 4.0 tech) and Evidence Based Medicine with data-driven procedures can revolutionize hospital management.

The ODIN Consortium consist of 20 organizations:

Partner	Short Name	Country
MEDTRONIC IBERICA SA	MDT	Spain
ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS	CERTH	Greece
IDRYMA TECHNOLOGIAS KAI EREVNAS	FORTH	Greece
THE UNIVERSITY OF WARWICK	UoW	United Kingdom
SCUOLA SUPERIORE DI STUDI UNIVERSITARI E DI PERFEZIONAMENTO S ANNA	SSSA	Italy

ROBOTNIK AUTOMATION SLL	ROB	Spain
MYSHERA SL	MYS	Spain
TWI ELLAS ASTIKI MI KERDOSKOPIKI ETAIREIA	THL	Greece
PHILIPS ELECTRONICS NEDERLAND BV	PEN	Netherlands
UNIVERSIDAD POLITECNICA DE MADRID	UPM	Spain
INFORMATICA EL CORTE INGLES SA	INETUM	Spain
UNIVERSITA CAMPUS BIO MEDICO DI ROMA	UCBM	Italy
UNIVERSITAIR MEDISCH CENTRUM UTRECHT	UMCU	Netherlands
SERVICIO MADRILENO DE SALUD	SERMAS	Spain
CHARITE - UNIVERSITAETSMEDIZIN BERLIN	CUB	Germany
CENTRE HOSPITALIER UNIVERSITAIRE HOPITAL NORD	AMIS	France
UNIVERSYTET MEDYCZNY W LODZI	MUL	Poland
MINDS & SPARKS GMBH	M&S	Austria
UDG ALLIANCE	UDGA	Switzerland
UNIVERSITA DEGLI STUDI DI FIRENZE	MEDICT	Italy

As part of the current research activities, we would like to achieve:

[Please provide the goals here]

If you agree to take part in the research, any personal information that will be collected from you will be used for internal processing and administrative purposes only, as well as to enable us to contact you, if any further information is required. Your details will be kept for a maximum period of XX months following the end of the research project. Unless you prefer otherwise, we will not publish any information in reports or communications materials that would enable you to be directly or indirectly identified.

What will I be asked to do?

[Please describe in detail the activities]

Recording

[Please describe here, whether the participation will be recorded, where and to whom will be recording be accessible, and for how long]

Where will the research take place take place?

The research will take place at [Please name the organization/ location, where the research will take place]

What will you use my participation for?

[Please list what the results of the participation will be used for]:

- XXX
- XXX

Additionally, the provided information from you may be used for writing of articles for peer-reviewed journals and magazines, for presentations at conferences and workshops, and/ or to promote the ODIN project. Unless indicated otherwise, any information relating to an identified or identifiable natural person (personal data) will be **anonymised**.

What are the potential risks of participating in research?

We do not envisage any potential risks for your rights and freedoms to be caused by your participation.

Are there any costs/ remuneration for the participation?

The involvement in the current research activities is neither chargeable (to you), nor remunerated (by us).

Storage of data and retention period

All data will be stored [Please specify where the data will be stored and for how long]

Observation notes and information from feedback forms will be shared with only those members of the consortium, who require access for the completion of their work. This information will be retained for the lifetime of the project. After the research ends, it will be permanently and irrevocably deleted after a maximum of XX years.

Data Protection Officer (DPO)

The DPO of our institution is: [Name]

For further questions, please do not hesitate to contact him/her under the following email address/
contact number: [*Please provide contact details of the organization's DPO*]

Data Controller

The Data Controller in the current research activities is: [*Name of your organization*]

Please contact him/her for further questions: [*Please provide contact details*]

Lawfulness of Data Processing

The legal basis of the processing of your personal data is based on your consent, the performance of a task carried out in the public interest, and the legitimate interests of the data controller (GDPR Art. 6(a, e, f)).

Your rights and confidentiality

All collected data will be anonymised. We will only collect and process data that is strictly necessary for running the research, for our internal processing, administrative purposes, and to enable us to contact you if we require further information. The record of your participation will be kept in a file separate from the research data. These data will not be shared with or disclosed to anyone outside the research team.

