



D8.6 Data ethics in public procurement for hospitals version 3

Deliverable No.	D8.6	Due Date	30/11/2024
Description	The report introduces the final ethics assessment of the planned and executed activities in the ODIN project and beyond it, including an update of the mapping and assessment of relevant data ethics principles for public procurement for hospitals, and sets the stage for the ethical activities beyond ODIN.		
Type	Report	Dissemination Level	CO
Work Package No.	WP8	Work Package Title	Legal, Ethical and Standardisation Aspects for Sustainability
Version	1.0	Status	Final



Authors

Name and surname	Partner name	e-mail
Adrian Quesada Rodriguez	UDGA	aquesada@udgalliance.org
Renata Radocz	UDGA	rradocz@udgalliance.org
Vasiliki Tsiompanidou	UDGA	vtsiompanidou@udgalliance.org
Iida Lehto	UDGA	llehto@udgalliance.org
Sébastien Ziegler	UDGA	sziegler@udgalliance.org
Ana María Pacheco	UDGA	admin@udgalliance.org
Javier del Rio	UPM	jrio@lst.tfo.upm.es
Pablo Lombillo	MYS	plombillo@mysphera.com
Vasileos Lolis	ITI	vaslwlis@iti.gr
Ilias Kalamaras	ITI	kalamar@iti.gr
Dimitra Triantafillou	ITI	dtriant@iti.gr
Petros Toupas	ITI	ptoupas@iti.gr
Sofia Granda	INETUM	sofia.granda@inetum.com
Alex Barnadas	INETUM	alex.barnadas@inetum.com ;
Luis Carrascal	INETUM	luis.carrascal@inetum.com
Antonio Jesus Gamito	INETUM	antonio-jesus.gamito@inetum.com
Daphni Plati	UIO	daphni.plati@gmail.com
Marcello Chiurazzi	SSSA	Marcello.Chiurazzi@santannapisa.it
Gastone Ciuti	SSSA	Gastone.Ciuti@santannapisa.it

History

Date	Version	Change
01/01/2024	0.1	D8.6 generation and first draft
01/03/2024	0.2	Updated legal analysis
01/04/2024	0.3	Revision of procurement section
11/05/2024	0.4	Alignment with relevant deliverables
01/06/2024	0.5	Questionnaire submitted to partners
24/06/2024	0.6	First draft ready, awaiting inputs from plenary meeting regarding questionnaire
24/07/2024	0.8	All inputs received, draft submitted for internal review
31/07/2024	0.9	Original deliverable submission date, delayed to align contents and recommendations with Certification Deliverable
15/11/2024	1.0	Inputs from certification deliverable integrated, inputs added addressing regulatory compliance certification and data governance avenues, questionnaires for annexes integrated, peer review integration
26/12/2024	1.1	Deliverable submitted to peer review
20/02/2025	1.2	Final submission

Key data

Keywords	Data ethics; public procurement; hospitals; data governance; transparency; accountability; ethical impact assessment
Lead Editor	Adrian Quesada Rodriguez (UDGA)
Internal Reviewer(s)	UPM: Alejandro M. Medrano Gil MYS: Pilar Sala

Abstract

The current document builds upon the results of the ODIN deliverable 8.4 and introduces new elements in line with the latest developments of the project, and in direct alignment with the actions carried out in other tasks of WP8 and WP1. The deliverable focuses on two main areas of action: 1) updating the research from the last deliverable on data ethics in hospital public procurement; and 2) presenting the procurement process in light of European dispositions and Key Exploitable Results (KERs) in a manner that aligns the expected outputs with the requirements of the ODIN's exploitation tasks towards easing future sustainability of the platform and its KERs.

The first of these activities is performed by using a praxis-oriented methodology. This document creates a link between the theoretical research findings and the project's practical implementation by mapping the most pertinent national, European, and worldwide instruments for ethical and regulatory compliance. In particular, the deliverable focuses on analysing the requirements for data procurement and the use of Artificial Intelligence (AI) under the General Data Protection Regulation (GDPR), the AI Act, the European Health Data Space Regulation (EHDS), the Medical Device Regulation (MDR) and the Data Governance Act (DGA). To ease understanding, transparency and impact maximization (particularly towards orientation of the project's various stakeholders regarding the procurement process and the considerations that should be addressed when preparing KERs -and their documentation- for ethical and regulatory compliance validation), decision trees have been generated for each regulatory framework.

The next sections of the deliverable present a restatement and re-examination of ODIN's key exploitable results in alignment with the work introduced in the previous iteration of this deliverable. To this end, pertinent ethical principles and values are further specified, contextualized, and enriched with partner's views and ethical values in the context of ODIN.

Finally, expands on the work done in WP1 by providing an illustrative overview of a potential data governance models for post-project sustainability of the ODIN results and datasets (of particular relevance towards exploitation of the data for secondary research in the context of a regulatory-learning/living lab approach). Finally, it offers insights into the ethical procurement of datasets which are of relevance to various stakeholders involved in these activities. The sum of these activities enabled the definition of a set of simplified (self) assessment questionnaires and the submission of a new set of certification criteria to the European Centre for Certification and Privacy for its potential adoption as a certification scheme.

Statement of originality

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

Table of contents

TABLE OF CONTENTS	5
LIST OF TABLES	7
LIST OF FIGURES	8
1 INTRODUCTION	9
1.1 BACKGROUND	10
1.2 DELIVERABLE CONTEXT	10
2 METHODOLOGICAL APPROACH	12
3 SUMMARY RESTATEMENT OF KEY ODIN EXPLOITABLE RESULTS AND POTENTIAL EXPLOITATION	13
3.1 ODIN KEY EXPLOITABLE RESULTS OF RELEVANCE.....	13
4 NORMATIVE REFERENCES AND BEST PRACTICES FOR DATA PROCUREMENT	20
4.1 DEFINITION OF PUBLIC PROCUREMENT	20
4.2 NATIONAL AND INTERNATIONAL ETHICAL DISPOSITIONS ON DATA PROCUREMENT.....	21
4.2.1 <i>Transparency, accountability and access to information</i>	22
4.2.2 <i>Privacy and Data Protection</i>	24
4.2.3 <i>Fairness and non-discrimination</i>	25
4.2.4 <i>Public interest and social responsibility</i>	27
4.2.5 <i>Environmental responsibility</i>	28
4.2.6 <i>Other recurring ethical themes</i>	30
4.2.7 <i>New Commission’s Priorities</i>	31
4.3 EUROPEAN REGULATORY FRAMEWORKS	33
4.3.1 <i>European regulatory requirements on public procurement</i>	33
4.3.2 <i>General Data Protection Regulation (EU) 2016/679 (GDPR)</i>	39
4.3.3 <i>AI Act and standard EU model contractual clauses</i>	44
4.3.4 <i>European Health Data Space Regulation (EHDS)</i>	50
4.3.5 <i>Data Governance Act (DGA)</i>	56
4.3.6 <i>Medical Devices Regulation (MDR)</i>	59
4.3.7 <i>Other relevant frameworks</i>	63
5 ETHICAL PRINCIPLE ANALYSIS IN THE ODIN PROJECT	65
5.1 ETHICAL PRINCIPLE RESTATEMENT.....	65
5.2 PARTNERS’ VIEWS ON ETHICAL VALUES AND PRINCIPLES WITHIN ODIN.....	66
6 ETHICAL DATA PROCUREMENT: GUIDELINES AND RECOMMENDATIONS	75
6.1 SUMMARY OF ETHICAL OUTPUTS FOUND IN PREVIOUS ITERATIONS OF THIS DELIVERABLE	75
6.2 UPDATED ETHICS-RELATED CONCLUSIONS AND QUESTIONNAIRE INTRODUCTION	78
7 PATHWAYS AND GOVERNANCE BEYOND ODIN	81
7.1 ODIN GOVERNANCE AVENUES.....	81

7.2 ODIN AS AN ETHICALLY COMPLIANT ENABLER OF LIVING LABS AND REGULATORY LEARNING IN HEALTHCARE 86

8 CONCLUSIONS AND WAY FORWARD 88

9 REFERENCES 90

10 ANNEX 1: SIMPLIFIED QUESTIONNAIRE FOR PUBLIC HOSPITALS CONSIDERING PROCUREMENT OF (PERSONAL) DATA (FOR AI TRAINING)..... 93

11 ANNEX 2: HIGH-LEVEL VIABILITY ASSESSMENT QUESTIONNAIRE FOR ETHICAL PROCUREMENT OF AI/LLM SOLUTIONS BY PUBLIC HOSPITALS 98

12 ANNEX 3: HIGH-LEVEL SELF-ASSESSMENT QUESTIONNAIRE FOR PROVIDERS OFFERING AI/LLM SOLUTIONS TO PUBLIC HOSPITALS IN THE EU 108

List of tables

TABLE 1. DELIVERABLE CONTEXT	10
TABLE 2. D8.3 KEY EXPLOITABLE RESULTS TABLE	13
TABLE 3. EXPLOITATION OF KEY EXPLOITABLE RESULTS (KERS)	16
TABLE 4 EXPLOITATION MAPPING WITH REGULATORY FRAMEWORKS	18
TABLE 5. DISPOSITIONS ON TRANSPARENCY, ACCOUNTABILITY, AND ACCESS TO INFORMATION	22
TABLE 6. DISPOSITIONS ON PRIVACY AND DATA PROTECTION	24
TABLE 7. DISPOSITIONS ON FAIRNESS AND NON-DISCRIMINATION	25
TABLE 8. DISPOSITIONS ON PUBLIC INTEREST AND SOCIAL RESPONSIBILITY	27
TABLE 9. DISPOSITIONS ON ENVIRONMENTAL RESPONSIBILITY	28
TABLE 10. OTHER COUNTRIES AND PRINCIPLES IN PUBLIC PROCUREMENT	30
TABLE 11. EUROPEAN COMMISSION’S PRIORITIES ON PUBLIC PROCUREMENT	32
TABLE 12. REQUIREMENTS OF THE DIRECTIVE PER PROCUREMENT STAGE	33
TABLE 13 REQUIREMENTS FOR PUBLIC PROCUREMENT IN THE AI ACT	45
TABLE 14. REQUIREMENTS FOR PROCUREMENT IN THE EHDS	52
TABLE 15. REQUIREMENTS FOR PROCUREMENT IN THE DATA GOVERNANCE ACT	56
TABLE 16. REQUIREMENTS FOR PROCUREMENT IN THE MDR	59
TABLE 17. OVERVIEW OF OTHER RELEVANT FRAMEWORKS	63
TABLE 18 ETHICAL PRINCIPLE RESTATEMENT	65
TABLE 19. PARTNERS’ VIEWS ON ODIN SOLUTIONS’ ACCESSIBILITY MEASURES.....	67
TABLE 20. PARTNERS’ VIEWS ON ODIN SOLUTIONS PROMOTING PATIENT, HEALTHCARE PROVIDERS’ AND HOSPITAL AUTONOMY.....	69
TABLE 21. ODIN DATA GOVERNANCE MODEL NEEDS AND RECOMMENDATIONS.....	82

List of Figures

FIGURE 1. PROCESS OF PUBLIC PROCUREMENT (FROM	21
FIGURE 2 FLOWCHART OF DIRECTIVE 2014/24/EU	36
FIGURE 3. PPDS LAYERS (SOURCE: EUROPEAN COMMISSION’S COMMUNICATION, 2023/C98 I/01)..	38
FIGURE 4. GDPR GENERAL FLOWCHART	40
FIGURE 5. GDPR FLOWCHART: REQUIREMENTS FOR PROCESSING SENSITIVE DATA.....	42
FIGURE 6 ADDITIONAL STEPS FOR HIGH-RISK DATA PROCESSING	43
FIGURE 7. DECISION TREE AI ACT (1).....	47
FIGURE 8. DECISION TREE AI ACT (2).....	48
FIGURE 9. EHDS DECISION TREE	54
FIGURE 10. DGA DECISION TREE (2)	57
FIGURE 11. MDR DECISION TREE	61
FIGURE 12. PARTNERS’ VIEWS ON ODIN BENEFITS AND HARMS.	68
FIGURE 13. PARTNERS’ VIEWS ON VULNERABLE POPULATIONS AFFECTED BY ODIN SOLUTIONS.....	69
FIGURE 14. PARTNERS’ VIEWS ON STAKEHOLDERS’ DECISION-MAKING AUTHORITY.....	69
FIGURE 15. PARTNERS’ VIEWS ON ODIN PRIVACY AND CYBERSECURITY RISKS.	70
FIGURE 16. PARTNERS’ VIEWS ON PRIVACY AND CYBERSECURITY BENEFITS OF ODIN.....	71
FIGURE 17. PARTNERS’ RESPONSES ON ODIN TRANSPARENCY ACTIVITIES.	71
FIGURE 18. PARTNERS’ FOCUS TO IMPROVE TRANSPARENCY.....	72
FIGURE 19. PARTNERS’ VIEWS ON ODIN SAFEGUARD MECHANISMS.	73
FIGURE 20. PARTNERS’ DEFINITION OF TRUSTWORTHINESS IN THE CONTEXT OF ODIN.	74
FIGURE 21. ODIN’S DATA ETHICS AND PROCUREMENT FRAMEWORK INTERPLAY -VENN DIAGRAM	76
FIGURE 22. CARE PRINCIPLES.....	77
FIGURE 23. HOW TO EMBED DATA ETHICS REQUIREMENTS PER PUBLIC PROCUREMENT STAGE (SWIMLANE DIAGRAM)	78
FIGURE 24. ODIN DATA GOVERNANCE FRAMEWORK PRINCIPLES.....	82
FIGURE 25. DATA GOVERNANCE MODEL VISUALISATION	85

1 Introduction

Harnessing the power of data has been at the forefront of the European Union's (EU) strategies and policies, as data is considered a founding pillar of innovation (European Commission, "A European Strategy for Data", 2020). Public authorities in the EU are both major producers and users of data in various sectors, frequently having to procure it from external sources. The European Commission has actually estimated that over 250.000 public EU authorities are spending around 14% of GDP (around €2 trillion per year) on the purchase of services, works and supplies (European Commission's Communication, 2023/C98 I/01).

That being said, it has been estimated that a mere 20% of all call-for-tenders is made available for analysis in one place, while the remaining 80 % is spread, in different formats, regions and subject to different procedures. As a result, it becomes highly demanding or even impossible to re-use data to develop or improve policy, transparency and the overall public authorities' procedures (European Commission's Communication, 2023/C98 I/01).

In the health sector, this problem is further highlighted, with multiple authorities and organisations all over the world, including the Commission, already adopting ad hoc legislation and guidelines to promote the secondary use of data, i.e. the use of data for purposes other than those for which it was originally collected. Given the sensitive character of both the data related to health and relevant infrastructures, ensuring the compliance of these initiatives with legal and ethical standards is of utmost importance, yet there remains no formal public procurement process including ethics established.

Based on the project's overall goal to define a dynamic foundation for smart hospital ecosystems, previous work performed by this ODIN WP has aimed at the establishment of a concrete set of guidelines based on the existing and upcoming regulatory and normative framework, to promote an ethical data procurement process within and beyond the project. As such, this deliverable constitutes the final version of Deliverable 8.4, providing the necessary updates to the ODIN ethics framework and practical perspectives on ethical data procurement, with a particular focus on the ODIN project results.

Building upon the findings of its previous versions, it provides an overview of relevant procurement processes and elaborates upon applicable normative references to identify current and upcoming trends and best practices associated with the emerging regulations. To further facilitate their understanding while easing the identification of relevant sections for the project's exploitable results, the main dispositions of relevant regulations are presented in the form of decision trees.

After a brief summary of ODIN's key exploitable results (section 4), established ethical procurement processes are considered in section 5 of this deliverable. This includes an examination of ethical values and principles that are entwined in the ODIN project, for which the partner's views (as detailed through a dedicated survey) are presented. This section leads to a series of recommendations and guidelines on ethical data procurement (section 6).

Section 7 re-examines the project's expected outcomes in the light of the previous sections, particularly considering how ethical data procurement practices are of relevance to secondary use of research data (including the potential secondary use of the data generated by ODIN), for which a connection is made between the project and recent developments in regulatory learning exercises and living labs. This section then presents a proposal for post-project data governance structures which could ease this process while fostering the credibility, compliance and reusability of such data.

Section 8 revisits the mitigation measures presented by the previous iteration of this deliverable to detail a set of recommendations (ways forward) to ensure ethics compliance in public

procurement in public hospitals. Thus, in addition to recommendations in regard to the correct way of sourcing datasets and obtaining consent, this section also highlights the importance of certification and standardisation for these activities. Finally, the annexes of this document present a practical set of questionnaires which will enable better communication between relevant stakeholders, documentation generation, and viability evaluation vis-à-vis data and solution procurement in public hospitals.

1.1 Background

ODIN has been aiming at the development of a safe, open, and decentralised platform that facilitates the integration of robotics, artificial intelligence, and Internet of Things environments with the hospital's data and infrastructure. In this context, ODIN has been focusing on the creation of a cooperative co-creation mechanism for the Innovation Procurement Journey that takes into account healthcare providers and suppliers, in a way that complies with national and European legal frameworks. In doing so, a federated multi-centre longitudinal cohort study was conducted to evaluate the impact, scalability, interoperability, and innovation potential of the ODIN Key Enabling Results and platform.

Previous iterations of this deliverable presented the overall ODIN approach and sought to provide an evaluation of existing and foreseen ethical implications of procuring data and AI solutions, which is an increasingly complex task given the EU's evolving legal environment. This deliverable provides the final iteration of this exercise, and builds on the relevant developments of all ODIN WPs (particularly WP1 and WP7) to connect the perspectives found in its predecessors with more practical recommendations, which can be transferred to the project's exploitation task for their consideration. To ensure its value to the general public, this deliverable aims to clarify the relationship between data ethics and the procurement demands of public hospitals.

1.2 Deliverable context

Table 1. Deliverable context

PROJECT ITEM IN THE DOA	RELATIONSHIP
Project Objectives	This deliverable contributes to meeting O2: Build a dynamic and collaborative co-creation mechanism for an Innovative Procurement Journey to guarantee the delivery and scale-up of innovative services that are accepted, safe, trusted and compliant with current standards and rules.
Exploitable results	This deliverable contributes to developing best practices and enablers regarding data ethics in public procurement, that would be utilised in the IPJ ODIN proposes, both within and beyond the project, including certain exploitable tools and solutions.
Workplan	This deliverable presents the final outputs of WP8, task 8.4, towards the identification and clarification of ethical and legal issues surrounding the project and its objectives. It also provides recommendations to ensure the ethically and legally compliant data procurement in hospitals beyond the project's duration.

Milestones	Dependency on Milestone 2 completion (Dependency met).
Deliverables	This deliverable focuses on data ethics, particularly during the procurement of data for research purposes by hospitals. It is connected with the work showcased in D8.2 and D2.5, as data ethics supports the development of privacy by design and privacy-enhancing products and infrastructures. Its outcomes are of relevance to the deliverables in WP9 regarding exploitation.

2 Methodological Approach

This deliverable expands on the content of its previous iterations by performing an updated review of the: a) legal frameworks, guidance, and associated documentation; b) academic literature, articles, and books; c) grey literature, such as reports or whitepapers; and d) recent deliverables generated by the ODIN consortium following the completion of Milestone 2, to identify:

- Relevant background information on the ODIN project (general information and clarification on the project's pilots, reference use cases, framework, key stakeholders and key solutions);
- Ethical principles and value analysis in the ODIN project;
- Impact identification and mitigation measures update;
- Normative references and best practices for ethical data procurement.

This document provides an update to the set of guidelines and recommendations that address ethical data procurement for public hospitals initially proposed in D8.4, and D8.4r1, which are complemented by multiple enhancements in the data provided (including decision trees for each regulation) and practical recommendations for data governance, amongst other elements.

The ODIN ethical framework already established is further tested and validated through a survey carried out amongst project partners towards the definition of priority considerations when addressing ethical requirements towards exploitation and sustainability of the project's KERs.









By undertaking an integrated ethical evaluation of the ODIN project in line with the examination of the requirements and best practices for data procurement, this deliverable seeks to identify potential barriers and potential enablers for the wider adoption of ODIN-related solutions, while considering the frameworks surrounding ethical compliance for planning, sourcing, deploying, training, and utilising data-intensive data applications.



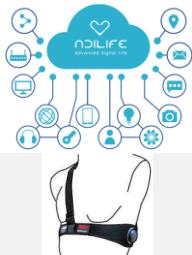




3 Summary Restatement of key Odin exploitable results and potential exploitation

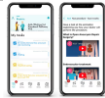



3.1 ODIN Key Exploitable Results of relevance

The KERs for the project were established already at the proposal stage, which then served as the baseline for the updates and the relevant work carried out in WP2 (particularly in T2.3 and D2.3) and WP9. KERs have been presented in Table 11 of D8.3, which is restated below to identify relevant regulatory and ethical dispositions in the context of the ODIN project, particularly towards the simplification of sustainability actions in the future.

Table 2. D8.3 Key exploitable results table

KERS	PROVIDER	DEVICE TYPE	CERTIFICATION & Status	IMAGE
PLATFORM and its components				
 ODIN Platform and its components	ODIN consortium	Platform, and its components and services	Described in detail on D3.12. Not recommended to follow MDR.	
ROBOTIC KERS				
 HOSBOT Robot	SSSA	Logistics support	<ul style="list-style-type: none"> • First version ready and under real environment testing. Robot used in the MUL Pilot. 	
 Robot TIAGo	PAL Robotics SL	Service and social robot	<ul style="list-style-type: none"> • First version ready and under real environment testing. <ul style="list-style-type: none"> • IEC/EN 60204-1 • The external power supply has the CE Marking and complies with the following European Directives and International Standards: <ul style="list-style-type: none"> ○ Electro-Magnetic Compatibility (EMC) Directive 2014/30/EU ○ EN 62368-1:2014 ○ IEC 60950-1:2005 • The internal batteries of the robot are certified by Eurofins according to IEC 62133 	
 Robot CETHBOT	CERTH	Social robot	<ul style="list-style-type: none"> • Validated in lab with more than 50 users. First version ready and under real environment testing. Used in Charité Pilot. 	
Robot Gateway	ODIN	Communication	<ul style="list-style-type: none"> • MQTT connectors ready and fully tested in the first two pilot performed by CETHBOT at Charité and HOSBOT at MUL 	-

RAMCIP	CERTH	Service robot	<ul style="list-style-type: none"> Validated in lab and in real homes with more than 50 users. 	
Mosaico FREKI	Mosaico Monitoraggio Integrato s.r.l.	Service robot	<ul style="list-style-type: none"> Not identified 	
Internet of Things (IoT)				
RTLS Devices	ODIN	Position control	<ul style="list-style-type: none"> The RTLS is developed. Final version of the RTLS connector is provided. 	-
Transparent Robot	SSSA	Environmental monitoring	<ul style="list-style-type: none"> Version Ready working with HOSBOT and TIAGo in testing environment. 	-
Proximity Sensor	SSSA	Position control	<ul style="list-style-type: none"> Version Ready working with HOSBOT and RB-1 in testing environment. 	-
IoT Gateway	ODIN	Integration	<ul style="list-style-type: none"> Mosquito is already deployed and all the robots and some AI use MQTT as a bridge to connect with ODIN. 	-
ADiLife telemedicine platform and BioHarness 3	ADiLife S.r.l	Monitoring system for vital parameters	<ul style="list-style-type: none"> CE Marked 93/42 Class I and MDR745 Class II pending 	
AI METHODS and its datasets				
Sleep disorder management	PEN	Detecting sleep disorders	<ul style="list-style-type: none"> AI-models trained and available as a KER to other ODIN KERs 	-
Automated patient inclusion system in the UCC	UMCU and PEN	Patient inclusion automatization	<ul style="list-style-type: none"> Patient data acquisition in ongoing to train the AI-based system 	-
 Early identification of patients at risk of malnutrition	FORTH	Energy intake	<ul style="list-style-type: none"> All subsystems are developed, and they need to be re-trained 	-
 Rehabilitation monitoring to prevent loss of mobility	FORTH	Rehabilitation	<ul style="list-style-type: none"> AI-models developed and set of exercises deployed. Working on the integration. 	-
 Oxygen monitoring therapy to prevent hypoxia	FORTH	Oxygen monitoring	<ul style="list-style-type: none"> AI-models developed. Integration in process. 	-
 Consumables management	FORTH	Cardiology stents management	<ul style="list-style-type: none"> Integration ready 	-
APPS and SERVICES				

GetReady	Medtronic	patient connecting solutions	<ul style="list-style-type: none"> • CE Mark. Security and full GDPR compliance. HIS integrated. 	
Forward	Medtronic	Platform for advanced management of surgical block processes	<ul style="list-style-type: none"> • Deployed and tested in several hospitals in Spain. 	
ORVital	MYSYPHER A	Optimizing surgical areas and ATLAS for traceability of infections.	<ul style="list-style-type: none"> • Commercial solutions deployed in more than 40 hospitals in Spain. 	
Luscii app	UMCU	Blood pressure measurement	<ul style="list-style-type: none"> • CE-certified as a Medical Device class IIa under the Medical Device Directives 	

As evident in the figure above, the platform and its relevant components are identified as the most prominent exploitable result of the project, as it is intended to function as a dynamic and adaptable "operating system" for smart hospitals, expertly integrating the rest of the KERs with the Hospital Information System (HIS).

The healthcare robotic solutions that have been developed throughout the project's lifetime and integrated into the ODIN ecosystem are also major exploitable results of ODIN, utilising the potential of AI to promote innovation in hospitals and facilitate relevant procedures. Said robotic solutions include the following:

- **HOSBOT** (acronym for HOSPital roBOT): This is an innovative, flexible and modular system architecture for autonomous mobile robots, designed for enhancing an optimised logistics into the hospitals. HoSBOT as a transportation technology provides value in the form of modularity and adaptability for smart hospitals.
- **CERTHbot**: a solution which includes several human-robot interaction (HRI) tools, which allow it to fulfil tasks directly linked to the welfare of patients. As such, it can provide emergency assistance, help patients with daily tasks, and interact with them on a personal level, leading to individualized assistance that improves patients' overall welfare.
- **TIAGo**: a service robot for clinical support and patient care aid possessing autonomous navigation capabilities, multimodal interfaces for patients' monitoring (wearable and environmental sensors), AI for smart assessment and assistive controller to physically support users as needed.

The above are supported by the several AI-based systems that have been developed throughout ODIN's runtime. Each of those systems has been developed through the use of state-of-the-art machine learning and deep learning algorithms, to perform a wide range of tasks, namely:

- **Calculation of the patients' energy intake**: In order to detect malnutrition early in patients, an AI-based system calculates the patients' energy intake and macronutrient consumption at the main meal of the day (lunch).
- **Rehabilitation monitoring to prevent loss of mobility**: In order to maximize the efficiency of physiotherapy treatment after major injuries, the patient is monitored while executing

several exercises with the RGB-d camera of the TIAGo robot and information regarding the number of repetitions and the correct execution of the exercises is provided.

- **Oxygen monitoring therapy to prevent hypoxia:** In order to enhance patients’ (correct) compliance with prescribed oxygen therapy and to reduce spending hospital resources on ensuring compliance with this, AI capabilities are introduced that are able to monitor patients during the assigned oxygen therapy and reduce the time of nurses dedicated to monitoring.
- **Consumables (cardiac stent) management:** The goal of this system is focussed on hospital consumable management and their future procurement, moreover, the prediction of a single consumable related to the Cardiology service: the stent device.

In addition to the above, ODIN has envisioned the establishment of a Historic Database Repository, hosted by each of the hospitals involved. The inclusion of this component on the ODIN platform enables the opportunity to turn data (historic data in particular) as new exploitable resources, which may enable the extraction of knowledge and to promote its analysis, fostering research and innovation.

Current efforts to ensure continuity of the ODIN research activities after the project’s finalization require the clarification of expected exploitation pathways in alignment with WP9 and the definition of appropriate governance (and data governance) models for post-project activities. This deliverable will seek to support these efforts by considering some of the ethical and practical issues associated with the exploitation and market-readiness process.

As detailed in D9.9, multiple business models are under consideration for the KERs, depending on their nature and organisational requirements (Perez and Guillen, 2024). In this regard, hospitals have the chance to decide on the type of contract for the KERs. For example, the ODIN platform can be offered in the form of support and service, freemium or dual licensing, partnership and integration, etc. Assistive robots can be bought in the classic option of product sales, subscription services, rental or leasing, etc. Finally, common business models for AI are software as a service, AI-enabled products or data monetisation. Some of them, such as AI in wearables, can be offered directly to the consumer or through healthcare providers. This means that the supplier should ensure that the wearable is easy to operate and comes with instructions not only for professionals to understand, but also for end-users. The identified KERs, their description, as well as their exploitation plan reported can be presented in the table below.

Table 3. Exploitation of Key Exploitable Results (KERs)

KER	Description	Exploitation
ODIN platform and components	The platform serves as a flexible operating system for smart hospitals through the integration of other KERs such as robotics, IoT, and AI within the HIS. The platform eases the work with the rest of the KERs, allowing for their development and customised use in hospitals. The KERs are to be treated as individual and separate pieces that are innovative or contributing to	Within the hospital, the platform makes it possible to develop and control logistics activities using specialized robots. Thus, in terms of procurement, ODIN platform secures traceability. Moreover, a unified data model serves as a basis for the development of AI models. The project has engaged since the beginning also with different

	the work of the hospitals. The platform also ensures the privacy, security, and trust of the KERs across the communication channels of the platform to respond to their dynamic developments.	stakeholders to ease the entrance into the market and the procurement of the KERs.
HOSpital roBOT (HOSBOT)	A self-governing mobile robot system intended to improve hospital logistical efficiency by fusing entirely automated and manual operations. It consists of an autonomous mobile robot (AMR) and a SmartRack which can carry different things.	In terms of procurement, the robots meet the requirements for security, efficiency, and traceability due to integration of RFID technology.
CERTHbot	An intelligence service robot which can contribute to the assistance of patients with daily tasks, monitor their well-being as well as improve surveillance.	This KER will make use of licensing schemes to grant software algorithm licenses to different robotics and AI firms so they can integrate the cutting-edge features into their own systems.
Service robot for clinical support and patient care aid	The UCBM robotic platform consists of a mobile robot (TIAGo, PAL Robotics) that can navigate on its own, multimodal interfaces for patient monitoring (wearable and environmental sensors), artificial intelligence (AI) for intelligent evaluation, and an assistive controller that can provide users with physical assistance when needed.	The robot uses AI algorithms to assess the well-being of the patients and help them with food, oxygen, or exercises. It will be presented as versatile customisable platform and it will be directly sold to healthcare facilities like the rest of the KERs.
AI based system for clinical application	A software-based AI system is created for each use case. Modern machine learning and deep learning algorithms are created to do this. Along with publicly accessible databases and datasets generated by the FORTH team specifically for the ODIN project, data from the pilots is also utilized.	The AI systems are designed for the purpose of future procurement and hospital management.

For procurement and data protection purposes, it must be noted that datasets also are considered KERs- data of information on the structure, including floorplans, databases of equipment, personnel details, and technical documents pertaining to hospital operations (Kalamaras, Lolis and Flevarakis, 2024). As such, the datasets developed and collected within the project are deemed essential to the ODIN sustainability action plan. Management and governance of such datasets in an ethical and regulatory compliant manner is of high relevance to the potential secondary use of this data, and for the potential adoption of these solutions by the market (due to increasing ethical considerations integration with procurement processes). In particular, datasets of patients are stored in the Hospital Information System (HIS) of each partner in possession of the data. This means that when data is collected, it needs to be sufficiently protected, especially when it will be processed for the purposes of training AI models as is the case with many of the above-analysed KERs. Given the nature of the data collected, the majority of the datasets within ODIN are subject to strict protection requirements and, on many occasions, cannot easily leave the partners’ premises.

Taking the above into consideration, it is of utmost importance to the success of the project, that data protection and ethics guidelines are respected in light of public procurement activities. This deliverable will describe in following sections how the secondary use of health data can be realised taking into account, for example, the implications of the European Health Data Space regulation, in light of research projects such as ODIN.

Finally, when considering the specific stakeholder perspectives on exploitation noted in D9.9, it is possible to generate a high-level mapping with the regulatory frameworks which will be introduced in the following section:

Table 4 Exploitation mapping with regulatory frameworks

Stakeholder	High-Level Exploitation Strategy	Relevant Regulatory Dispositions
Industrial Partners	<ul style="list-style-type: none"> - Provide technological backbone through robotics, IoT, and AI innovation. - SSSA focuses on robotic system integration, IP management, and creating spin-offs. - Medtronic IHS explores remote monitoring solutions for perioperative and chronic conditions. - Mysphera aims to enhance its RTLS with robotics and AI for hospital optimization. - Inetum plans global commercialization via expertise gained. 	<ul style="list-style-type: none"> - Medical Devices Regulation (MDR): For the development and use of medical devices. - AI Act: Compliance with AI system deployment in healthcare. - GDPR: Ensure data protection in IoT and AI systems. - Data Governance Act: For secure data sharing and reuse.
Healthcare Providers	<ul style="list-style-type: none"> - Serve as primary users and sources of real-world feedback. - Inform refinements to ensure platform meets dynamic healthcare needs. 	<ul style="list-style-type: none"> - GDPR: Ensure patient data protection. - European Health Data Space Regulation: For the secure sharing of health data.

	<ul style="list-style-type: none"> - Key participants include SERMAS, UMCU, UCBM, SAS, CUB, and MUL. 	<ul style="list-style-type: none"> - EU Public Procurement Requirements: Compliance in procuring ODIN-related technologies.
Academia and Research	<ul style="list-style-type: none"> - Contribute through development of advanced algorithms and methodologies. - Advance foundational science supporting platform capabilities. - Key entities: UPM, CERTH, UCBM, FORTH. 	<ul style="list-style-type: none"> - GDPR: Ensure research data complies with privacy standards. - AI Act: Adherence in developing AI methodologies. - Data Governance Act: For safe and compliant data handling.
Regulatory Bodies	<ul style="list-style-type: none"> - Ensure compliance with healthcare regulations and standards. - UDG Alliance focuses on data protection and certification services. - Offer consulting services to healthcare companies for compliance and foster innovative market services. 	<ul style="list-style-type: none"> - GDPR: Data protection and privacy (certification) - AI Act: Oversight on AI systems and certification activities - European Health Data Space Regulation: Certification of platforms handling health data. - Data Governance Act: Enable secure governance frameworks.
End-Users	<ul style="list-style-type: none"> - Direct beneficiaries (patients and healthcare staff). - Provide feedback and engagement to tailor the platform to real-world needs effectively. 	<ul style="list-style-type: none"> - GDPR: Ensure privacy and data protection for patients. - European Health Data Space Regulation: For access and control of personal health data.
Technology Integrators	<ul style="list-style-type: none"> - Integrate disparate systems for seamless operation within healthcare facilities. - Ensure ODIN platform compatibility with existing technological infrastructures. 	<ul style="list-style-type: none"> - GDPR: Data protection in system integration. - AI Act: Compliance for AI-based integration. - Data Governance Act: Facilitate legal data exchange. - European Health Data Space Regulation: Interoperability in health data systems.
Funding Bodies/Investors	<ul style="list-style-type: none"> - Provide financial support for development and expansion. - Enable platform growth to meet emerging challenges and opportunities. 	<ul style="list-style-type: none"> - EU Public Procurement Requirements: Funding compliance. - GDPR: Ensure funding supports privacy-compliant initiatives. - AI Act: Compliance for funding AI-based projects.

The results of this deliverable have been communicated to WP9 partners and have been considered when performing exploitation and project sustainability planning. The project’s final deliverable on the ODIN Legacy pathways will further advance the perspectives shared in this document towards the materialization of the project’s potential.

4 Normative References and Best Practices for Data Procurement

4.1 Definition of Public Procurement

The term "public procurement" describes the method used by government agencies, local governments, and other public bodies to acquire goods, services, or labour from businesses (*Public procurement - European Commission*, no date).

The traditional form of public procurement is competitive tendering (*Public tendering rules in the EU*, no date). It consists of several techniques:

- Open procedure: The primary method of tendering, which gives every organisation an equal chance to submit a bid and enables anyone to submit one in order to provide the goods or services needed. The primary prerequisites include being accessible to all qualified bids, being publicised, having precise technical specifications, and having precise assessment standards (Events, 2019).
- Restricted procedure: It is similar to the open procedure in the sense that anyone can apply to participate. However, there is a process of pre-selection before the submission of the complete tender.
- Competitive negotiated procedure: Pre-qualification and negotiation phases are included (however contracting authorities may choose to award a contract without negotiation if they have reserved the right to do so). The negotiation phase is held with the pre-qualified group of tenderers (Burrows, 2024).
- Competitive dialogue: this makes it possible to have a conversation in phases with the goal of lowering the number of bidders (Burrows, 2024).
- Innovation partnership: When a good or service that is still off the market needs to be purchased, this process could be employed. Several businesses might take part in the process at different points (*Public tendering rules in the EU*, no date).
- Design contest: This process is employed to generate a design concept (*Public tendering rules in the EU*, no date).

Below is an illustration of the procurement process in steps ('Special report on Public procurement in the EU: Less competition for contracts awarded for works, goods and services in the 10 years up to 2021', 2023):

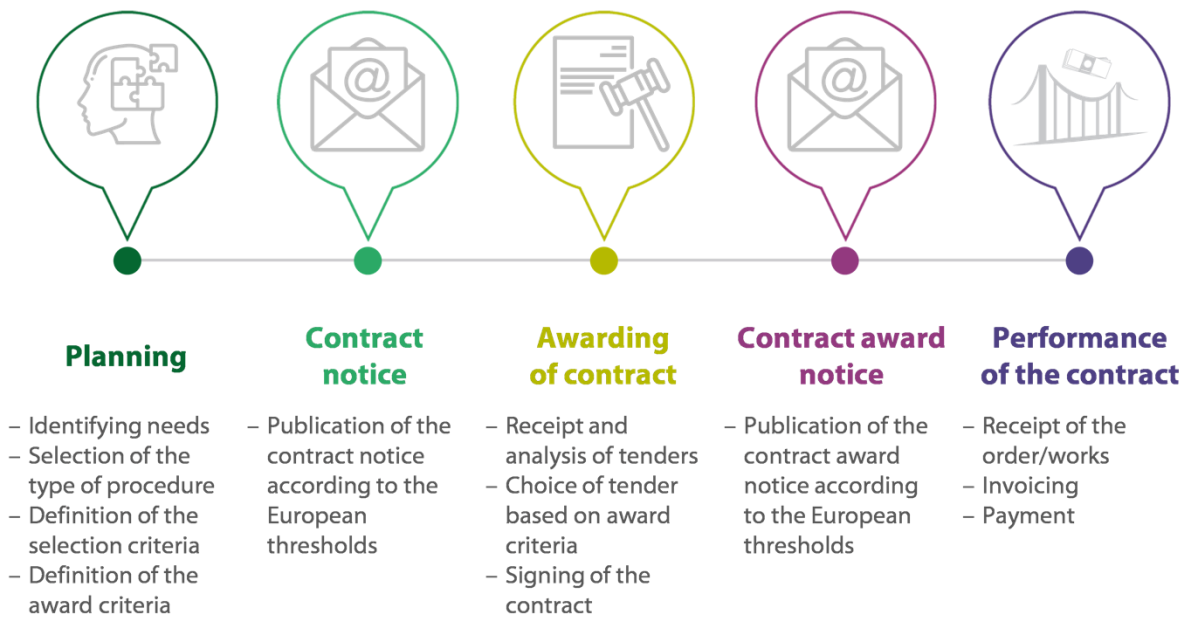


Figure 1. Process of public procurement (from

In Europe, the main instrument on public procurement is Directive 2014/24/EU whose provisions have been observed in more detail in section 3.3.1 (*Public procurement | EUR-Lex*, no date). The fundamental parts of the process under the Directive can be summarised as follows:

- Procurement rules should follow European legislation when the thresholds for sums for contracts (updated as of 01.01.2024) are exceeded.
- The process is decided on the basis of two criteria: (a) lowest price; and (b) best quality with regards to innovation, technical aspects, cost-effectiveness, with regards to social and environmental issues and European policies, conditions of delivery and trading.
- The contractors and the products must comply with European legislation for technical security, data protection, sustainability, efficiency, etc.

4.2 National and International Ethical Dispositions on Data Procurement

Taking the above into account, public procurement needs to consider and incorporate ethical aspects during all steps of the process. In the context of this deliverable, this means that hospitals seeking to procure data and/or solutions should only do so from sources that can ensure that their data is obtained and processed in an ethical manner¹. Moreover, ethical considerations have to be accounted for throughout the whole performance of the contract, including by the hospitals themselves as they implement the procured solutions, and through due diligence and vigilance

¹ This is particularly relevant when the data is procured in with the development, refinement or deployment of an AI system, or when the target for procurement is an AI model/system

on how procured or directly contributed data from their patients is used in connection with the procured systems.²

As was highlighted in the previous iterations of this deliverable, Member States have integrated the European Directives on Public Procurement into their national legislation in different manners. To ease assessment of the key outputs of this examination by ODIN WP9 in its pathway towards project legacy, the following section of this deliverable includes a summary of the recurring ethical principles present in the national legislation of the countries of the ODIN pilots, as well as the corresponding international dispositions.

4.2.1 Transparency, accountability and access to information

Several regulatory and/or administrative dispositions specify these values as important to data processing or procurement, the following table presents a non-exhaustive list of relevant frameworks:

Table 5. Dispositions on transparency, accountability, and access to information

Country	Source	Explanation
The Netherlands	Data Ethics Decision Aid (DEDA)	Citizens must be able to opt out effectively. Requirement to be open and honest with the public, and provide them the opportunity to voice any concerns about the project's outcomes.
Italy	National Action Plan on Ethical Public Procurement	Transparency as part of public procurement
Spain	Royal Legislative Decree 3/2011 of November 14 which provides the revised text of the Public Sector contracts related norms; and Law 31/2007, of October 30, on contracting procedures in the special sectors (water, energy, transports and postal services). Code of Principles for Public Procurement (Direccio General de	Transparency and access to information as fundamental principles of public procurement

² D8.3 on certification scheme strategy and ODIN's sustainability plan has already identified procurement of technology in healthcare as a key area for standardisation, as further discussed in later sections of this deliverable.