All information we collect about you will be kept strictly confidential unless we are required to share your information with the European Commission as part of our obligations. However, the researcher has a duty of care to report to the relevant authorities possible harm/danger to the participant or others. If this was the case, we would inform you of any decisions that might limit your confidentiality. All data, including audio files, will be stored on password protected computers, in a secure location at the [*Please provide the location of your local storage or the location of the secure server within the EU*]. Every effort will be taken to protect your identity. You will not be identified in any report or publication of this study or its results. You can review any recording/notes that concern you should you choose to do so.

You have the right to access, update, correct and erase all personal data. As to the qualitative information that you provide us with, **you have a right to withdraw** the same up to the point of publishing the information in the relevant deliverable. Your researcher will inform you as to the planned publication date.

You have a right to lodge a complaint. To do so, please contact the researcher or project coordinator (details below); they will pass your complaint onto an independent panel.

Right to withdraw

You may withdraw your consent from this project at any time without giving a reason. You may walk away at any time. You may tell the researcher at any time that you would like to stop. Simply tell the data processor to delete your data or whether you are fine for these data to continue to be processed. You may be asked why you have decided to withdraw, but you are under no obligation to give a reason.

Sensitive information

Sensitive personal data relates to specific categories of data which are defined as data relating to a person’s racial origin; political opinions or religious or other beliefs; physical or mental health; sexual life; criminal convictions or the alleged commission of an offence; trade union membership. If sensitive data is collected, it is done to be compliant with the project’s non-discrimination requirements and will be fully anonymized.

Research with participants in non-EU countries

If you are from outside of the EU, we ask you to note that the personal data will be transferred to and stored in the EU/EEA.

Keeping in touch with the project

As ODIN is a research and innovation action, it is essential to share the high-quality results of the project with stakeholders who are likely to benefit from it. You can choose to be kept informed about the project’s progress, and will thus be put on a mailing list, however this is not mandatory.

For more information on the project, please contact:

Project Coordinator	Researcher
Name:	Name:
Organisation: Medtronic SA	Organisation:
E-mail:	E-mail:

C.2 Sample Information Consent Form



CONSENT SHEET

I volunteer to participate in the current research conducted by the ODIN consortium, coordinated by MEDTRONIC SA, entitled ODIN. The ODIN consortium consists of 20 organisations:

Partner	Short Name	Country
MEDTRONIC IBERICA SA	MDT	Spain
ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS	CERTH	Greece
IDRYMA TECHNOLOGIAS KAI EREVNAS	FORTH	Greece
THE UNIVERSITY OF WARWICK	UoW	United Kingdom

SCUOLA SUPERIORE DI STUDI UNIVERSITARI E DI PERFEZIONAMENTO S ANNA	SSSA	Italy
ROBOTNIK AUTOMATION SLL	ROB	Spain
MYSPHERA SL	MYS	Spain
TWI ELLAS ASTIKI MI KERDOSKOPIKI ETAIREIA	THL	Greece
PHILIPS ELECTRONICS NEDERLAND BV	PEN	Netherlands
UNIVERSIDAD POLITECNICA DE MADRID	UPM	Spain
INFORMATICA EL CORTE INGLES SA	INETUM	Spain
UNIVERSITA CAMPUS BIO MEDICO DI ROMA	UCBM	Italy
UNIVERSITAIR MEDISCH CENTRUM UTRECHT	UMCU	Netherlands
SERVICIO MADRILENO DE SALUD	SERMAS	Spain
CHARITE - UNIVERSITAETSMEDIZIN BERLIN	CUB	Germany
CENTRE HOSPITALIER UNIVERSITAIRE HOPITAL NORD	AMIS	France
UNIVERSYTET MEDYCZNY W LODZI	MUL	Poland
MINDS & SPARKS GMBH	M&S	Austria
UDG ALLIANCE	UDGA	Switzerland
UNIVERSITA DEGLI STUDI DI FIRENZE	MEDICT	Italy

The project is funded by the European Commission under the Horizon 2020 funding programme, grant agreement number 101017331. The project began in 1st March 2021 and will continue for the duration of 42 months.

By signing this form, I agree to take part in the ODIN research. The nature of the research, my involvement in it and my rights regarding my participation are explained in the Information Sheet accompanying this form.

Please place an “X” in the box on the right to affirmatively consent to the following statements:	
1. I confirm that I have read and understood both this form and the accompanying Information Sheet. I had the time and opportunity to ask questions as needed.	<input type="checkbox"/>
2. I understand that I am free to withdraw my consent at any time without giving reason and that my participation in this project is voluntary.	<input type="checkbox"/>
3. I am aware of the potential risks and benefits of this research study.	<input type="checkbox"/>
4. I consent to participate in the research activities as described in the Information Sheet having been fully informed of the potential risks, benefits and alternatives of the research study: a) [XXX Insert research activity 1] b) [XXX Insert research activity 2, etc.]	<input type="checkbox"/> <input type="checkbox"/>
5. I consent to the processing of my data. My personal data can be gathered to be used, stored and shared in the ways described on the accompanying Information Sheet. The personal data collected will be processed following the GDPR and pseudonymised/anonymised to the greatest extent possible.	<input type="checkbox"/>
6. I consent to [being [audio/video] recorded] having my personal data processed, and having notes of my activities taken for: a) Ongoing research to improve ODIN user requirements, revise design, develop ODIN technologies and ODIN policy management; b) Dissemination activities (e.g., articles for peer-reviewed journals, presentations at conferences); c) Promotion of ODIN in general.	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
7. I understand my right to request access to any, and all, personal information that I have voluntarily provided as part of my participation, and that I may ask for that information to be rectified and/or amended if it is inaccurate, or request that all personal information that I have provided be deleted (if not yet already anonymised).	<input type="checkbox"/>
8. I understand that the ODIN consortium intends on retaining my personal details for a period of up to XX months following the completion of the project. Information from research activities will be permanently and irrevocably deleted after a maximum of 5 years after the end of the project.	<input type="checkbox"/>

Project Coordinator

Name:

Organisation: MEDTRONIC SA

E-mail:

National Data Protection Officer

Name:

E-Mail:

Tel.:

Appendix D How to Determine the roles of Data Controller, Data Processor and Joint Controllers in the Praxis

In order to support the consortium members in identifying their roles in the personal data processing activities, the following flowcharts provide guidance based on practical questions.