	Contractacio Publica, no date), Catalonia	
Germany	Federal Government’s Data Ethics Commission Opinion	Transparency and accountability to be ensured through appropriate documentation
Poland	Policy for AI Development in Poland’	Setting regulations to guarantee accountability, openness, and auditing when it comes to public administration’s use of algorithms (AI)
United Kingdom (UK)	Data Ethics Framework	All actions, procedures, and data under its scope are to be transparent. The public can easily access information about the project, its procedures, and its results in comprehensible language. Throughout the project, efficient supervision and governance procedures should be used to ensure accountability.
International Sources		
OECD	Good Practice Principles for Data Ethics in the Public Sector and Guidelines for Integrity in Public Procurement	Throughout the procurement process, maintain transparency to guarantee that all possible vendors receive the same treatment. Make sure exclusions in soliciting competitive bids are sufficiently disclosed. Accountability and control are important. Publishing source code and open data can facilitate citizen engagement and transparency. Hospitals should be ex-post and ex-ante accountable for risk management
World Economic Forum (WEF)	AI Procurement in a Box: AI Government Procurement Guidelines	Provide algorithmic accountability and transparency

World Health Organisation (WHO)	Ethics and governance of artificial intelligence for health (World Health Organisation, 2021; World Health Organization, 2024)	AI should be understandable to users and medical professionals; Before AI is designed or implemented, enough data is released or recorded. Human oversight serves as a guarantee to make sure AI systems carry out the duties they are given correctly and to provide accountability in the event of mistakes.
DataEthics.eu	White Paper on Data Ethics in Public Procurement of AI-based Services and Solutions	People should be given the knowledge and resources to comprehend and use AI-based services. Accountability impact assessments should be performed. Suppliers should be also accountable

4.2.2 Privacy and Data Protection

The following table presents the relevant dispositions on privacy and data protection examined from an ethical perspective, while the analysis of the normative framework will be presented in Section 4.3 below.

Table 6. Dispositions on privacy and data protection

Country	Source	Explanation
The Netherlands	Data Ethics Decision Aid (DEDA)	If personal data is utilised, it should comply with national regulations and the GDPR. a DPIA should also be performed and a DPO for the project designated. Data should be protected through anonymisation/ pseudonymisation/generalisation.
Italy	National Action Plan on Ethical Public Procurement	Data procurement should be protected in alignment with several data ethics principles specified in the action plan.
Germany	Federal Government’s Data Ethics Commission Opinion	Privacy and security are ethical principles for data. The data should be of high quality.

Poland	Policy for AI Development in Poland'	Open public data should comply with data protection laws
United Kingdom (UK)	Data Ethics Framework	Refers to data governance, which includes approving access to, storing, and assessing consent for, data, and data assessment. DPIA should be referenced. The quality of the data should be high.
International Sources		
OECD	Good Practice Principles for Data Ethics in the Public Sector and Guidelines for Integrity in Public Procurement	Open data should be protected according to privacy, ownership and security requirements.
World Economic Forum (WEF)	AI Procurement in a Box: AI Government Procurement Guidelines	Data protection and privacy laws should be accounted for when procuring AI.
World Health Organisation (WHO)	Ethics and governance of artificial intelligence for health (2024)	Conduct a transparent assessment of the ethics and data protection before choosing a technology.
DataEthics.eu	White Paper on Data Ethics in Public Procurement of AI-based Services and Solutions	Award standards evaluation based on the best price-to-quality ratio. The requirements for data ethics, privacy, the environment, etc., should be reflected in the quality criteria when procuring.

4.2.3 Fairness and non-discrimination

Fairness and non-discrimination are of particular relevance to procurement processes, while in the context of data and (AI) solution procurement, their bearing is increased due to intrinsic considerations surrounding their training, implementation and potential (mis)use by the various stakeholders in the procurement chain.

Table 7. Dispositions on Fairness and non-discrimination

Country	Source	Explanation
The Netherlands	Data Ethics Decision Aid (DEDA)	The possibility of prejudice should be examined and make sure all groups are fairly represented in the databases. Likelihood that

		the project/solution may encourage bad behaviour should be evaluated vis-à-vis a potential situation in which the project's outcomes might be abused for other goals, and consider long-term implications on society.
Italy	National Action Plan on Ethical Public Procurement	Principles of equal treatment and impartiality are recognized as part of public procurement
Spain	Code of Principles for Public Procurement (Direccio General de Contractacio Publica, no date), Catalonia	Public procurement should advance social responsibility.
Germany	Federal Government's Data Ethics Commission Opinion	If risk of potential discrimination when data is used in healthcare is identified, data processing beyond original purpose should be prohibited.
Poland	Policy for AI Development in Poland'	AI should be developed according to the fundamental rights in the EU charter including the right to not be discriminated.
United Kingdom (UK)	Data Ethics Framework	Employ an internal ethical AI approach and accountability in the model performance to avoid discrimination.
International Sources		
OECD	Good Practice Principles for Data Ethics in the Public Sector and Guidelines for Integrity in Public Procurement	Fairness and non-discrimination are part of the principle that hospitals should serve public good.
World Economic Forum (WEF)	AI Procurement in a Box: AI Government Procurement Guidelines	All of the chosen data must satisfy the fairness requirements. Recent data that is typical of the people the AI solution is intended to help is required. AI systems should not include bias.

World Health Organisation (WHO)	Ethics and governance of artificial intelligence for health (2024)	Inclusivity and equity are vital for the functioning of AI and biases should not be present.
DataEthics.eu	White Paper on Data Ethics in Public Procurement of AI-based Services and Solutions	When picking a supplier and AI, the AI should be chosen so that it does not allow for bias and so that all stakeholders are included throughout the design process of the algorithm. Social responsibility is also ensured through engagement of all stakeholders.

4.2.4 Public interest and social responsibility

Public interest and social responsibility are recognised as elements of consideration when planning for the procurement and/or deployment of new solutions.

Table 8. Dispositions on public interest and social responsibility

Country	Source	Explanation
The Netherlands	Data Ethics Decision Aid (DEDA)	Responsibility is a general consideration alongside data governance and legal compliance.
Italy	National Action Plan on Ethical Public Procurement	Publicity and integrity as part of public procurement and data ethics
Spain	Code of principles for public procurement (Direccio General de Contractacio Publica, no date), Catalonia	Public procurement should advance social responsibility.
Germany	Federal Government's Data Ethics Commission Opinion	Technology advancement, network impacts, and anticipated cumulative effects must all be considered when evaluating the possible implications of data processing. If data is reused, it should benefit the public
Poland	Policy for AI Development in Poland'	AI should be developed in a human-centric manner that

		considers the EU Charter fundamental rights
United Kingdom (UK)	Data Ethics Framework	No particular provision on social responsibility.
International Sources		
OECD	Good Practice Principles for Data Ethics in the Public Sector and Guidelines for Integrity in Public Procurement	Hospitals should be ex-post and ex-ante ethically and socially responsible for risk management.
World Economic Forum (WEF)	AI Procurement in a Box: AI Government Procurement Guidelines	No particular provision on social responsibility.
World Health Organisation (WHO)	Ethics and governance of artificial intelligence for health (2024)	Public interest and health should be promoted.
DataEthics.eu	White Paper on Data Ethics in Public Procurement of AI-based Services and Solutions	At the preliminary risk assessment stage of the procurement process, a risk assessment on social and environmental impact should be conducted.

4.2.5 Environmental responsibility

Environmental responsibility and sustainable practices are elements of relevance to the procurement process, particularly when addressing AI/big data processing activities, as they normally require significant processing infrastructure and corresponding increases in energy consumption³.

Table 9. Dispositions on environmental responsibility

Country	Source	Explanation
The Netherlands	Data Ethics Decision Aid (DEDA)	No particular provision on environmental responsibility.

³ These should be accounted for regardless of whether this increased energetic consumption takes place on-site in a hospital or in a data-server performing “cloud” based processing activities.

Italy	National Action Plan on Ethical Public Procurement	Environmental sustainability and energy efficiency as part of public procurement and data ethics
Spain	Code of principles for public procurement (Direccio General de Contractacio Publica, no date), Catalonia	Public procurement should advance sustainability and innovation.
Germany	Federal Government’s Data Ethics Commission Opinion	Environmental sustainability is a deciding factor for the awarding of contracts in public procurement.
Poland	Policy for AI Development in Poland’	No particular provision on environmental sustainability.
United Kingdom (UK)	Data Ethics Framework	No particular provision on environmental sustainability.
International Sources		
OECD	Good Practice Principles for Data Ethics in the Public Sector and Guidelines for Integrity in Public Procurement	Data ethics considerations include environmental sustainability. It is imperative to adopt strategies to mitigate carbon emissions and give priority to clean and renewable energy sources when it comes to data centres.
World Economic Forum (WEF)	AI Procurement in a Box: AI Government Procurement Guidelines	AI procurement should include the establishment of minimal specifications for the vendor's data hosting environment (security on business laptops handling sensitive data, for example) as a requirement.
World Health Organisation (WHO)	Ethics and governance of artificial intelligence for health (2024)	AI as a whole should be sustainable. AI systems need to take energy efficiency and the environment into account. Sustainability in the workplace is also important to consider because health care providers may require specialised training in order to use AI systems securely.

DataEthics.eu	White Paper on Data Ethics in Public Procurement of AI-based Services and Solutions	At the preliminary risk assessment stage of the procurement process, a risk assessment on social and environmental impact should be conducted.
---------------	---	--

4.2.6 Other recurring ethical themes

Aside from the above-mentioned ethical principles, the Belmont Report (1978) also includes beneficence, justice, and respect for persons, which have already been considered in other ODIN activities (in particular in D8.2)⁴. More information can be found in the previous version of this deliverable (D8.4 rev1).

The importance of ethics in the public procurement process has been emphasized by other jurisdictions around the globe as presented in the following table:

Table 10. Other countries and principles in public procurement

Country/Organisation	Source	Underlying principles
Hungary	Code of Ethics 2016 (Közbeszerzési Etikai Kódex)	Public procurement should follow the principles of legality (fairness, equity, and lawful use of rights), transparency (responsibility and efficiency) and non-discrimination (integrity).
Spain	Royal Legislative Decree 3/2011 and Law 31/2007	The procurement process should be conducted with equal treatment and without discrimination against candidates, with unrestricted access to tenders, publicity and transparency, and effective use of public funds.
Sweden	Public Procurement Act (Sw. lag 2016:1145 om offentlig upphandling), the Utilities Procurement Act (Sw. lag (2016:1146) om upphandling inom försörjningssektorerna), the Concessions	Equal treatment, non-discrimination, proportionality, transparency (openness and predictability), and mutual recognition (Ch. 12, S.9: <i>Communication and storage of data in a procurement matter shall be conducted</i>

⁴ Furthermore, these elements are also part of the ethical recommendations and guidelines for Horizon projects established by the European Commission.

	Procurement Act (Sw. lag (2016:1147) om koncessioner) and the Defense Procurement Act (Sw. lag (2011:1029) om upphandling på försvars- och säkerhetsområdet)	<i>in such a way that the data is not distorted)</i>
Australia	Public Governance, Performance and Accountability Act 2013 (Cth) ("PGPA Act"), in particular Commonwealth Procurement Rules ("CPRs")	Value for money is the primary principle. Public procurement should also follow practices for non-discrimination, accountability, efficiency, effectiveness, transparency, and other ethical principles. Related bidders should follow ethical guidelines so that there is no conflict of interests
Japan	The Accounting Act and the Cabinet Order on Budgets, the Settlement of Accounts, and Accounting	<p>Economic efficiency: To ensure the most cost-effective procurement, with a focus on the advantages for the taxpayers who fund the government and local government.</p> <p>Competitiveness: To create procedures to stop uncompetitive behaviour and to encourage competition through general competitive bidding, where discretionary contracts are the exception rather than the rule.</p> <p>Fairness: Adhering to all regulations required to preserve public confidence in proper accounting procedures and ensuring equal opportunities for rivals functioning as competing parties in public procurement.</p> <p>Transparency: Establishing mechanisms for information disclosure to encourage outside observation.</p>
UNCITRAL	UNCITRAL Model Law on Public Procurement 2014	The model law is based on the principles of accessibility, openness, competitiveness, integrity, fairness, transparency, and efficiency. These principles serve as guidelines to governments on how to modernise their procurement procedures.

4.2.7 New Commission's Priorities

a. In 2017 the European Commission published a new public procurement strategy (European Commission, 2017) with 6 clear priorities to improve procurement in practice. Inter alia this

includes ‘Transparency, integrity and better data’ and the ‘Digital transformation of public procurement’.

The table below provides an overview of the above priorities:

Table 11. European Commission’s priorities on public procurement

Increasing Transparency, Integrity And Better Data	Better and more accessible data should be made available in public procurement, while respecting the fundamental rights, and in particular, the right to protect personal data, to the extent applicable
	Electronic procurement systems must produce good-quality data
	The Commission would propose new e-forms to improve the collection of data. These forms have already been established under Regulation (EU) 2019/1780
	Setting up publicly accessible contract registers to provide transparency on awarded contracts
Boosting The Digital Transformation Of Procurement	New technologies enable to streamline and simplify the procurement process
	The whole public procurements process must embrace digital transformation from planning, notification, submission until invoicing and archiving.
	The Commission will further improve and promote standards (like eCertis) that enable digital transformation of procurement at national level and complementary tools like the Single Digital Gateway

b. Guidance on Innovation Procurement (European Commission, 2021)

Although not legally binding, the European Commission in 2021 published guidelines on innovation procurement (European Commission, 2021a). It focuses on ensuring that procurements award the best quality, cost-efficiency, and promotes solutions that value environmental and social benefits. Under its definition ‘innovation procurement’ is any procurement that either buyers the process of innovation or the outcomes of innovation (European Commission, 2021a, p.6). Although no direct reference to data ethics principles is found in this document, the guidance provides a dedicated section on the intellectual property protection of data, datasets and databases (European Commission, 2021a, p.70).

4.3 European Regulatory Frameworks

This section seeks to complement the previously identified dispositions, with a broader examination of applicable regulatory frameworks and a closer examination of the associated decision trees which may apply to relevant stakeholders when pursuing compliance with these requirements. This section seeks to enable a broader understanding of the commonalities surrounding ethical data procurement in public hospitals while supporting and contextualizing the Annexes of this deliverable.

4.3.1 European regulatory requirements on public procurement

The main regulatory framework on public procurement is set out under EU Directive 2014/24/EU (Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC Text with EEA relevance,) and EU Directive 2014/25/EU. However, the latter applies only to public procurement by entities operating in specific sectors (namely water, energy, transport, and postal services). Hence, regarding the healthcare sector and, in the context of the ODIN project, only the former Directive 2014/24/EU includes relevant specifications (hereafter ‘Directive’).

4.3.1.1 Directive 2014/24/EU

This Directive establishes rules on the procedures for procurement by contracting authorities concerning public contracts as well as design contests, whose value is estimated to be not less than the threshold amounts set out under Art 4 of the Directive, and while it established numerous requirements during all stages of public procurement, it is relevant to note that no specific reference to data ethics is included in its dispositions.

The following table provides an overview of some of these requirements and how each could be used to embed data ethics in the public procurement process:

Table 12. Requirements of the Directive per Procurement Stage

PROCUREMENT STAGE	REQUIREMENT	DESCRIPTION	RELATION WITH DATA ETHICS
Preparation	Preliminary market consultation – Art 40	Conduct market consultations, seek advice from independent experts and authorities but ensure that this does not distort competition.	Data ethics encourages market consultation, so distorting competition is a risk that should be addressed
	Technical specifications – Art 42	Depending on the service/work clear technical specifications must be met.	Detailed technical specifications on the expected data quality, security, accuracy and governance

			should be included
	Labels – Art 43	When works have environmental, social or other characteristics the award criteria might require specific labels as a means of proof.	Data labels (and regulatory compliance certifications) that ensure quality, compliance or other characteristics may be included
Choice of participants and award of contracts	Selection criteria and exclusion grounds- Arts 57 ⁵ and 58	Exclusion grounds must not exist for awarded candidates, who should also fulfil the selection criteria.	The exclusion and selection criteria can include data ethics requirements, especially under art 57(4)(a). For instance, exclusion of candidates who mishandle data.
	Quality assurance standards and environmental management standards	Contracting authorities shall refer to quality assurance standards, drawn up by independent bodies	Quality assurance standards for data ethics might be developed (they already exist for specific areas, such as personal data protection)

⁵ Health Care Without Harm (Health Care Without Harm, 2014) Europe explored the opportunities the new Directive will provide for a more sustainable public procurement in healthcare. Among others, it welcomed the self-cleaning option under art 57, where even companies that initially were excluded could potentially become eligible tenders if they can demonstrate that they have become a reliable counterparty. Especially if data ethics will be included in the exclusion criteria, this self-cleaning option could be highly beneficial in the long term so as not to hinder innovation and allow entities who have exploited data in the past to participate in the public procurement process as long as they can demonstrate that they now do not exploit data. In addition, under art 18(2) Member States shall ensure that successful tenderers comply with environmental, social and labour laws. Although this is left to the discretion of the Member States, fragments of data ethics principles could also be found via national laws that transpose this Directive.

	Contract award criteria	The most economically advantageous tender shall be identified on a best-price quality ratio which is assessed on criteria including qualitative environmental and social aspects.	On these criteria data ethics requirements could be introduced, particularly when assessing the quality of data avoiding bias (social aspect), environmental footprint of data storage etc.
	Life-cycle costing – Art 68	Life-cycle cost evaluation shall consider costs related to acquisition, maintenance and end-of-life costs.	The cost throughout the lifecycle of ethical data procurement should also be considered
Contract performance	Conditions for performance of contracts – Art 70	Contracting authorities may lay down special conditions related to the performance of a contract.	Clauses that ensure fundamental rights protection and sustainability could be included

The following figure presents a flowchart generated to illustrate the process of public procurement under Directive 2014/24/EU⁶, to assist in the assessment of overall compliance with this Directive and help identify best practices.

⁶ The flowchart in Figure 2 focuses particularly on the obligations of the contracting authorities and the economic operators. It is important to note that an organisation might have further obligations under this directive.

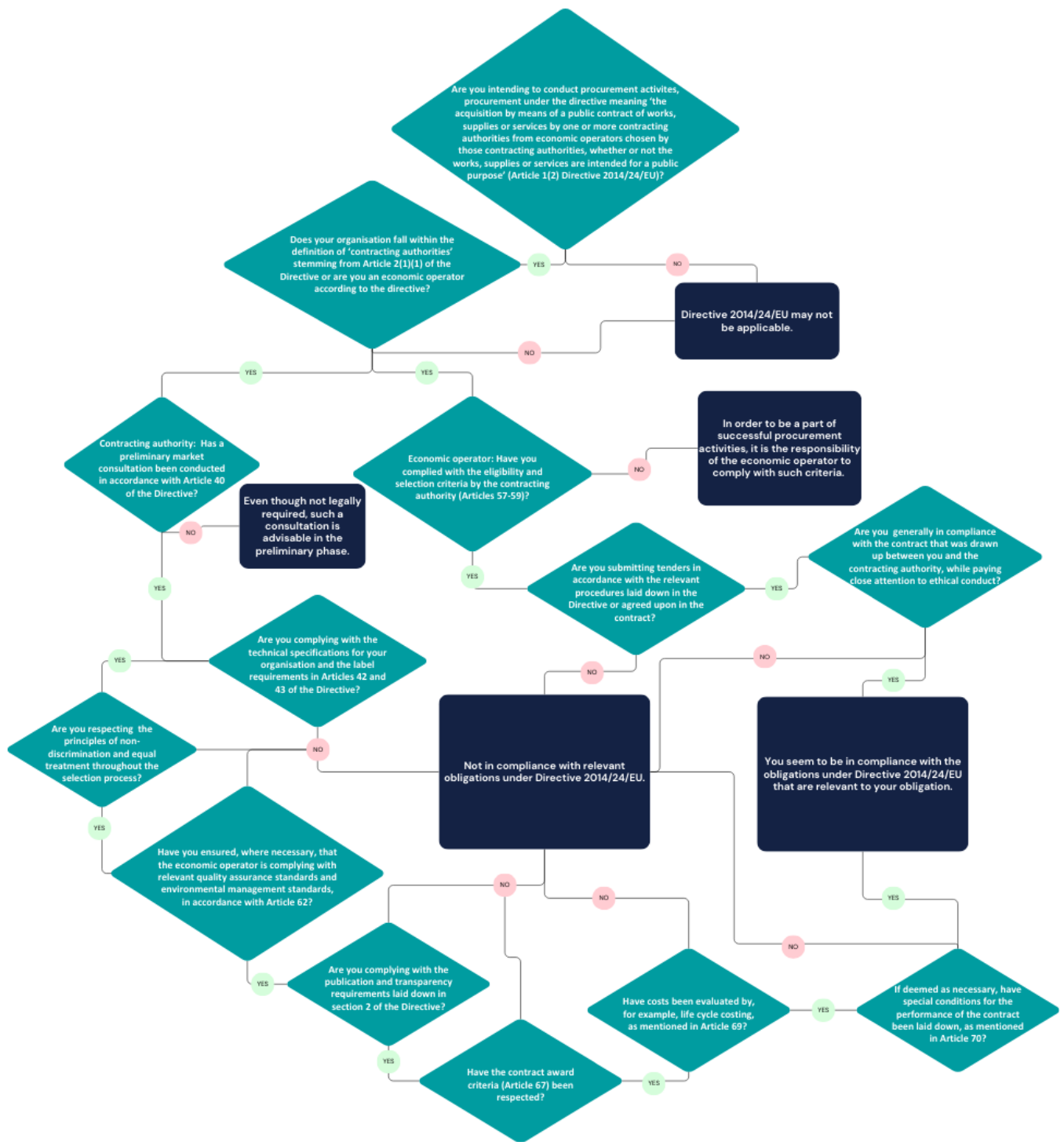


Figure 2 Flowchart of Directive 2014/24/EU

The flowchart above can be further explained through the following points:

1. The first action sought by the flowchart relates to the **determination by relevant stakeholders of whether the Directive is applicable to their respective situations**. In order to do so, the following points are taken into account:
 - a. Whether the organisation’s activities fall within the definition of ‘procurement’, according to Article 2(1) of the Directive.