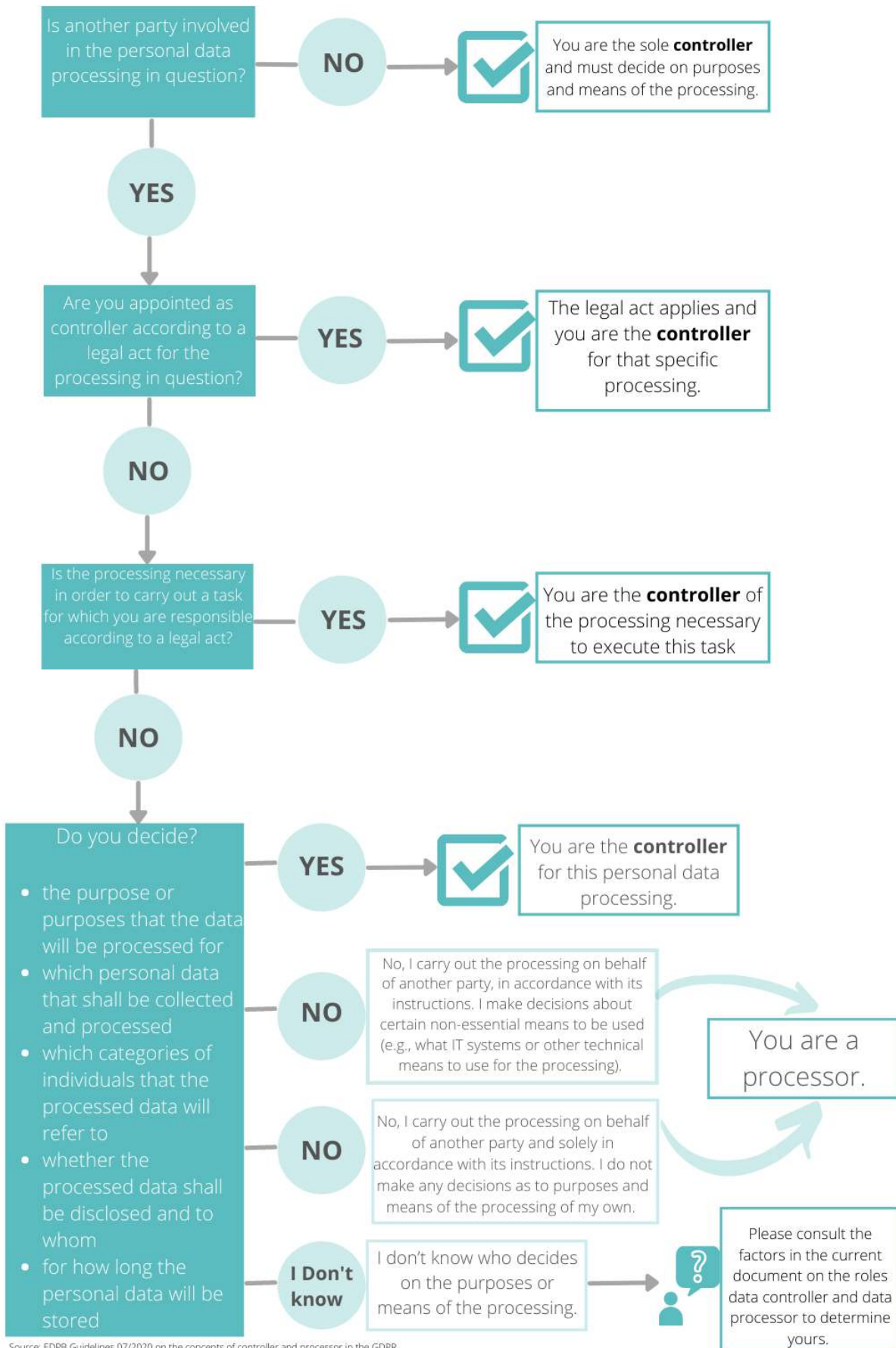
D.1 Data Controller or Data Processor

The following figure presents a summary of common indicators whether a consortium party handles as a data controller or a data processor. The envisioned methodology is as follows:

1. Consult the flowchart in the following page
2. Should there still be unclarities or questions regarding your role, please consult the figure “*Indications for Data Controllers and Data Processors in the GDPR*”
3. If any more doubts remain, please get in touch with the DPO of your organization, or with the project’s DPO at aguesada@udgalliance.org.

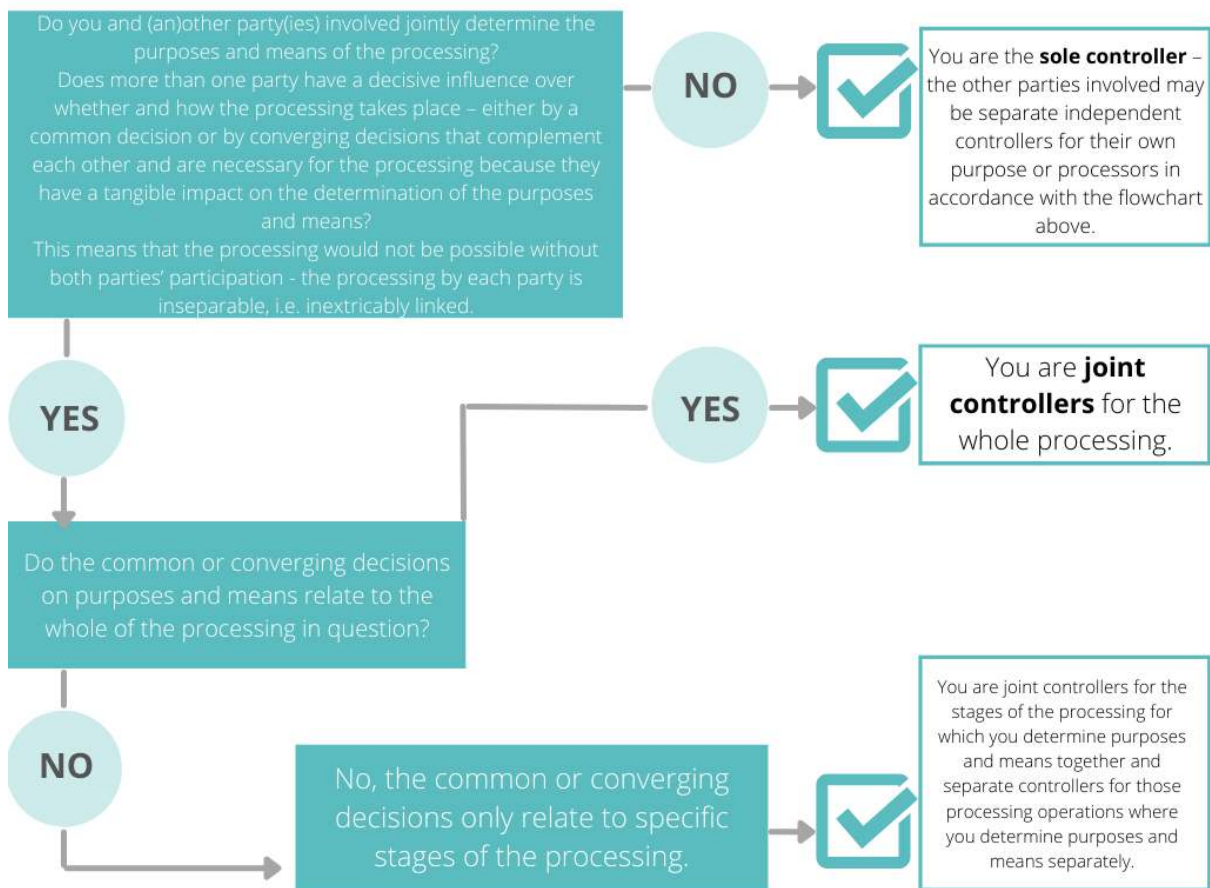
INDICATIONS	
The following factors should help you to determine the appropriate qualification of your role:	
DATA CONTROLLER	DATA PROCESSOR
<ul style="list-style-type: none"> • You obtain a benefit from, or have an interest in, the processing (other than the mere payment for services received from another controller) • You make decisions about the individuals concerned as part of or as a result of the processing (e.g. the data subjects are your employees) • The processing activities can be considered as naturally attached to the role or activities of your entity (e.g. due to traditional roles or professional expertise) which entails responsibilities from a data protection point of view • The processing refers to your relation with the data subjects as employees, customers, members etc. • You have complete autonomy in deciding how the personal data is processed. • You have entrusted the processing of personal data to an external organisation to process the personal data on your behalf. 	<ul style="list-style-type: none"> • You process the personal data for another party’s purposes and in accordance with its documented instructions - you do not have a purpose of your own for the processing. • Another party monitors your processing activities in order to ensure that you comply with instructions and terms of contract. • You do not pursue your own purpose in the processing other than your own business interest to provide services. • You have been engaged for carrying out specific processing activities by someone who in turn has been engaged to process data on another party’s behalf and on this party’s documented instructions (you are a sub-processor).
Source: EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR	

Figure 8: Indications for Data Controllers and Data Processors in the GDPR



Source: EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR.

D.2 Joint Controllorship Flowchart



Source: EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR.

Appendix E Declarations of Compliance with National Regulations

This section compiles the declarations of compliance obtained from relevant partners in the framework of the POPD requirement N.2 for the ODIN project. Further information will be provided in subsequent iterations of this deliverable as necessary.



This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No. 833805

Declaration of Compliance with GDPR and national legislation

Name of the Legal Representative: **María Benítez Montoro**
Legal Representative for [Organization]: **Robotnik Automation, S.L.L.**
Contact details: **mbenitez@robotnik.es**

As the Legal Representative for Robotnik Automation, S.L.L. (hereinafter 'Organisation'), I **María Benítez Montoro** have been provided with information relating to the data processing operations that may be carried out by members of this Organisation in order to fulfil our obligations within the ODIN project.

This Organisation will perform or contribute to data processing operations, which will make it a (joint) Data Controller, as defined by Article 4(7) of the General Data Protection Regulation. The Organisation will comply with all requirements relating to that role.

I have checked if special derogations pertaining to the rights of data subjects or the processing of genetic, biometric and/or health data have been established under the national legislation of the country where the research takes place. The following national derogations and national legislations apply in this project: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

I can confirm that the members of the Organisation involved in the ODIN project will be made fully aware of their obligations in this regard.

I have reviewed the text of the GDPR, including provisions in the GDPR that grant Member States legislative competence, and I am familiar with the GDPR implementation act of the country in which this Organisation resides. I confirm that this Organisation is in compliance with the GDPR and all national GDPR implementation acts that are applicable to this Organisation.

I confirm that all personal data collection and processing will be carried out according to EU and national legislation. Specifically, I confirm that in case of further processing of previously collected personal data, the Organisation will identify a lawful basis for the data processing and that the appropriate technical and organisational measures, as defined in the ODIN DMP and internal rules, are in place to safeguard the rights of the data subjects.