- b. Whether the organisation itself falls under the Directive's definition of either 'contracting authority' or 'economic operator'.
- 2. The second stage of the flowchart eases the **assessment of compliance** for each respective organisation type.
 - a. In regard to **contracting authorities**, the following points of compliance are specifically considered:
 - i. Whether the contracting authority has conducted a preliminary market consultation, in accordance with Article 40 of the Directive.
 - ii. Whether the contracting authority is complying with the technical specifications relevant to its activities and the label requirements in Articles 42 and 43 of the Directive.
 - iii. Whether the contracting authority is respecting the principles of non-discrimination and equal treatment throughout the selection process.
 - iv. Whether the contracting authority has ensured, where necessary, that the economic operator is complying with relevant quality assurance standards and environmental management standards, in accordance with Article 62.
 - v. Whether the contracting authority is complying with the publication and transparency requirements laid down in section 2 of the Directive.
 - vi. Whether the contracting authority is respecting the contract award criteria, laid down in Article 67 of the Directive.
 - vii. Whether the contracting authority has evaluated costs by, for example, life cycle costing, as mentioned in Article 69 of the Directive.
 - viii. Whether, if deemed as necessary, special conditions for the performance of the contract have been laid down, as mentioned in Article 70 of the Directive.
 - b. In regard to **economic operators**, the assessment of compliance considers in particular the following points:
 - i. Whether the economic operator has complied with the eligibility and selection criteria by the contracting authority (see Articles 57-59 of the Directive).
 - ii. Whether the economic operator is submitting tenders in accordance with the relevant procedures laid down in the Directive or agreed upon in the contract.
 - iii. Whether the economic operator is generally in compliance with the contract that was drawn up with the contracting authority, while paying close attention to ethical conduct.

Overall, this flowchart can point actors, namely contracting authorities and economic operators, bound under Directive 2014/24/EU towards the path of compliance, and in this light, ease the work of ODIN stakeholders and partners towards upcoming exploitation activities.

4.3.1.2 Public Procurement Data Space

In addition to the above, the European Commission has been working on the establishment of a Public Procurement Data Space (PPDS), meant to create a platform at the EU level to access in a concentrated manner public procurement data that are now dispersed at EU, national and regional level (European Commission's Communication, 2023/C98 I/01). The PPDS is meant to be launched by 2025 and will be consisting of four layers:

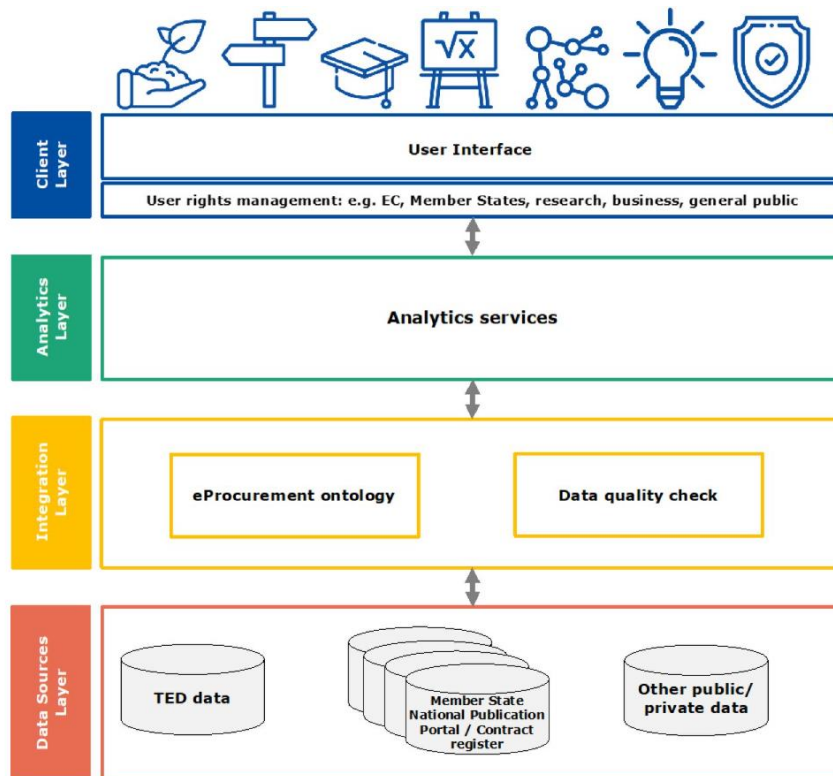


Figure 3. PPDS layers (Source: European Commission’s Communication, 2023/C98 I/01)

In particular, the above-depicted layers will include the following information:

- **Data Source Layer:** The platform will collect heterogeneous data from the TED portal, the Member States’ public procurement portals and other public and private databases.
- **Integration Layer:** It will collect the above data sources and translate them into a common, machine-readable data format. During this process, the data quality will be further validated through a data quality dashboard.
- **Analytics Layer:** Integrating AI, Machine Learning and Natural Language Processing, it will allow Member States to establish their own analytics layers.
- **Client Layer/User Interface:** The platform will give end users (including public authorities, businesses, citizens, NGOs, researchers etc) access to the data in the integration layer and/or derived insights in the analytics layer.

The primary goals behind the establishment of the PPDS lie precisely in the improvement of data quality and the automation of data flows in a manner that promotes the re-use of data to improve operations, promote innovation and manage crises, such as the COVID-10 pandemic in a more efficient manner.

This development is of extremely high relevance for EU research projects like ODIN in their pathways towards sustainability, as it is expected to present an aggregated hub for understanding ethical procurement requirements and overall procurement trends, which will in turn enable the development of tailored solutions by relevant parties to match specific and emerging market needs.

4.3.2 General Data Protection Regulation (EU) 2016/679 (GDPR)

As specified in the previous iteration of this Deliverable, the GDPR presents the main regulatory reference for the assessment of ethical and regulatory compliance of personal data processing activities throughout the entire data lifecycle, including the stages involved in the procurement of such data. The GDPR provides for specific principles and requirements on the protection of personal data, providing individuals with more control over how it is used. While the core responsibility of the implementation of these dispositions is assigned to data controllers, joint controllers and data processors, Recital 78 of the regulation makes reference to providers and developers of software solutions, reminding the need to integrate data protection by design and by default across the entire lifecycle of the processing, including appropriate technical and organisational measures. In this context, more and more institutions are pushing for deeper incorporation of compliance with GDPR requirements during the specification of data/solution procurement processes.

This need has been further reinforced by the various guidelines emerging from the EDPB, which has considered the various personal protection-related issues raised by emerging technologies. One example of such relevant guidelines can be found in its latest opinion on AI models⁷, where the EDPB clarifies how the various stakeholders are liable for compliance, and addresses questions regarding anonymity of the models, legitimate interest, and consequences of using unlawfully processed (or procured, to match the specific context of this deliverable) data for the development of AI models⁸. This and other relevant elements for ethical data procurement have been addressed by the EDPB in its efforts to foster EU-wide regulatory harmonization.

This being considered, the figure below presents a high-level process for validating compliance with the GDPR in alignment with the Europrivacy GDPR Certification Criteria validated under Art. 42 by the EDPB. For research activities, and, in particular, those carried out in the ODIN project, the process analysed below is of particular relevance, however it should be further complimented by integrating the relevant specifications developed in EDPB and national authority guidelines, opinions and other documentation.

⁷ Available in: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en

⁸ It is noteworthy that the EDPB specifies that anonymity of an AI model should be assessed in a case-by-case basis (with the goal to determine whether it is very unlikely to “1) directly or indirectly identify individuals whose data was used to create the model, and 2) to extract such data from the model through queries”. Additionally it clarifies legitimate interest as a legal basis for the development and deployment of AI models, and provides a three-step test for its assessment.

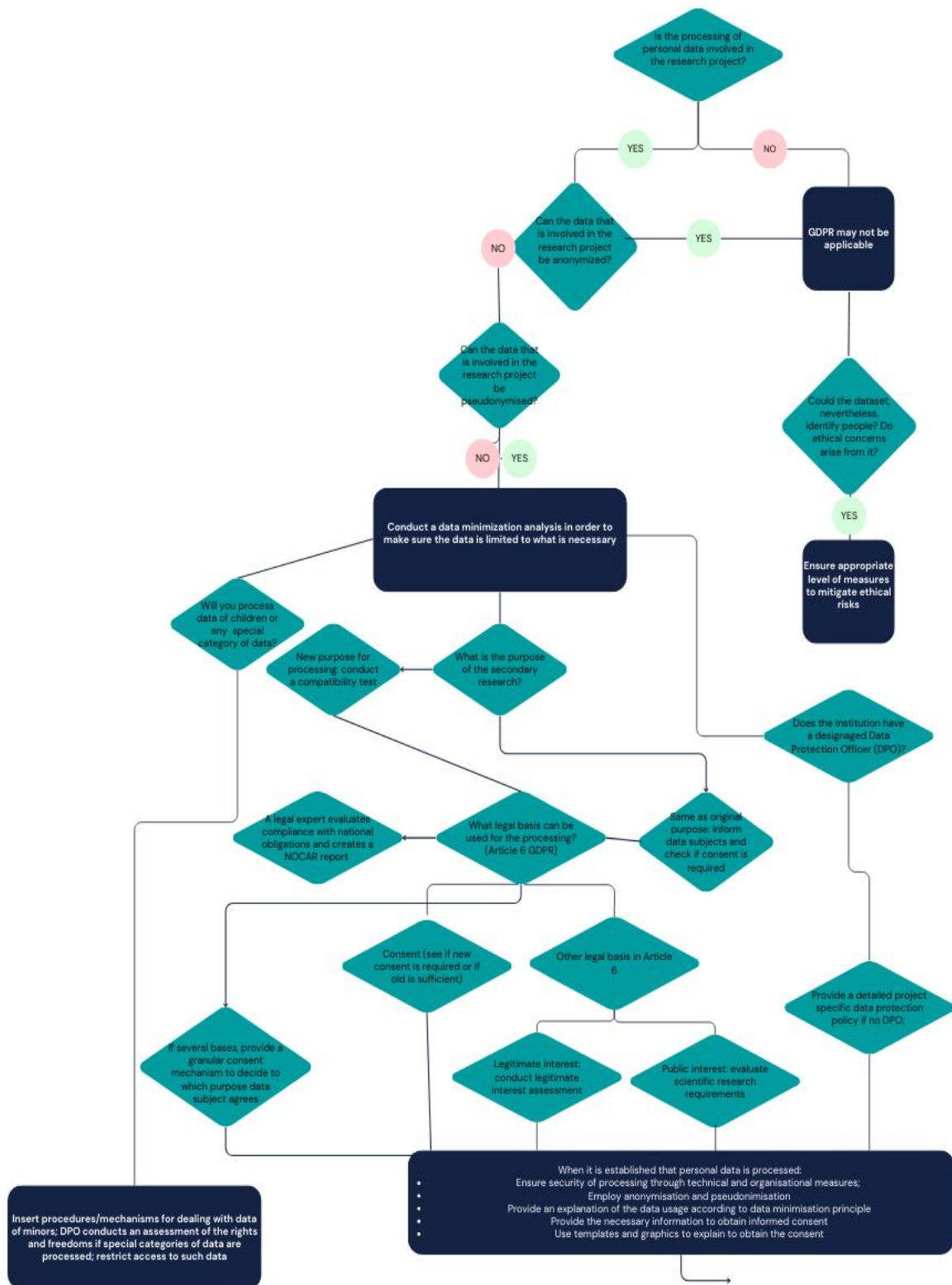


Figure 4. GDPR General Flowchart

As previously noted, the flowchart found in Figure 4 above presents the overall process to be followed when planning and/or carrying out due-diligence activities in the context of a data processing activity, while the last arrow points to Figure 5 below, which will further analyse the specificities of processing special categories of data. Overall, they seek to present a visual representation of the regulatory requirements, and should be considered indicative by interested stakeholders, as a demonstration of compliance with the requirements (particularly when requested by a supervisory authority) will require extensive documentation.

It is worth highlighting that **the activities recommended in the flowcharts are to be based on further prior baseline compliance activities**, such as the development of a Record of Data Processing Activities (ROPA), which will enable the identification of processing which could be undertaken by the different stakeholders, as well as their respective roles and responsibilities.

The following points summarise the key elements considered:

1. Identification of the data and data minimisation, including through anonymisation: it is important to highlight that the processing of anonymised data is allowed without major restrictions imposed by the GDPR. During the data minimisation process, it is important to ensure that the data remains sufficient, pertinent, and restricted to what is strictly required to fulfil the purpose for which it was collected.
2. Identification of the purpose of the processing (in the case of ODIN, of the research): if the processing involves personal or pseudonymised data, it is necessary to understand and clearly identify the purpose of the processing activities. If the data will be further used, then it is important to identify whether the secondary processing has the same purpose as the original one, as follows:
 - a. Same purpose: the data subjects should be informed about the further processing.
 - b. If the purpose differs, then a compatibility test needs to be performed pursuant to Recital 50 of the GDPR. The test includes the consideration of any connection between the initial goals and those of the intended further processing, such as:
 - i. the setting in which the personal data was collected;
 - ii. the reasonable expectations of the data subjects regarding their continued use based on their relationship with the controller;
 - iii. the type of personal data;
 - iv. the implications of the intended further processing for the data subjects; and
 - v. the presence of suitable safeguards in both the original and intended further processing operations.

Lawfulness of the Processing: A legal basis under Art. 6 GDPR must be established. If the data is reused and the grounds for the original processing is consent, then additional consent for the secondary processing must be acquired, or an alternative legal basis, such as a legitimate interest of the controller or public interest, must be established. These actions may then be accompanied by specific considerations to be considered when the processing of sensitive personal data is envisaged:

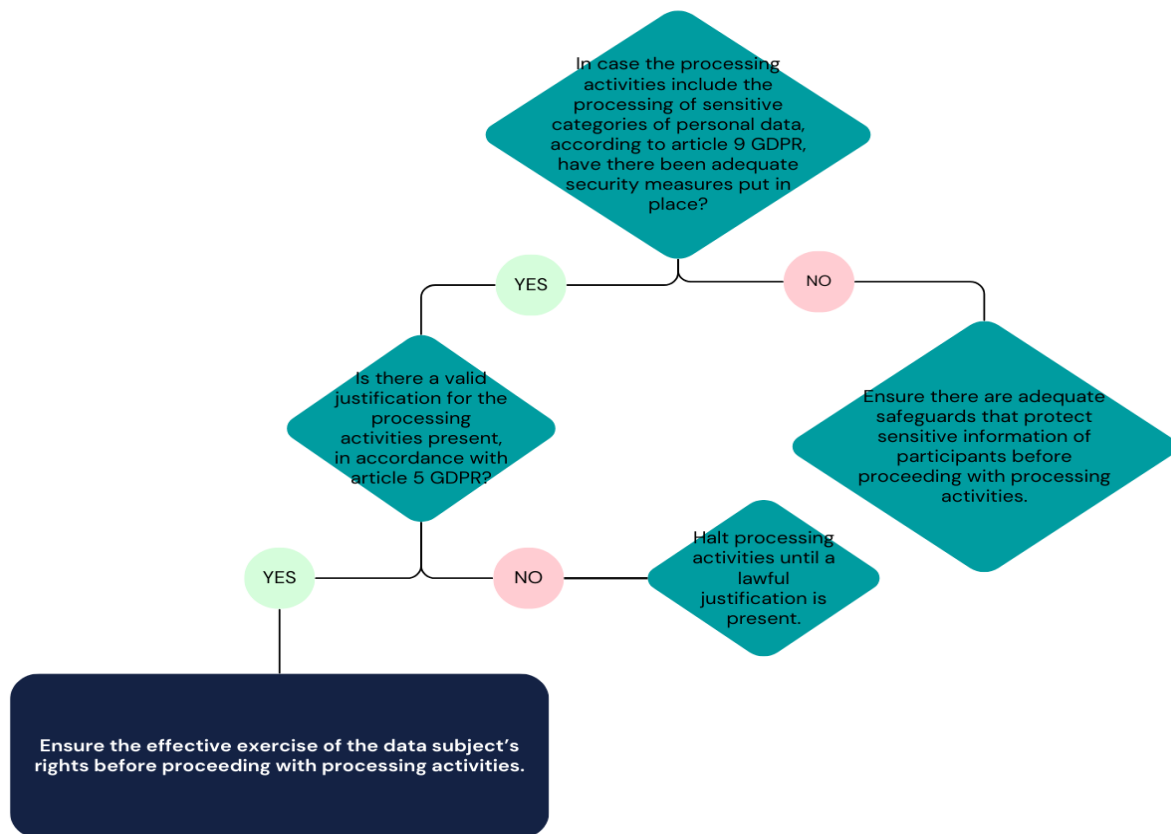


Figure 5. GDPR Flowchart: Requirements for Processing Sensitive Data

As noted in figure 5, sensitive data processing fundamentally requires further examination of both the lawfulness of the processing and the appropriateness of the safeguards in place. Additionally, processing of sensitive data for certain purposes (e.g. training of AI algorithms), or alongside the use of specific techniques and/or technologies, is likely to trigger additional requirements found in the GDPR and associated regulations. Figure 6 seeks to map the main flowchart associated with these requirements, taking into account the increased risk of the processing:

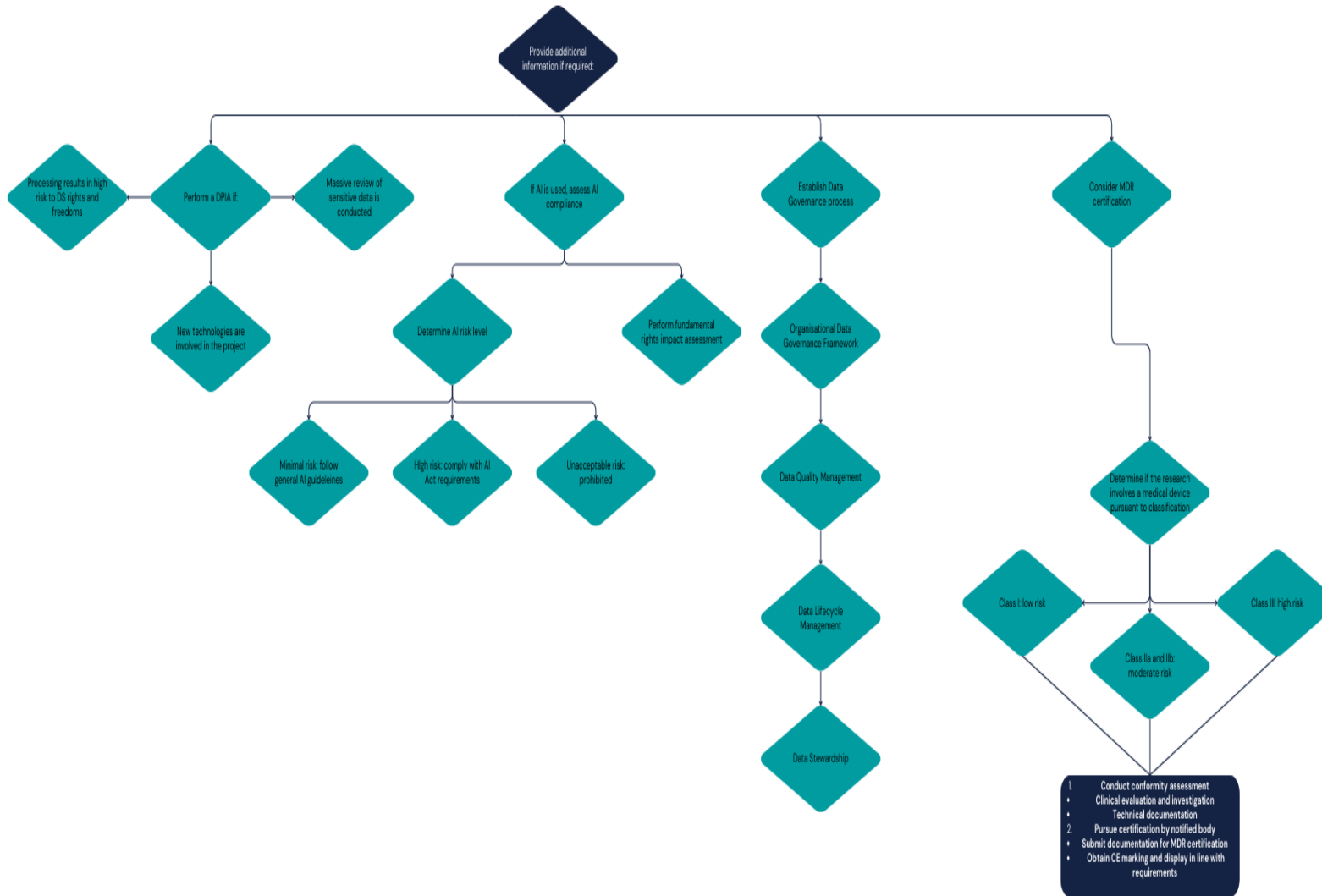


Figure 6 Additional steps for High-Risk Data Processing

The flowchart in Figure 6 includes the following elements:

1. Performance of a DPIA pursuant to Article 35 GDPR: Where the processing activities involve new technologies, processes sensitive data, or if there is a risk to the rights and freedoms of the subjects, then a Data Protection Impact Assessment must be performed. The relevant documentation must include information on:
 - a. how the data is collected;
 - b. how the data subjects will be informed of such high-risk data processing activities;
 - c. how such activities will keep data subjects' rights and freedoms safeguarded.