This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No. 833805

This also includes that in case personal data are transferred from the EU to a non-EU country or international organisation, I confirm that such transfers will be in accordance with Chapter V of the General Data Protection Regulation 2016/679.

Signature:



Name: María Benítez

Date:

23-11-2021

Robotnik

MINDS & SPARKS

Vienna, 9th December 2021

ODIN: Declaration of Compliance to complementary national regulations

Applicable legislation is the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC) and the Austrian legislation on the protection of personal data “Datenschutzgesetz (DSG), BGBl. I Nr. 165/1999, idgF. which has incorporated the GDPR in the national legal framework.

No biometric, genetic or health data will be collected and/or processed.

Dr. Peter Leitner
Managing Director



MINDS & SPARKS GmbH
Gumpendorfer Straße 73/17
1060 Vienna
Austria

E-Mail contact@mindsandsparks.org
Web www.mindsandsparks.org
Phone +43 1 9972019



Declaration of Conformity
to Data Protection and Processing Legislation

The undersigned, Dr. Panagiotis Chatzakos, who is the Security officer and the EU Data Representative of TWI Hellas Astiki Mi Kerdoskopiki Etaireia, confirms that all data collection and processing will be carried out in full accordance with EU and national legislation.

For the avoidance of doubt, in cases where the corresponding legislative requirements differ, the stricter policy will be applied.



Data Security Officer
Dr. Panagiotis Chatzakos

ODIN

Declaration of compliance with the national legal framework

In the context of ODIN project and more specifically the activities of WP5, datasets will be generated by humans' monitoring in hospitals (e.g. patients, healthcare personnel, caregivers) by robotics assistants.

We declare that this data processing activities undertaken in the context of the ODIN project are in conformity with the applicable national legal norms EU and international legislation as quoted below:

- The Universal Declaration of Human Rights and the Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data
- Directive 95/46/EC & Directive 2002/58/EC of the European parliament regarding issues with privacy and protection of personal data and the free movement of such data.
- The EU General Data Protection Regulation (GDPR) which replaced the Data • Protection Directive 95/46/EC to harmonize and re-shape all data privacy laws across
- Law 4624/2019 (Greek Government Gazette A137) By Law 4624/2019 , measures are laid down for the implementation of the GDPR and Directive (EU) 2016/680 is incorporated into national legislation.
- Law 2471/1997 (Greek Government Gazette A50) Law 2472/1997 was repealed, except for the provisions specifically mentioned in article 84 of Law 4624/2019.

Compliance with these norms/measures is guaranteed through:

- Data management planning guided by robust data practices, strategies and policies that will be respected and followed by all the members of the consortium.
- Data processing in alignment with proportionality and minimization, the core principles related to the processing of personal data according to GDPR
- Data protection implementing the concept of 'privacy by design' and 'privacy by default' which provides a framework systems' design, databases and processes on respect for data subjects' fundamental rights.
- In consistency with 'data protection by design', appropriate technical and organisational measures have to be implemented in order to give effect to the GDPR's core data-protection principles (articles 5 and 25 GDPR).

- Consent procedure and information of the project shared to participants in alignment with GDPR to enable data subjects to be informed accordingly in an explicit and understandable format and exercise their fundamental rights during the overall lifecycle of the project.

Signature

Ioannis Chalinidis, DPO, 15/12/2021

A handwritten signature in black ink, appearing to be 'Ioannis Chalinidis', written over a horizontal line.

ACREDITACIÓN



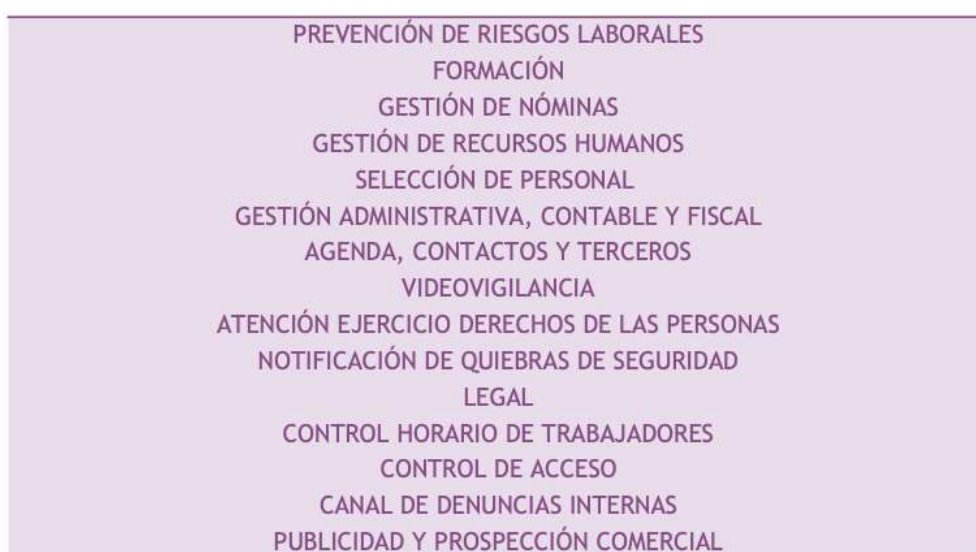
GESPRODAT S.L. acredita que la empresa:

GESPRODAT S.L. accredit that the company:

MYSPHERA, S.L.

Ha evaluado las medidas de protección de los tratamientos que contienen datos de carácter personal listados a continuación:

Has assessed the protection measures of the processing of personal data listed below



resultando adecuadas conforme a las disposiciones de la
which are in compliance with the provisions of the

NORMATIVA VIGENTE

Reglamento (UE) 2016/679 del Parlamento Europeo, de 27 de abril de 2016 y la Ley Orgánica 3/2018, de 5 de diciembre, sobre la Protección de Datos y Garantías de los Derechos Digitales

Certificado válido para la(s) siguiente(s) instalaciones

Auditoría en modalidad online

Fecha: 04/09/2021



Adela Castellar Alcaina
Director General



Date December 18th
Regarding Declaration of compliance

To whom this may concern,

*Division Laboratories,
Pharmacy and Biomedical
Genetics*

Central Diagnostic Laboratory

Phone +31 (0) 6 50177633
s.haitjema@umcutrecht.nl

Hereby I declare UMC Utrecht is fully compliant with national regulations that complement GDPR regarding the rights of data subjects and the processing of health data.



Saskia Haitjema MD PhD
PI for the ODIN project

Visiting address:
Heidelberglaan 100
3584 CX Utrecht
The Netherlands

Correspondence:
Internal postal address G03.550
P.O. Box 85500
3508 GA Utrecht
The Netherlands



Madrid, December 20, 2021

DECLARATION OF CONFORMITY

Mr. Carlos Muñoz Pérez of legal age, with D.N.I. number 01097195-A and on behalf of INETUM ESPAÑA, S.A., with legal address María de Portugal 9-11, 28050 Madrid, and Spanish tax number A-82206400.

Declares,

The Inetum group at the European level has carried out an internal project of adaptation to the GDPR, in order to define and implement the necessary actions to ensure compliance with the General Data Protection Regulation (EU) 2016/679, of April 21, 2016, and the local legislation in force.

To this end, the degree of compliance with the GDPR in Inetum companies in Spain has been evaluated and determined an action plan to adapt our contracts, systems, processes and organization to the new context.

Once the adaptation project has been completed, a periodic audit process has been initiated in order to determine the adequacy of the measures and controls to the Law and its regulatory development and identify improvements and propose necessary corrective or complementary measures.

Signed.: INETUM ESPAÑA

Firmado por 01097195A
CARLOS MARIA MUÑOZ (R:
A28855260) el día
20/12/2021 con un
certificado emitido por AC

Mr. Carlos Muñoz Pérez
General Manager

Inetum

María de Portugal, 9 – 28050 Madrid (España)
Tel. +34 91 383 63 20

CUB has provided the declaration of compliance with national regulations, which is an online documentation on the institutional webpage:

https://www.charite.de/en/service/data_protection/.

Medtronic

Global Data Protection & Privacy Office Statement of Compliance



Overview

The Medtronic Data Protection and Privacy Program ('Privacy Program') seeks to **"Enable the Medtronic Mission through ensuring the privacy and proper use of the data of our people, assets, and systems by implementing policies, procedures and safeguards"**.

The Privacy Program supports each Medtronic business, function and geographical region to:

- develop and implement appropriate privacy protections for Personal Data,
- demonstrate accountability for the Personal Data that Medtronic controls,
- facilitate compliance with global data protection and privacy laws and regulations, and with Medtronic privacy policies and standards, and
- satisfy compliance obligations concerning data protection and privacy.