As part of the DPIA, it is recommended that the DPO is consulted.

2. Assessment of the presence of AI and system compliance: Under the GDPR, AI compliance is considered as part of the automated decision-making dispositions. That being said, the use of AI is now further regulated under the AI Act (see dedicated flowchart below).
3. Demonstrating adequate compliance measures: this point can be achieved through maintaining proper documentation, as well as through the diverse certification options available, such as the EU Data Protection Seal under the GDPR⁹, or certification under the MDR/AI act.
4. Establishing a Data Governance Process: Necessary step to comply with the growing regulatory landscape. In the context of the GDPR, it is directly linked with data protection by design and by default requirements. This is also relevant for any secondary use of the data, where the reasonable expectations of the data subject need to be taken into account to determine whether they should be notified of the further processing, including the reason for the additional processing and their rights.

Given the central role of data within the ODIN project, it is recommended that any data-oriented exploitation activities consider the elements found in these flowcharts, so as to adequately prepare the necessary compliance documentation. These requirements could also be of relevance towards the exploitation of the project's solutions, as regulatory compliance capabilities are increasingly considered within procurement processes.

4.3.3 AI Act and standard EU model contractual clauses

The use of AI in the EU is currently primarily regulated through the AI Act, while the procurement of AI is regulated through standard EU model contractual clauses (*EU model contractual AI clauses to pilot in procurements of AI | Public Buyers Community, 2023*). The AI Act stipulates that the AI Office bears the responsibility to assess and encourage the convergence of best

⁹ In order to facilitate standardised reporting of personal data protection compliance actions, adhering to the Europrivacy compliance assessment methodology (www.europrivacy.com), which is in line with the only European GDPR Certification Scheme (EU Data Protection Seal) approved by the European Data Protection Board, is advisable and this can pave the way for opportunities of post-project certification of the developed solutions Overall, a Europrivacy certification officially validates compliance with European data protection regulations, the GDPR. It is maintained by the European Centre for Certification and Privacy and recognised by data protection authorities of 30 countries, including all EU Member States. This certification scheme provides a flexible but highly reliable method to prove compliance and instate trust in data subjects due to its official status.

practices for AI systems in public procurement procedures. While the AI Act is still in development, public organisations can choose to use the EU model contractual clauses voluntarily. If they rely on the clauses, they need to evaluate and customise their content, on a case-by-case basis, assessing if the various sections of these standard contractual clauses are adequate and appropriate for acquiring a specific AI system. Depending on the risk of the AI, as classified under Article 6 of the AI Act, public organisations may make use of clauses for high-risk AI and non-high-risk AI, describing how AI systems should be procured. The AI Act does not require abiding by these rules when non-high-risk AI is involved, but adherence to them is advised in order to increase the credibility of AI applications. In order to increase transparency, control and accountability, the clauses can be extended also to non-AI systems. Neither the AI Act nor the contractual clauses mention explicitly ethical considerations in public procurement.

That being said, according to the Draft EU Clauses, AI suppliers should ensure that an accountability framework is in place to check the responsibilities of the staff in terms of requirements for development, compliance, examination, and management of data. Moreover, Article 3 mandates transparency in the purpose of data collection when using data to train algorithms as well as measures about the design of the AI, data collection and data management for various operations, formulation of assumptions, and examination of biases, which in particular can have an adverse impact on the health of the people, as well as ensuring measures against such biases and addressing other existent gaps. Transparency is also a requirement in the design of AI systems. Finally, AI systems should be developed in such a manner that their functioning is clear and understandable to public organisations (Article 6).

In addition to the above, the table below illustrates the main requirements for AI Act compliance tailored to data procurement in public hospitals. According to the Act, when AI systems and related data are procured, both the supplier and the public body (in the case of ODIN, public hospitals interested in the integration of these solutions), need to ensure that the requirements are met.

Table 13 Requirements for Public Procurement in the AI Act

Requirement for procurement	Description
Risk-based classification	AI solution examination must follow different requirements for compliance in public procurement depending on the risk classification of the AI.
Risk Management System and Quality Management System	Risk and Quality Management Systems must be incorporated into the AI system for the identification of risks to health stemming from the use of AI.
Data Governance, Cybersecurity, Accuracy, and Robustness	Data protection and cybersecurity measures must be integrated into the AI, especially when sensitive data is involved. Further measures to ensure the system’s robustness and accuracy of the results must be in place.
Technical documentation, instructions for use, and record-keeping	All AI solutions must be accompanied by instructions for their use and the required technical documentation, which are clear and can be easily understood by the Users. The AI solutions need to also have a function to automatically record/log events (in line with transparency and explainability requirements as the

	AI should be designed to be comprehensible and easy to operate).
Human oversight	The AI solutions must have the capability to be overseen by humans. The individuals appointed to oversee the AI need to be trained on how to work with the AI. Thus, training on the selected tool must be available and/or sufficiently documented.
Datasets security and control	Datasets and IPR belonging to the public organisation or the supplier should not be transferred/used by third parties without a specific agreement.
Ethical considerations	AI should be used in line with the seven principles from the Ethics Guidelines for Trustworthy AI. These are: accountability, societal and environmental well-being; diversity; non-discrimination, and fairness; human agency and oversight; technical robustness and safety; privacy and data governance; transparency
CE marking	High-risk AI should bear the CE marking to show compliance with the AI Act

As performed for prior regulations, the following flowcharts present the main procedural elements found in the AI Act:

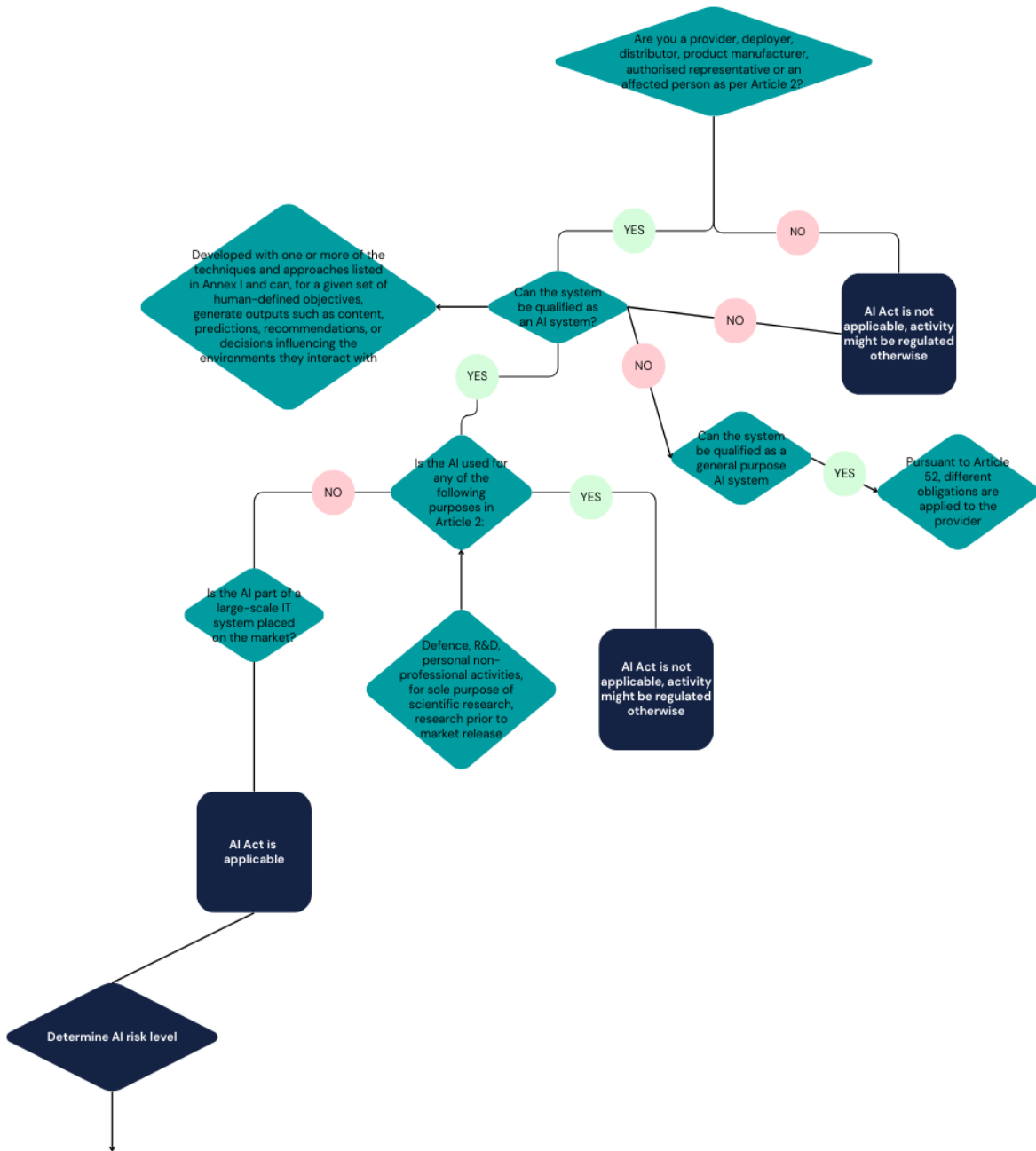


Figure 7. Decision Tree AI Act (1)

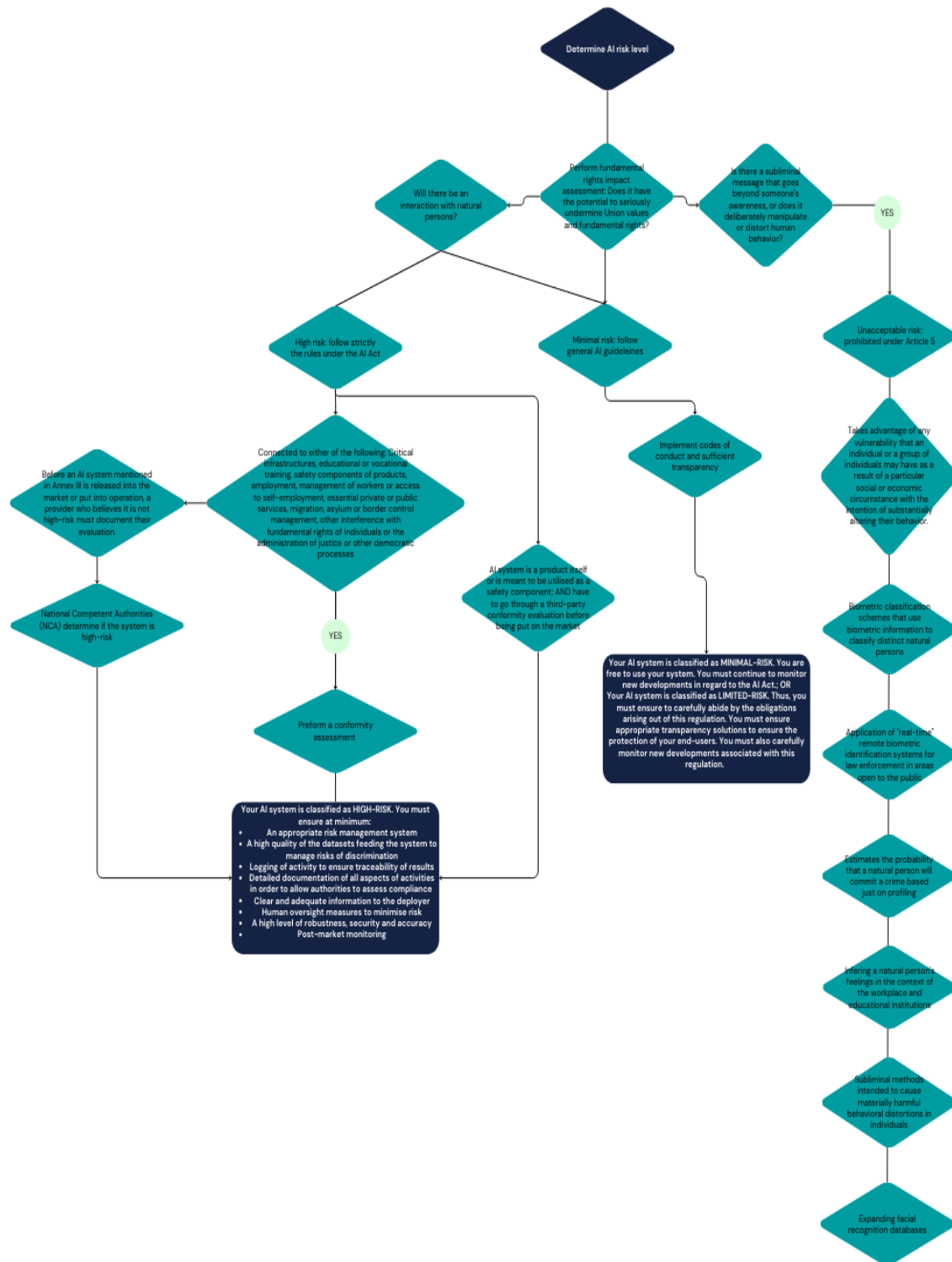


Figure 8. Decision Tree AI Act (2)

In this context, figure 8 presents the first step towards determining compliance actions for the AI: 1. Determining the material application of the AI Act to the system in question.

- a. Ensuring that the stakeholder/organisation that is at the centre of the compliance investigation falls under the scope of Article 2 AI Act, namely whether they are a provider, deployer, product manufacturer, authorised representative or otherwise affected person.
 - b. Determining whether the system can be classified as an AI system under the AI Act. Here it is important to look at the definition of an artificial intelligence system in Article 3(1) of the AI Act in conjunction with the techniques and approaches listed in Annex I.
 - i. Determining whether the system in question can be qualified as a general purpose AI system which, in accordance Article 52 of the AI Act is subject to different and more stringent transparency requirements.
 - c. Evaluating the purposes that the AI system is used for. If the AI system is used for any of the following purposes, the AI Act is not applicable, as they are either prohibited or otherwise regulated (see Article 5 AI Act); National defence, R&D, personal non-professional activities, solely for scientific research, research prior to market release.
2. After the applicability of the AI Act has been determined, figure 8 presents the flowchart towards classifying the AI system in accordance to the different risk levels that are introduced by the legislation. As such, an impact assessment of EU fundamental rights and values must be conducted in order to determine whether any of these values were undermined by the functioning of the system.
- a. If it is found that there are subliminal messages (or similar elements) which goes beyond the user's awareness or has the potential to deliberately manipulate or distort human behaviour, the AI system must be classified as carrying an unacceptable risk and is, thus, prohibited under the AI Act. Factors of such a classification are:
 - Taking advantage of any vulnerability that an individual or a group of individuals may have as a result of a particular social or economic circumstance with the intention of substantially altering their behaviour.
 - The use of biometric classification schemes that are able to classify natural persons.
 - The application of real-time remote biometric identification systems for law enforcement in areas open to the public.
 - The estimation of the probability of natural persons to commit a crime based just on profiling.
 - The inferring of a natural person's feelings in the context of the workplace and educational institutions.
 - The use of subliminal methods that are intended to cause materially harmful behaviour in individuals.
 - Expanding facial recognition databases.
3. If the fundamental rights impact assessment of point 2 determines that there will be an interaction with natural persons, the AI system can be classified as either a minimal risk system or a high risk system, in accordance with the criteria laid down in Article 6 of the AI Act.

- a. If the AI system is classified as presenting minimal risk, the stakeholder must follow the general AI guidelines, implement codes of conduct and ensure a sufficient degree of transparency.
 - i. Has the stakeholder done so, he is free to use the AI system in accordance with the AI Act, however, he should stay aware of changes in the regulation which may lead to a different classification of the system in question.
- b. If the AI system is classified as presenting a high risk system, it is important for the stakeholder to strictly follow the rules laid down for such system in the AI Act. Furthermore, it is important to further assess characteristics of the AI system that may alter the rules that it is subject to under the AI Act.
 - i. A conformity assessment (see Article 3(20) AI Act) must be performed if the AI system is connected to either of the following:
 - Critical infrastructures
 - Educational or vocational training
 - Safety components of products
 - Employment or management of workers or access to self-employment
 - Essential private or public services
 - Migration, asylum or border control management
 - Other interference with fundamental rights of individuals, administration of justice or other democratic processes
 - ii. If it is not believed that the ai system in question should be classified as high risk, before an ai system that is mentioned in annex iii is put on the market or in operation, the provider must document his evaluation for the National Competent Authority to decide on the risk level.

In regard to the activities conducted within the ODIN project, it is important for partners and stakeholders to be aware of the obligations that the AI Act puts upon various different actors connected to these AI systems. This is especially true for exploitation and sustainability-oriented preparatory activities, where performance of a risk qualification of any AI systems developed and the generation of associated documentation will be fundamental towards the presentation of these results to eventual procurement activities. Furthermore, D8.3 identifies AI systems as a key area for possible standardization activities and provides a further in-depth analysis in connection to the ODIN certification strategy.

As in the case of the GDPR, the EU AI Office is expected to generate relevant guidelines, opinions and other supporting documents to bolster the operationalization of the AI Act. These elements should be considered by relevant stakeholders when examining the procurement or deployment of AI models or datasets to be used in the training of such models.

4.3.4 European Health Data Space Regulation (EHDS)

The European Health Data Space (EHDS) Regulation focuses on two main goals, namely the establishment of interoperable Electronic Health Records (EHR) and the reuse of health data for purposes that benefit society as a whole.

Building upon legislation such as the GDPR, the MDR, the In-Vitro Diagnostics Regulation and the AI Act, the EHDS sets requirements tailored for electronic health record systems (EHR systems) directed at promoting interoperability and data portability of such systems. Hence, for medical devices and high-risk AI systems to be interoperable with the EHR systems, they will need to comply with the essential requirements on interoperability under the EHDS Regulation. According to the EHDS transparency can be achieved through a system for mandatory requirements and certification (for EHR systems), which is being further discussed in D8.3 in light of a certification and standardization strategy for the ODIN platform.

Concerning the secondary use of electronic health data, the EHDS complements the Data Governance Act and the Data Act, providing more specific rules for the health sector. These specific rules cover the exchange of electronic health data and may impact on provider of data sharing services, formats that ensure the portability of health data, cooperation rules for data altruism in health and complementarity on access to private data for secondary use.

The EHDS regulation intends to ‘provide a consistent, trustworthy, and efficient system for reusing health data for research, innovation, policy-making, and regulatory activities’ and, thus, improve the use of secondary health data’ (*European Health Data Space - European Commission, 2024*). It is within the ambitions of the European regulator that this regulation finds a balance between making health data available for the public interest and to respect the wishes of patients as individuals.

There are several ways this regulation attempts to achieve said goal. Firstly, the general aim of this regulation is to create a pan-European infrastructure for health data, which involves a regulated and harmonized space for data sharing. Thus, the use of secondary research data becomes more available through being more regulated. The intention here is to make sharing of health data less risky, thus, avoid data breaches and excessive data sharing. As such, the EHDS regulation can make patients, as well as organisations more willing to share such health data. Additionally, by supporting innovation and technical development in this regard, pathways for new and improved ways of securely sharing secondary health data remain open and can, thus, increase the use of such by advancing the current state-of-the-art.