Data Protection and Privacy Principles

The Medtronic Privacy Program is built upon a global privacy framework, incorporating the following seven specific privacy principles that are uniformly addressed throughout the Company's geographic footprint.

1. **Notice** - Where Medtronic collects Personal Data directly from individuals, it will provide notice about the purpose(s) for which it collects and uses the Personal Data, the non-vendor third parties (names are excluded due to confidentiality) to which Medtronic discloses the Personal Data, and the choices and means, if any, Medtronic offers individuals for limiting the use and disclosure of their Personal Data.

Where Medtronic processes Personal Data of Data Subjects on behalf of its customers (the 'Data Controller'), Medtronic will provide its customers with the information that the customer as a Data Controller needs to assess compliance with data protection laws. Also, to the extent possible, Medtronic will design its relevant systems and applications in order to enable the customer to see, change, and delete its Data Subjects' Personal Data. To the extent that Medtronic's systems or applications do not yet allow the customer to fully execute the Data

Subjects' requests, Medtronic is able to execute the requests in accordance with the customer's instructions.

2. **Choice** - Where required by law, Medtronic will offer Data Subjects the option to choose whether or not their Personal Data may be disclosed to a non-vendor third party, or may be used for a purpose other than the purpose for which it was originally collected or subsequently authorized by the Data Subject.
3. **Consent** - When collecting Personal Data as a Data Controller, and where required by law, Medtronic will provide Data Subjects the opportunity to affirmatively and explicitly consent to the disclosure of their Personal Data to a non-vendor third party or to the use of the Personal Data for a purpose other than the purpose for which it was originally collected or subsequently authorized by the Data Subject.
4. **Data Integrity** - Medtronic will only use Personal Data in ways that are compatible with the purpose(s) for which it was collected, subsequently authorized by the Data Subject or as authorized by law. To the extent possible, Medtronic will take reasonable steps to assess and verify, where applicable, that Personal Data is relevant to its intended use, as well as accurate, complete, and current.
5. **Transfers to Third Parties** - Medtronic will obtain assurances from third-party vendors with whom Data Subject's Personal Data is rightfully shared, that the third-party vendors will safeguard the Personal Data consistent with Medtronic's privacy policies. Where Medtronic is aware that a third-party vendor is using or disclosing Personal Data in a manner contrary to Medtronic's policies, Medtronic will take reasonable steps to stop the third-party vendor from such improper use or disclosure.
6. **Access and Correction** - Upon request and verification, Medtronic will grant Data Subjects reasonable access to their Personal Data. In addition, Medtronic will take reasonable steps to permit Data Subjects to correct, amend, or delete Personal Data that is demonstrated to be inaccurate or incomplete.
7. **Security** - Medtronic will take reasonable precautions to protect Personal Data in its possession from loss, misuse and unauthorized access, disclosure, alteration, and destruction.

**Personal Data: information that can directly or indirectly identify an individual.*

*** Data Subject: an identified or identifiable person*

**** Data Controller: the party that determines the purposes and means of the processing of personal data*

Regional and local requirements

The Privacy Program team partners with in-country counsel to identify, address and incorporate local laws and regulations into the privacy program framework and policy structure. This approach provides flexibility in implementation of privacy requirements globally.

People and processes

Any Medtronic employee directly involved in processing Personal Data or Sensitive Information is required to be trained and made aware of his/her responsibilities regarding this information. The Privacy Program team partners closely with the Global Security Office to enable the implementation of security safeguards including role-based access, standardized authentication methods, audit and monitoring capabilities, encryption, and other standard controls.

Medtronic has a data breach response program in place that provides for a swift analysis, escalation and response process in case of data privacy incidents.

Compliance

Medtronic proactively performs privacy impact assessments to identify, assess and addresses privacy risks, and designs new products and applicable services in accordance with “privacy by design” principles. Additionally, Medtronic uses standard templates and processes developed by the Privacy Program to ensure the appropriate privacy provisions are incorporated into third party contracts. Medtronic’s goal is to make its products as safe and secure as possible, while maintaining ease of use for the patients, physicians and others who depend on them. These fundamental objectives are aligned to promote and foster a robust Privacy Program.

Luca Staffa

Luca Staffa
EU Data Protection Officer