First of all, it is important to note that the adoption of the EHDS regulation will clarify the research exception in the GDPR, as it solidifies its status as a legitimate purpose. For this it is important to take into account that the European Health Data Space aims at ‘providing a trustworthy and efficient set-up for the use of health data for research, innovation, policy-making and regulatory activities (secondary use of data)’ (*European Health Data Space - European Commission, 2024*). In light of research under the GDPR Article 89, which is addressing safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, Member States are able to implement national rules surrounding what classifies under the research exception. Thus, legal certainty was lacking on the EU level, which did not get lifted with the publication of the Guidelines 05/2020 on Consent and Guidelines 03/2021 on the Processing of Personal Data for Scientific Research Purposes by the European Data Protection Board. As such, the EDPB avoided a detailed clarification of the applicability of the research exemption in light of the GDPR. However, in light of the establishment of the European Health Data Space and the adoption of the EHDS regulation, the position of scientific research under the GDPR gets shifted towards being considered as a legitimate purpose for processing. The latter becomes evident, for example, when examining Article 33(2) of the proposed EHDS regulation, which states that ‘data processed for the provision of health or care or for public health, research, innovation, policy making, official statistics, patient safety or regulatory purposes, collected by entities and bodies in the health or care sectors, including public and private providers of health or care, entities or bodies performing research in relation to these sectors, and Union institutions, bodies, offices and agencies’ is covered by the provisions of

secondary use of health data. Additionally, when taking into account the object and purpose of the EHDS and its proposed regulation, namely bringing forward the potential of health data in regard to primary, as well as secondary use, the latter by its very definition including research purposes, it becomes evident that the research exemption in light of the GDPR has been clarified on European level.

Furthermore, the promotion of interoperability of health data and, thus, a standardized format in which health data will be kept, increases the use of secondary health data in practice. Hence, the EHDS regulation attempts to solve the issue of health data being scattered and unusable due to system dependencies. The aim of the regulation is to make health data better accessible for researchers from all throughout Europe and, thereby, lifting several of the bureaucratic and technical barriers that they encounter.

In order to practically realise the above-mentioned points, the European Health Data Space foresees the use of so-called Health Data Access Bodies (see Article 37 EHDS regulation). Through the use of these intermediaries, researchers are able to easily access secondary health data by providing a centralized system to request and provide such data, which, for example, especially simplifies large-scale research that is not bound to the same country.

Next to benefits for conducting the research itself, these intermediaries also provide another layer of institutionalized trust and oversight to the secondary use of health data in the European Health Data Space. Since these bodies are able to decide on the access applications of researchers, there is a clear effort to safeguard patient data by providing such designated organizations. Thus, patients or individuals may recognize the authority of the Health Data Access Bodies and are more likely to trust in such a centralized system.

Furthermore, in view of the practical aspects of the EHDS regulation, TEHDAS is an EU initiative that supports the implementation of the European Health Data Space as a ‘Joint Action Towards the European Health Data Space (TEHDAS)’. Especially TEHDAS2 is intended to practically implement the EHDS regulation in light of a harmonized ‘implementation of the secondary use of health data in the European Health Data Space’. As this initiative creates certain conditions and a necessary infrastructure for the implementation of this regulation, it creates a layer of accountability among the Member States.

The main procurement-related requirements found in the EHDS regulation can be found in the following table. Additionally, figure 9 below presents a flowchart for the EHDS as it has been described above and seeking to clarify the main elements to be considered when seeking to develop a EHDS-compliant Electronic Health Records system (from the manufacturer’s perspective).

Table 14. Requirements for procurement in the EHDS

Requirement	Description
CE marking	Electronic health record systems (EHR) need to have a CE marking to show compliance by the manufacturer with the regulation and other frameworks
Technical standards and specifications	The format of the systems contains datasets with health data, coding systems, and specifications for the exchange of information. This is valid for certain types of priority data such as a patient summary, laboratory results, etc. EHR and high-

	risk AI should be considered in conformity when they meet these technical common specifications
Security processing	Access to health data should be allowed only when security measures are in place. Such are restricted access, using state-of-the-art technological means, data limitation and minimisation, maintain identifiable logs, mitigation of potential security threats.
Data quality	Datasets should have a data quality and utility label. The labels include: data documentation, technical quality, data management, coverage representation of datasets, time on access and provision, data enrichments

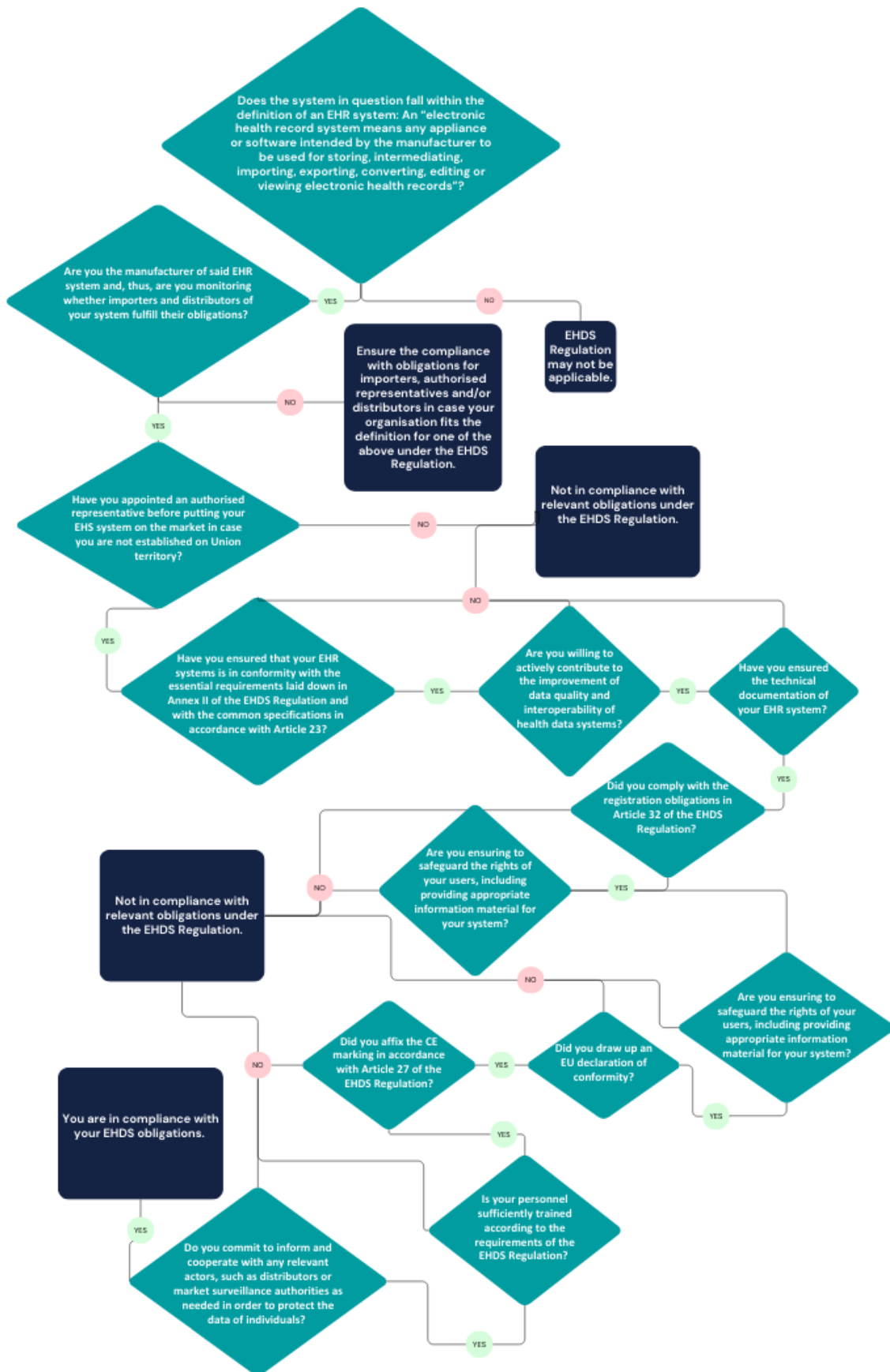


Figure 9. EHDS Decision Tree

An overview of the elements in this flowchart can be found below.

1. Firstly, the applicability of the EHDS Regulation to the system in question must be assessed. As such, the following steps must be conducted:
 - a. Determining whether the system falls within the definition of an EHR system in accordance with Article 2(2)(n) EHDS Regulation.
 - b. Determining whether the relevant stakeholder that is checking its compliance is the manufacturer of said system. It is important to note here that, if it is found that the manufacturer role is not applicable here, the actor may have obligations under a different role according to the EHDS Regulation.
2. After ensuring the applicability of the EHDS Regulation and also of the relevant flowchart, the compliance of the manufacturer with this regulation will be assessed at hand of the following considerations:
 - a. Whether the manufacturer has, in case he is not located on Union territory (if he is located on Union territory this question can be disregarded and the manufacturer may move to the next question) appointed an authorised representative before making the EHR system available on the EU market, in accordance with Article 18 of the regulation.
 - b. Whether the manufacturer has ensured that the EHR system is in conformity with the essential requirements laid down in Annex II of the EHDS Regulation and with the common specifications in accordance with Article 23.
 - c. Whether the manufacturer is willing to actively contribute to the improvement of data quality and interoperability of health data systems?
 - d. Whether the manufacturer has ensured the technical documentation of the EHR system in accordance with Article 24.
 - e. Whether the manufacturer has complied with the registration obligations laid down in Article 32 of the regulation.
 - f. Whether the manufacturer is ensuring to safeguard the rights of users, including providing appropriate information material.
 - g. Whether the manufacturer drew up an EU declaration of conformity.
 - h. Whether the manufacturer has affixed the CE marking in accordance with Article 27 of the regulation.
 - i. Whether the personnel of the manufacturer is sufficiently trained in accordance with the requirements laid down in the EHDS regulation.
 - j. Whether the manufacturer is committing to inform and cooperate with relevant actors, such as distributors or market surveillance authorities as needed in order to protect the data of individuals.

Should all questions be answered in the affirmative by the manufacturer, the flowchart indicates that there is a high chance that he is in compliance with relevant obligations under the EHDS regulation. However, it remains the responsibility of the manufacturer to continuously monitor compliance and, thus, fulfil his due-diligence requirements that accompany the role of manufacturer.

Overall, this flowchart can be very relevant for ODIN partners and stakeholders due to the applicability of the EHDS regulation to the project as a whole (particularly towards secondary use of project data). In regard to data procurement and exploitation activities the flowchart may help

stakeholders to ensure adequate compliance with this regulation and, thus, adequate protection of the personal data that is involved in the project. Due to the sensitive nature of the data involved, it is important to regularly assess compliance with the EHDS regulation, which prescribes specialized rules for these systems, thus, ensuring a unified approach. The flowchart can be a quick and easy way to help fulfil due-diligence requirements in this regard.

4.3.5 Data Governance Act (DGA)

The Data Governance Act provision on prohibition of exclusive arrangements (Article 4) stipulates that grants should be in line with EU public procurement law: *“The grant of an exclusive right pursuant to paragraphs 2, 3 and 4, including the reasons as to why it is necessary to grant such a right, shall be transparent and be made publicly available online, in a form that complies with relevant Union law on public procurement.”*

Apart from these dispositions, the Act includes the following ethical requirements:

Table 15. Requirements for procurement in the Data Governance Act

Requirement	Description
Transparency and Informed Consent	According to data altruism, data should be shared based on the consent from data subjects to handle their personal information or sharing from data holders to permit use of their non-personal information without asking for or receiving payment
Ethics councils or boards	Guarantee that the data controller upholds strict guidelines for scientific ethics and the defence of basic rights, and that there are efficient and easily understandable technical ways to revoke or amend permission at any time.
Open by design and by default	Foster the process of making personal and confidential data available for reuse while also facilitating the safeguarding of such data and aiding in the anonymization process.
Justified and necessary agreements	Conclude agreements only when using the data is the only way to maximise its benefits to society. For instance, in situations where only one entity—which specialises in processing a particular dataset—is able to provide the service or supply the good that enables the public sector organisation to offer the good in the public interest. To maintain transparency, the, agreement should be published on the website and follow the rules for public procurement.

As in the case of the previous regulations, a flowchart has been prepared to address the main practical dispositions of this act. Figure 10 focusses on two main actors under the DGA, namely Data Intermediary Service Providers and Public Sector Bodies intending to re-use data that is in their possession, and it lays down the obligations that can be found for these actors in the regulation.

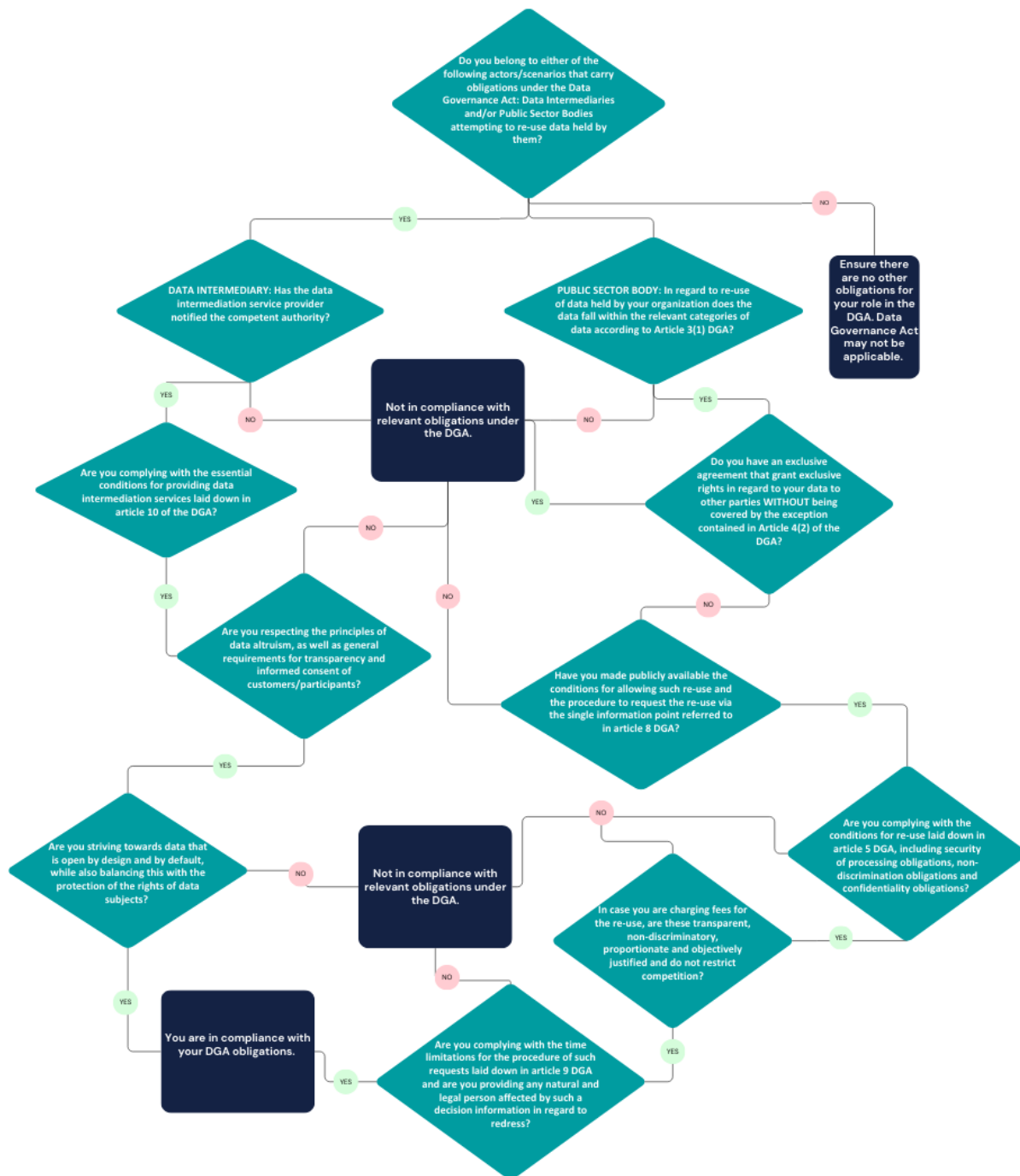


Figure 10. DGA Decision Tree (2)

The following steps serve to further clarify the elements found in figure 10:

1. In consulting Article 2 of the Data Governance Act, it must be determined whether the organisation in question is acting as either a Data Intermediary Service Provider or a Public Sector Body. It is important to note that only because an organisation may not fit the definition of those roles in Article 2 DGA, this does not mean that the organization does not have any obligations under the DGA.
 - a. In case the organisation in question acts as a Data Intermediary, the following points should be considered to assess compliance with relevant obligations:

- i. Whether the Data Intermediary Service Provider has notified the competent authority in accordance with Article 11 DGA.
 - ii. Whether the Data Intermediary Service Provider is complying with the essential conditions laid down in Article 10 DGA.
 - iii. Whether the Data Intermediary Service Provider is aware of, and respecting the principles of data altruism, requirements for transparency and informed consent of customers/research participants.
 - iv. Whether the Data Intermediary Service Provider is striving towards data that is open by design and default, while also balancing this with the protection of the rights of the data subjects.
- b. In case the organisation in question is a Public Service Body intending to re-use data that is held by itself, the following points are considered in order to assess compliance with relevant obligations:
 - i. Whether the data held by the Public Sector Body falls within the relevant categories of data according to Article 3(1) DGA.
 - ii. Whether the Public Sector Body has an exclusive agreement that grants exclusive rights to the data held by this body to other parties without being covered by the exception contained in Article 4(2) DGA.
 - iii. Whether the Public Service Body has made publicly available the conditions for allowing such re-use and the procedure to request the re-use via the single information point referred to in Article 8 DGA.
 - iv. Whether the Public Service Body is complying with the conditions for re-use laid down in Article 5 DGA, including security of processing obligations, non-discrimination obligations and confidentiality obligations.
 - v. In case the Public Sector Body is charging fees for the re-use of this data, whether these fees are transparent, non-discriminatory, proportionate and objectively justified and do not restrict competition.
 - vi. Whether the Public Sector Body is complying with time limitations for the procedure of such requests for the re-use of data laid down in Article 9 DGA and whether redress possibilities are provided to any natural and legal person affected by such a decision.

In the case that the organisation is in fact complying with its obligations as a Data Intermediary Service Provider or a Public Sector Body, the flowchart indicates that the organisation is may be fulfilling its due-diligence and that its actions are aligned with the DGA requirements. It is, however, still the responsibility of the Data Intermediary Service Provider/Public Sector Body to ensure a high level of compliance and to monitor any new developments that may affect their obligations under the DGA.

The DGA flowchart is a helpful tool for ODIN, and furthers procurement and exploitation activities, as it filters out the relevant obligations in light of the project and its future. As such, stakeholders and consortium partners can easily make use of this tool and apply it directly to the relevant activities. As such, the flowchart may help with the overall security of data procurement activities in enabling a broader awareness of requirements and, thus, compliance as a whole.

4.3.6 Medical Devices Regulation (MDR)

The European Medical Device Regulation (MDR), aims to ensure high standards of quality and safety for medical devices being marketed in the European Union (EU). This regulation imposes specific requirements for public procurement in hospitals when obtaining, buying, integrating or training AI-based medical devices. Hence, for the purpose of ODIN project, in parallel with the previous regulations, as part of their conformity assessment for the MDR, project enablers and/or solutions which could qualify as medical devices must comply with requirements dealing with risk management and quality criteria concerning the training, validation, and testing of data sets (Biasin et al., 2023, p. 481).

Under the MDR dispositions, the procurement of tissues and cells should be carried out according to Directive 2004/23/EC. In addition to these dispositions, the European Commission has published a Factsheet for Procurement Ecosystem of medical devices and in vitro diagnostic medical devices^{10 11}.

These requirements ensure the protection of patient data, compliance with legal standards, and the ethical use of AI technologies. The following table provides an overview of important considerations associated with MDR dispositions:

Table 16. Requirements for procurement in the MDR

REQUIREMENT	DESCRIPTION
Classification of AI Medical Devices	Depending on its classification, AI medical devices shall comply with the required conformity assessment (which can range from self-certification by manufacturers for class I devices, to the assessment by a Notified Body, for higher-risk classes).
CE Marking	AI-based medical devices shall meet the essential requirements outlined in the MDR, including safety, performance, and clinical benefit and bear the CE mark as an indicator of compliance with EU regulations.
Clinical Evaluation and Investigation	AI models trained on the transferred data shall be subject to clinical evaluation to ensure their safety, efficacy, and performance. This involves validation studies to confirm that the AI performs as intended in real-world clinical settings. Likewise, post-market surveillance

¹⁰ Available at: https://health.ec.europa.eu/system/files/2020-08/procurementecosystem_factsheet_en_0.pdf

¹¹ In line with this, guidelines published by Health Care Without Harm (HCWH) Europe list five recommendations for sustainable procurement practices for medical devices: conducting baseline assessments, prioritising products, identifying alternatives, raising awareness internally and getting buy-in, preparing and monitoring contracts. Available at https://noharm-europe.org/sites/default/files/documents-files/5720/Guidelines_for_Procurement_of_Safer_and_Sustainable_Medical_Devices_Final_WEB.pdf

	mechanisms shall be implemented to certify ongoing compliance with MDR requirements.
Training of AI models- Data Protection and Privacy	<p>Patients whose data will be used to train AI models must give their informed consent, proving their awareness about how their data will be used, the purpose of the data transfer, and their rights under GDPR.</p> <p>Data shall be anonymized to protect patient identity. When it is not feasible, pseudonymization techniques should be employed.</p> <p>In alignment with the GDPR's principle of data minimization, the minimum necessary data should be transferred for AI training purposes.</p>
Data Security	Robust security measures, such as encrypted channels and secure protocols, shall be implemented. Moreover, strong authentication mechanisms shall ensure that data is only accessed by authorized personnel.
Ethical Considerations	To assess and mitigate potential biases in data and AI models the data used shall be representative. Ethical concerns that arise throughout the development and deployment of AI systems shall be properly addressed.
Technical and Operational Requirements	Detailed and comprehensive documentation of the data transfer process shall be maintained. This includes data selection criteria, anonymization techniques, security measures and consent procedures, among others. Additionally, for the purpose of training AI, data standards and formats shall be interoperable with existing hospital information systems and comply with healthcare data standards.
Vendor Due Diligence	As part of the procurement requirements, it shall be ensured that AI medical devices are certified by the adequate Notified Body (if their classifications require it) and verified that they are compliant with MDR requirements. Additionally, to ensure that vendors involved in data processing and AI development comply will MDR and GDPR's requirements data processing agreements (DPAs) shall be established.
Procurement Process	Contracting authorities may lay down special conditions related to the performance of a contract.
Staff Training	Medical and technical staff shall undergo proper training covering the use and maintenance of AI devices.

The following flowchart considers the relevant dispositions in the Medical Devices Regulation, focusing on the compliance obligations of the Medical Device manufacturer (and not on those requirements of relevance for importers, distributors, etc.)

1. Assessment of applicability of the regulation, including:
 - a. Whether the device in question falls under the definition of a 'medical device' according to Article 2(1) MDR.
 - b. Whether the organisation in question falls under the definition of manufacturer according to the regulation. Again, it is important to realise that even if the organisation does not fall within the definition of manufacturer, it may still have obligations under the MDR as another actor.
2. Analysis of the manufacturer's compliance with key obligations laid down in the MDR, including:
 - a. Whether the manufacturer is ensuring that the medical device that is being placed upon the market is being duly supplied, properly installed, maintained and used in accordance with its intended purpose.
 - b. Whether the manufacturer is ensuring that the medical device meets the general safety and performance requirements that are applicable, taking into account its intended purpose, set out in Annex I MDR.
 - c. Whether an effective quality management system has been established, maintained and kept up to date as prescribed in the MDR.
 - d. Whether the manufacturer has provided a documented and well-maintained risk management system before the device is placed on the market, as described in section 3 of Annex I MDR.
 - e. Whether the manufacturer ensures that information given to the users of said device is given in an indelible, easily legible and clearly comprehensible manner and available in all relevant Union languages.
 - f. Whether the manufacturer ensures that a system for the recording and reporting of incidents and field safety corrective actions are in place for said medical device.
 - g. Whether the manufacturer has ensured that an evaluation of the medical device has been conducted and, whether this evaluation has been documented in accordance with the documentation requirements.
 - h. Whether the manufacturer is committed to cooperate with competent authorities and provide all relevant information and documentation, if necessary.
 - i. Whether the manufacturer is respecting the relevant registration obligations laid down in the MDR, such as registration in the EUDAMED data base and whether it is ensured that economic operators are registered.
 - j. Whether the manufacturer ensured that there are effective measures in place that allow the effective handling of complaints under the MDR, as well as the possibility for natural and legal persons, to claim compensation for damages caused by a defective device in accordance with national and Union law.
 - k. Whether the manufacturer ensured that a post-market surveillance system has been implemented and kept up to date, and, if necessary for the respective device according to its class in the MDR, whether a Periodic Safety Update Report has been planned or prepared.
 - l. Whether the personnel involved in the manufacturing process is sufficiently trained in regard to their obligations, including the risk management strategy, post-market surveillance and quality management strategy.

As presented before, the MDR’s dispositions (and particularly those elements addressing certification requirements for Medical Devices) are of relevance to the future exploitation of the ODIN solutions. Work on the MDR has been particularly addressed as part of ODIN T8.2 and its associated deliverable, which will present the relevant certification strategy for the project. A certification strategy for the ODIN project, which is encompassed in D8.3 also refers to the implications of the Medical Device Regulation in respect to certification.

4.3.7 Other relevant frameworks

Additional public procurement rules (of tangential relevance to this exercise) can be found in other regulatory frameworks, which are further summarised in the following table:

Table 17. Overview of other relevant frameworks

Legislation	Relevant Provision(s)	Explanation
European Data Act (Regulation), (EU) 2023/2854	Preamble 96	Both consumers and suppliers of data processing services should use implementation and compliance tools, especially those released by the Commission as an EU Cloud Rulebook and a Guidance on public procurement of data processing services, to promote interoperability and switching between data processing services. Standard contractual clauses are advantageous because they foster a more balanced relationship between users and providers of data processing services, boost confidence in those services, and provide legal certainty regarding the requirements for switching to other data processing services.
Regulation on the free flow of non-personal data (EU) 2018/1807	Preamble 13	When procuring data, public entities should allow for the free flow of non-personal data and abstain from creating data localisation restrictions.
Horizon Europe Regulation 2021/695	Article 26	Tendering pre-commercial procedures should comply with ethical principles, competition rules, the ‘best value for money’ principle, and allow for multiple sourcing. The contractor producing results in pre-commercial procurement must be the owner of the findings’ intellectual property rights.
Single Market Programme (EU) 2021/690	Preamble 16	Procurement should be strengthened through: professionalisation of public buyers, training and advisory services, transparency, integrity, and better data, creation of specialised IT tools for data gathering and

		data analysis so that access to the market for SMEs is fostered.
European Standardization Regulation, (EU) 2012/1025	Article 13, Article 14	ICT technical specifications that are not national or European standards can be still accepted if they comply with the Regulation for procurement purposes. As such, they should demonstrate market acceptance through maintenance, availability, under FRAND, relevance, neutrality and stability, quality.
NIS 2 Directive, (EU) 2022/2555	Article 24	The use of European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881 may be required for ICT solutions when being procured.

4.3.7.1 International standards

Aside from the international standards that were provided in D8.4 v1, one can consider also IEC 62304:2006 Medical device software — Software life cycle processes, ISO 14971:2019 Medical devices - Application of risk management to medical devices, and ISO 27000 series & IEC 81001-5-1. Additional research on this topic and has been carried out by ODIN Task 8.2 and in the associated deliverables which present relevant information for the exploitation activities of the project. Thus, D8.3 on certification scheme strategy and sustainability plan analyses available international standardization organizations in depth and compares these to national and regional standards, whereby 147 standards were identified.

5 Ethical principle analysis in the ODIN project

5.1 Ethical principle restatement

In the context of the ODIN project, relevant solutions and datasets for project sustainability have been identified in multiple instances¹². As showcased in the previous sections of this document, ethical considerations are not only of relevance to public procurement processes, but also becoming increasingly integrated with security and privacy considerations.

A comprehensive examination of ethics can minimize potential risks associated with the exploitation of ODIN KERs, solutions, and datasets (particularly as necessary to demonstrate due diligence, and compliance from the project partners). From an external perspective, the clarification of these requirements also serves to generate and maintain public trust in the research outputs, promotes the adoption of best practices across current and upcoming research projects (and towards their exploitation and sustainability actions). This being considered, the following table serves to synthesize the main foundational ethical principles identified thus far by ODIN T8.3:

Table 18 Ethical principle restatement

Ethical Principles	Analysis
Autonomy	Autonomy is a core principle in ethics that guarantees the absence of undue influences that could hinder the individuals' capacity of self-determination and self-governing. Thus, autonomy is highly intertwined with fundamental human rights and freedoms, such as the freedom of thought and conscience, the freedom of expression and the right to privacy.
Balance of power	Organizations which possess more information and knowledge than the individuals may take advantage of their position for purposes different than safeguarding the individuals' privacy rights, thus, misusing their power for undermining individuals' autonomy.
Privacy and data protection	Various types of health data, which is considered as sensitive data, will be processed in the context of the ODIN project. The ODIN project should not only acknowledge the need to safeguard privacy in healthcare and software usage but also consider the potential risks that may arise from the inconsistent/unethical use of AI applications/tools.
Accountability	Mechanisms for preventing the abuse of the powers of the relevant tools that are utilized in the context of the ODIN

¹² Including the Description of Action, the Consortium Agreement, the project's Data Management plans, the relevant deliverables on sustainability and particularly (for an ethics perspective) on the two previous iterations of this deliverable.

	project, as well as for monitoring the reduction of harm and should be established.
Transparency /Trustworthiness	The necessary information and details about both the software and its developers should be accessible to users in order to be able to assess the relevant actions and their impact.
Explainability/explicability	The functioning of the relevant algorithms and the necessary pertaining information should be effectively clarified by the developers.
Justice and non-discrimination	Benefits, burdens, challenges and opportunities should be equitably distributed. In the context of the ODIN project non-discrimination should be ensured by the designment of universal and inclusive technologies that won't preclude any individual.
Accessibility	It is of vital importance that the benefits from ODIN technologies and their solutions/results are widely accessible and adopted by hospitals.
Security, non-maleficence, and beneficence	In the context of the ODIN project, which seeks to promote health-related solutions, it is essential that the principle of maximizing benefits while minimizing/reducing harmful impacts would be strictly followed.
Confidentiality and fairness	Fair treatment for all vendors is highly required throughout the whole procurement process.

5.2 Partners' views on Ethical Values and Principles within ODIN

The above-described ethical principles and values were identified as primordial for the ODIN project and led the design and implementation of the project's activities, including its pilots. The present section will mainly focus on presenting the discussions, views, and opinions of the project's partners on how ODIN has aligned with the above, to which extent, as well as the actions they deem necessary to evolve the ODIN activities beyond the project. The outcomes of this section will be taken into consideration for the development of targeted recommendations beyond the project.

In order to promote the discussion on ethics and ensure partners' active participation¹³, a workshop on Ethics was organised during the ODIN Plenary Meeting taking place in Siena from June 25th to June 26th. All partners present, both in person and online, were invited to join an interactive questionnaire allowing for anonymous responses to be displayed in real-time, with a two-fold goal:

- To encourage participation from all partners without discrimination;

¹³ And in alignment with the actions planned in the previous iteration of this deliverable.

- To provide additional information and clarifications in real-time while promoting open dialogue.
- To add any corrective action if needed.

Taking the above into consideration, the questions were aligned with the above-recognised ethical values and principles and were focusing on the following:

1. How do the ODIN solutions ensure equal accessibility for all users?

For this part, partners were invited to provide free-text answers, that better reflected their personal views and opinions regarding the ways in which the ODIN solutions ensure equal access by end-users. In this regard, the Consortium highlighted various elements that facilitate users in utilising the ODIN solutions. The following table summarises said responses starting from the most repeated one to the least.

Partners' Response	Comments
Easy-to-use solutions that are self-explanatory and do not require specific expertise.	The partners highlighted that the ODIN solutions have been designed by default to be easily understood and used, regardless of the level of specialised knowledge of the user, taking into particular consideration the clinicians' needs.
Clear and easy-to-use instructions and manuals.	Particular focus was placed on the provision of instructions and manuals that can further guide users when interacting with the ODIN solutions and solve any questions that may arise.
Training solutions adapted to users' needs.	Similarly, training end users depending on their individual skills and characteristics was also deemed an important measure towards ensuring equal access to the ODIN solutions.
Good Graphical User Interface (GUI)	The quality of the ODIN GUI was also pinpointed as one of the facilitators for end-users' equal accessibility.
Implementation of usability standards and methodologies.	The adoption and integration of usability standards and methodologies, also in accordance with FAIR principles, has also been noted in the process of promoting equal access to the ODIN solutions.
Development in collaboration with end-users	Clinicians, who will be primarily deploying the ODIN solutions, were involved from the start of the project and a co-creation approach was adopted and implemented, thus enhancing the solutions' adoption and usability.

Table 19. Partners' views on ODIN solutions' accessibility measures.

2. Do the ODIN solutions have the potential to disproportionately benefit or harm certain groups of people within hospitals?

Partners were also asked to vote on whether they believed that the ODIN solutions had the potential to disproportionately benefit or harm certain groups of people within hospitals. As demonstrated below, the majority of the Consortium adopted a balanced approach recognised that the ODIN solutions could incur either result depending on their use and safeguards implemented, while many thought that there were far more benefits. It is worth highlighting that only a very small portion thought that the ODIN solutions could exclusively harm certain stakeholders.

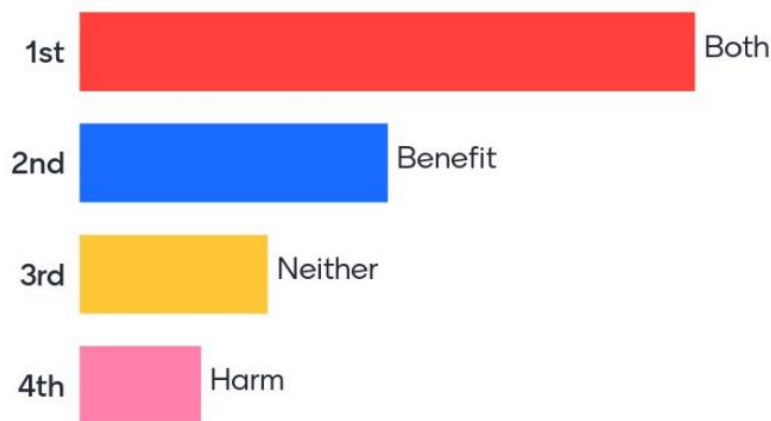


Figure 12. Partners' views on ODIN benefits and harms.

3. Who are the patient populations that might be more vulnerable to the consequences of using the ODIN solutions?

Following up on the above questions, partners were asked to identify the patient populations that could be more vulnerable to the consequences of the ODIN solutions. The following word cloud contains the Consortium's responses, ranking first patients, elderly populations and people with disabilities. In this regard, some partners opted to highlight the importance of three additional factors, namely:

- The patients' psychological state, recognising the difference between calm and anxious patients;
- The education level of populations; and
- The digital literacy of populations, as a distinct factor to the education level.



Figure 13. Partners’ views on vulnerable populations affected by ODIN solutions.

4. Do you believe that certain stakeholders within hospitals are more likely to having their decision-making authority undermined by the ODIN solutions?

Given the use of Artificial Intelligence solutions within the project’s solutions, the potential to affect stakeholders’ decision-making authority was overwhelmingly recognised by partners, as evidenced below. That being said, ODIN has already integrated a number of solutions and features to minimise said risk as will be demonstrated in the following question.

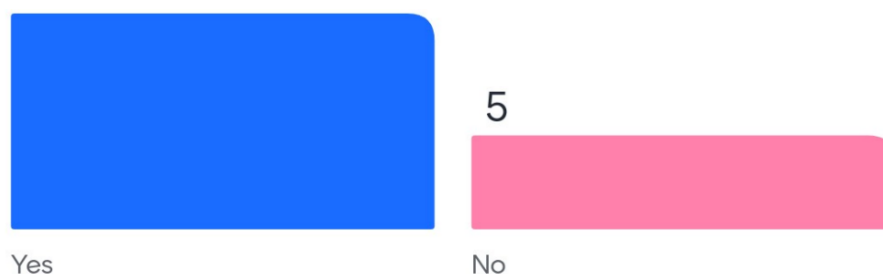


Figure 14. Partners’ views on stakeholders’ decision-making authority.

5. How do the ODIN solutions promote and support the autonomy of patients, healthcare providers, and the hospital ecosystem? (eg. features etc)

As described above, a number of safeguards have been put in place to ensure that the autonomy of all stakeholders relevant to ODIN, including patients, healthcare providers, and hospitals, is respected and promoted. The table below summarises some of those measures, as reported by partners.

Table 20. Partners’ views on ODIN solutions promoting patient, healthcare providers’ and hospital autonomy.

Hospital and Healthcare providers Level	Patients’ Level
Adaptable Workflows	Open and scalable platform
Open and scalable platform	Training on the use of the solutions

Disaster preparedness	Dashboards displaying all relevant information
By reducing the workload of hospital staff	Monitoring of patients' status
Training on the use of the solutions	
Dashboards displaying all relevant information	

6. What are the risks of the ODIN solutions for patient privacy and cybersecurity?

Shifting the focus to privacy and cybersecurity, ODIN partners were inquired about their main risks to privacy and cybersecurity for ODIN, according to their opinion. As verified below, the main concern seems to be personal data and security breaches, including hacking, that could jeopardise the data and system's integrity. Concerns were also raised regarding the potential failures of encryption and authentication measures deployed.

Given the importance of consent for data processing performed within ODIN, the risk of patients' withdrawing consent was also identified as potentially harming the ODIN solutions. At the same time, the need to ensure the adequate use of data by end users and to focus on the potential re-use for research purposes were highlighted.



Figure 15. Partners' views on ODIN privacy and cybersecurity risks.

7. What are the benefits of the ODIN solutions for patient privacy and cybersecurity?

In order to minimise and address the above-recognised concerns, the Consortium has implemented a number of security measures, as reported in more detail in the Data Management Plan. Among those, the partners identified the benefits presented below to be enhancing the privacy and security framework of ODIN.

As indicated below, particular emphasis was placed on the use of federated machine learning practices within ODIN, as a privacy-enhancing technology of major importance. Authentication and role-based access measures, as well as the use of Transport Layer Security (TLS), encryption and adequate key management were also highlighted. What is more, the creation of a trusted environment in which the ODIN solutions operate, as well as the fact that no Personally Identifiable Information (PII) is stored in the platform were considered privacy and security-promoting.

Finally, the contribution of the work performed by Task 3.3 on security and the overall GDPR compliance activities within the project, including the data protection framework established, were underlined.



Figure 16. Partners’ views on privacy and cybersecurity benefits of ODIN.

8. Do the ODIN solutions communicate their inputs, outputs, benefits, and limitations in a transparent and explainable manner?

As will be further analysed below, the partners voiced the need for additional activities promoting transparency, ensuring that the ODIN inputs, outputs, benefits and limitations are actively communicated in a clear and explainable manner.

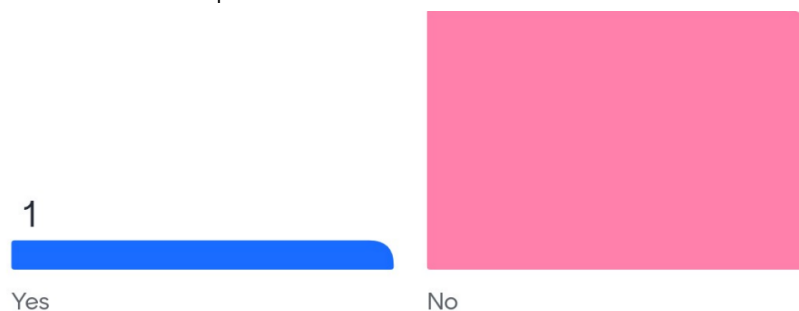


Figure 17. Partners’ responses on ODIN transparency activities.

9. How could transparency be improved?

Since the vast majority of partners voted in favour of more transparency regarding the ODIN solutions, they were further invited to propose solutions and points of focus. As summarised in the figure below, the main focus was placed on increasing communication and dissemination activities, including through the ODIN website and participation in relevant conferences.

Moreover, the need to adapt the content of each communication to the particular needs and characteristics of each audience addressed was raised. In order to achieve this, it was deemed essential to ensure that reports and relevant activities on the project’s and pilots’ activities need to be simplified, abstaining from going into too many technical details and descriptions, so as to

ensure that is easily understood by a wider audience of different education levels and fields. That goes hand-in-hand with the need to further explain the project’s solutions in a clear and easily understood manner.

Finally, the partners underlined the need to cooperatively design a consortium-wide exploitation strategy and jointly plan the activities. An option that was suggested in this regard is the establishment of a Resources Manager that would include all of the ODIN solutions, providing guidance and monitoring the exploitation activities.



Figure 18. Partners’ focus to improve transparency.

10. Which are the mechanisms addressing instances where the solutions' outputs may lead to negative consequences?

In addition to the above, partners were invited to provide their opinions on the mechanisms in place to ensure that the solutions outputs do not lead to negative consequences. In this regard, the focus was placed on the human factor, whether in the form of human supervision or in the form of the final decision being made by a human, using the solutions as an auxiliary measure and not a decision-making system.

The features integrated regarding explainability and bias control were given further attention. Finally, testing and validation of results and outputs were heavily relied upon to ensure that no negative consequences are incurred for stakeholders.



Figure 19. Partners' views on ODIN safeguard mechanisms.

11. How would you define "trustworthiness" in the context of the ODIN solutions within hospitals?

The final question focused on the concept of trustworthiness within ODIN. As can be verified by the figure below, trustworthiness, on one hand, was closely tied to transparency, explainability and traceability of results and solutions. In this regard, the integrity of the data and the solutions, as well as the robustness of the whole system were underscored.

On the other hand, accuracy and ensuring the solutions' goals are efficiently achieved were a major part of trustworthiness, in order to inspire trust and confidence. For this, it was deemed essential to further demonstrate the proficiency of the Consortium and the solutions built, highlighting the measures in place to ensure said results including testing. Finally, addressing privacy, security and usability concerns was also crucial to ensure the trustworthiness of the ODIN solutions.



Figure 20. Partners' definition of trustworthiness in the context of ODIN.

The results of this exercise served as an informative baseline for the recommendations transmitted by WP8 to WP9 (reflected on the final deliverable on project legacy) and served as a fundamental element for the development of the annexes to this deliverable.

6 Ethical Data Procurement: Guidelines and Recommendations

6.1 Summary of ethical outputs found in previous iterations of this deliverable

The previous versions of the deliverable analysed and developed an initial set of guidelines and recommendations to address ethical dataset sourcing towards AI/ML solutions intended for the healthcare industry.

Taking into account the above analysis and the normative landscape that is currently being formed, this chapter aims to provide a compact overview of the best practices that need to be included in the IPJ process for ODIN to embed data ethics. The previous version of this deliverable has developed four main sub-sections, namely under the titles 'Reflect', 'Implement', 'Demonstrate' and 'Embed', inspired by the 'ethical platform for responsible delivery of an AI project' by Leslie D and the Alan Turing Institute. In the context of these four main sub-sections, key ethical themes, such as human dignity, fundamental human rights protection, transparency, explainability, environmental protection, and inclusivity, that supplement each other, were identified, and were analysed in correlation with the CARE principles. These principles provide a 4-dimensional view of these themes and give useful high-level guidance on what should be done to ensure each ethical theme is embedded throughout the IPJ process. More precisely, under the 2nd sub-section of the previous version of this deliverable ('IMPLEMENT' & 'DEMONSTRATE'), the FAST principles were thoroughly examined, considering the stages of public procurement and the lifecycle of the product/service. The FAST principles incorporate all ethical themes and the CARE principles and, as such, comprise the following principles: fairness, sustainability, accountability, and transparency. Under the last sub-section, namely the 'EMBED' sub-section, a practical diagram was provided to better visualise how and when these requirements are applicable (Leslie, 2019). The complete analysis of these four main sub-sections can be found in the published, previous version of this deliverable, under the title (*ODIN D8.4 r1*), and more specifically in pages 57-69.

The Venn diagram below reiterates the importance of the interaction between the four sections mentioned previously:



Figure 21. Odin’s Data Ethics and Procurement Framework Interplay -Venn Diagram

The ‘Reflect’ part of the previous version of the deliverable mapped out 10 ethical themes: human dignity, fundamental rights protection through fairness and legal compliance, prevention of misconduct or incompliance, transparency, explainability, serving public good, environmental protection, traceability, accountability and control, and finally universal design. Each of these ethical themes supports the others and calls for either proactive action or precautions to lessen their negative effects. They were illustrated also in a 4-dimensional view through the CARE principles, which provides for way of integration throughout the IPJ process as shown in the figure below.

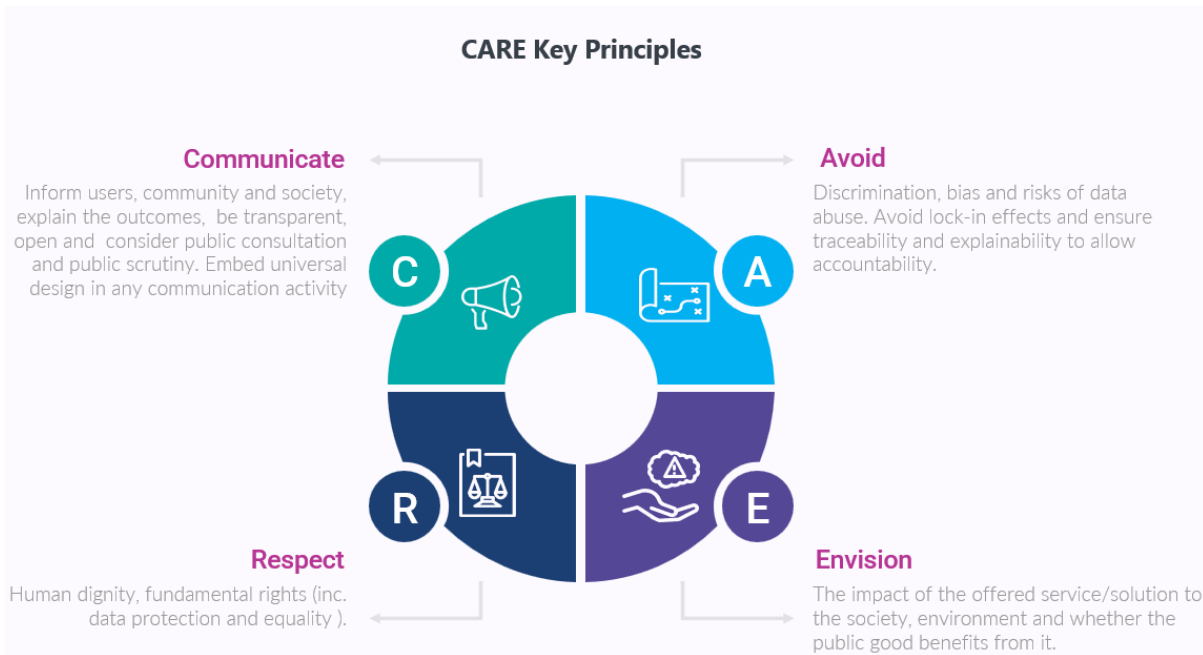


Figure 22. CARE Principles

As a next step, previous versions of the deliverable outlined the practical requirements of the CARE principles and the key ethical themes in the form of FAST principles while accounting for public procurement and the lifecycle of the product/service. It was concluded that to achieve the practical aspects of the ethical themes, implementation of a data governance/accountability framework and oversight mechanisms as explained in section 7 of this deliverable. This was presented in the form of tables which depicted the principles of fairness, accountability, sustainability, and transparency. Several measures can be highlighted from the tables: conducting DPIAs, labelling, mitigating bias, trustworthy data access control, contact with the users for feedback, secure and detailed architecture of the ODIN platform especially for activity tracking, communication with the stakeholders, conducting reports and publishing them.

In order to guarantee the successful execution of these suggestions throughout the ODIN project, a brief checklist that encapsulates the aforementioned recommendations was designed. The checklist contains points that should guide implementers based on a swimlane diagram as well as European legislation. For example, as required by the GDPR, implementers should ensure a clear purpose for processing, categorisation of the type of data, conducting DPIAs, labelling, data policy, and implementing technical and organisational measures for security, while also showing consideration for ethical principles.

Lastly, a swimlane diagram was embedded that illustrates how ethical considerations are implemented from the beginning of the procurement to the end, as explained also in the first section on why procurement is needed.

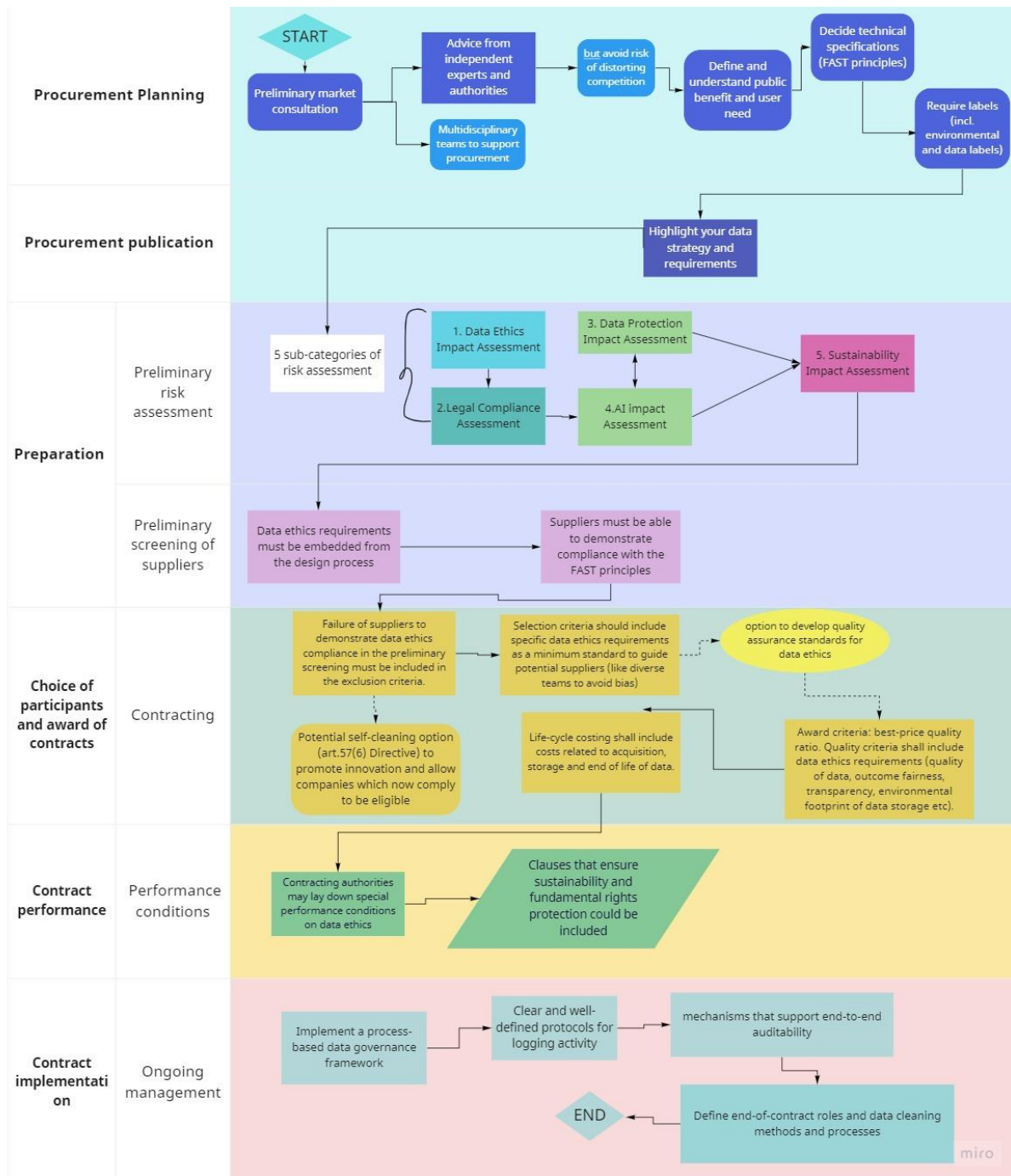


Figure 23. How to embed data ethics requirements per public procurement stage (swimlane diagram)

6.2 Updated ethics-related conclusions and questionnaire introduction

As was previously established, in the healthcare industry, high-quality datasets are essential for AI because they support precise diagnosis, patient safety, dependability, credibility, generalisation, bias reduction, regulatory compliance, and the promotion of research and innovation. As such, obtaining (procuring, generating and/or purchasing of) high-quality data

guarantees that healthcare AI systems operate at peak efficiency and eventually enhance patient outcomes. (Davenport and Kalakota, 2019) (de Hond et al., 2022).

The source of the training datasets is crucial to achieving high-quality requirements. When trained on inadequate, erroneous, or irrelevant data, machine learning models can experience serious setbacks that impair their robustness and performance. (CloudFactory, no date). Healthcare organisations can create fair, reliable, and advantageous AI-based solutions for patients and society at large by prioritising ethical considerations when gathering datasets. (Tomasì, 2023) (Lawton, 2023) (Shaher A., 2023). Contrary to other jurisdictions, commercial procurement of datasets containing personal data (thus, of relevance to eHealth applications), is complexified in Europe due to stringent regulatory requirements. As such, ethical sourcing (explored in section 6.3) and alignment with relevant regulatory developments (such as the European Health Data Space Regulation) is of utmost importance for innovative solution development and adoption in the region.

This considered, an efficient data governance policy must be in place within the procuring organization to guarantee the processing of patient health data in a way that is both ethically and legally acceptable¹⁴, particularly whenever the procurement or data processing activities are tied to the integration of AI in hospitals¹⁵, which has been identified to be a priority action point for the EC.

ODIN addresses the above-mentioned points by integrating innovative solutions which allow hospitals to procure and handle data in a safe, secure, and privacy-compliant manner¹⁶. The visualizations provided in the previous sections seek to provide an operational-oriented perspective of the applicable requirements, in a manner that is more easily integrable with business processes within the hospital ecosystem.

In addition to this, T8.3 has sought to synthesize its main outputs in three questionnaires (Annexes 1-3) which may facilitate discussions between the various stakeholders involved in the procurement journey. These questionnaires have been designed to ensure the ethical and legal procurement and use of AI/LLM solutions, particularly those involving personal data, within public hospitals in the EU. They target three different stakeholders:

- **Annex 1: Public Hospitals Procuring Data for AI Training:** This simplified questionnaire focuses on the minimum requirements and documentation needed when public hospitals procure data (especially sensitive personal data) for training AI, like LLMs. It aims to

¹⁴ An example of the elements that should be considered is how to mitigate ethical concerns about manipulating data subjects' behaviour or exploiting 'perceived consent', for which any expected health data sharing (including those activities performed in the context of a off-site deployment of an AI system), should have clear objectives and trusted beneficiaries. Data sharing data should be performed in a transparent manner to further valuable health research, the results of which will benefit patients' communities. By designating independent external experts or organisations with a reasonable level of skill in all relevant sectors, who have no stake in the data subjects' privacy and are unrelated to the data controllers' purposes, those goals can be demonstrated and safeguarded. A governance system like this might guarantee impartial, transparent oversight, which could increase reliability and confidence.

¹⁵ As previously noted, the European Commission's 2020 AI white paper highlights how crucial the promotion and adoption of AI in hospitals is, as well as the importance of initiating a dialogue across healthcare to support public procurement of AI systems, aiming at transforming the process of public procurement (Shaip, 2022). As mentioned in this deliverable, however, data misuse, bias, poor-quality data inputs used to train AI models, and personal data privacy are just a few of the ethical issues around data usage that have been brought up by the ever-expanding data analytics potential.

¹⁶ ODIN's WP2 is of relevance to this point, as it has sought to facilitate health care, productivity, and stakeholder involvement through the Innovative Procurement Journey (or "IPJ").

facilitate discussions between technical and legal teams to assess the viability of data procurement for AI development.

- **Annex 2: Public Hospitals Procuring AI/LLM Solutions:** This high-level questionnaire outlines the legal and ethical considerations for public hospitals when procuring AI/LLM solutions. It complements existing resources, like the European Association of Medical Devices Notified Bodies' work on AI in medical devices. It helps prepare documentation for viability assessments by technical, medical, legal, and administrative teams.
- **Annex 3: AI/LLM Solution Providers:** This self-assessment questionnaire outlines the legal and ethical requirements and best practices for providers offering AI/LLM solutions to public hospitals. Completing it helps providers prepare necessary documentation (like DPIAs and FRIAs) to facilitate certification and viability assessments by the hospital's teams.

By offering a structured and simplified approach for ethical data and AI procurement in healthcare (tailored to the relevant stakeholders and their roles/responsibilities), these annexes may bring value to ODINs WP2-9 IPJ, sustainability and legacy-oriented activities. Their implementation and further adaptation by future research projects is furthermore recommended.

7 Pathways and governance beyond ODIN

7.1 ODIN Governance Avenues

As already highlighted, the ODIN project has developed a number of solutions and outputs that can benefit not only the research community but also the healthcare sector and society as a whole. In order to maximise said impact, a clear and robust Governance framework needs to be established, facilitating the reuse of the ODIN outcomes and related knowledge while ensuring legal and ethical compliance.

In view of the above, the ODIN Consortium has already started relevant discussions on the ways forward to efficiently manage the ODIN outcomes, particularly relevant with regard to the data collected and produced within the project. In the course of these discussions, ODIN partners have paid particular focus to the identification of their individual needs and the corresponding principles to be encompassed by the ODIN Data Governance framework beyond the project.

As such, the need to ensure data security and privacy have been at the forefront of said needs, considering, in particular, the sensitive nature of many of the datasets as they include personal data related to health. In this regard, the proposed Data Governance model needs to encompass adequate data policies and management measures, including consent management, as well as facilitating data subjects' rights, providing for clear data retention procedures, in line with the data minimisation principle, and promoting the adoption of effective security measures, including encryption, anonymisation and/or pseudonymization, as well as adequate access controls.

Beyond that, data quality, including completeness, accuracy, consistency, and integrity has also played a central role in the development of an adequate Data Governance framework. The following figure provides a summary of the overarching principles of the ODIN Data Governance Framework, addressing the partners' needs and requirements.

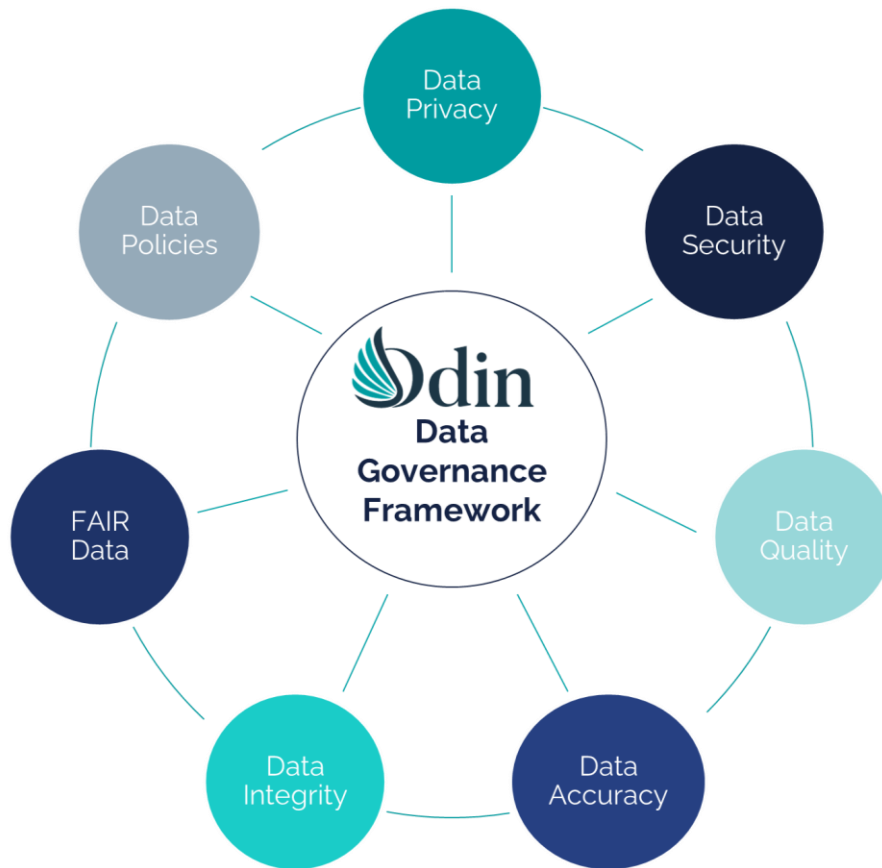


Figure 24. ODIN Data Governance Framework Principles.

In light of the aforementioned requirements, the present section presents a proposed Data Governance model, addressing the main questions with regard to Data Governance, namely identifying the reasons behind it, the stakeholders and related responsibilities, the data policy specifications, the location of the data, the timeframe and related milestones, as well as the related processes, standards and rules. The following table summarises said points and the suggestions currently reviewed by the Consortium.

Table 21. ODIN Data Governance Model Needs and Recommendations.

Data Governance Focus	Explanation	ODIN Data Governance Model Recommendations
Why	Defines the reasons behind the Data Framework.	The ODIN Data Governance Model has been identified as essential in order to move forward for the following primary reasons: <ul style="list-style-type: none"> a) To promote the exploitation of ODIN data beyond the project’s duration; b) To ensure the scalability of the ODIN solutions and their wide-spread adoption; c) To ensure compliance with relevant legal and ethical requirements.

Who	Identifies the Stakeholders and corresponding Responsibilities.	<p>In the context of ODIN, the relevant stakeholders can be identified as follows:</p> <ul style="list-style-type: none"> • ODIN stakeholders: <ul style="list-style-type: none"> ○ Coordination Team: coordinates the data governance activities at a central level. The Data Governance Coordination team is different from the project’s Coordination Team and can be comprised of representatives from all partners. ○ Data Owners: are the original owners of the data and, in their majority, correspond to healthcare providers within ODIN. ○ Data Stewards: are in charge of creating the data governance processes and procedures and monitoring their application, including tracking quality and enforcing compliance. ○ Data Custodians: are in charge of designing and implementing effective security measures to provide a secure environment for accessing and reusing the data. They correspond to the technology providers. • External stakeholders: <ul style="list-style-type: none"> ○ Data Users: can correspond to the EHDS Regulation data users, having successfully gone through the process of the Data Permit request in order to perform research on the data. ○ Patients: main data subjects who contribute their data to perform research. The Data Governance framework needs to facilitate the exercise of their rights and provide an adequate protection framework.
What	Specifies the Data Policy requirements.	In alignment with the already existing data policies within ODIN, the approach remains two-fold, as follows:

		<ol style="list-style-type: none"> 1. Promoting data availability, in accordance with FAIR and Open Science principles to the greatest extent possible; 2. Ensuring data protection and security, respecting data privacy in particular. <p>As such, the ODIN Data Policy to move beyond the project shall, particularly, encompass the following elements:</p> <ul style="list-style-type: none"> • Lawfulness of any personal data processing, purposes of processing, and data sharing requirements; • Provisions to facilitate the exercise of data subjects' rights; • The procedure to ensure data quality; • Data access requirements, conditions, and procedure; • The security measures in place and related security procedures; • Procedures to manage data breaches and security incidents; • Further compliance requirements; • The intellectual property requirements and attribution requirements.
Where	<p>Defines the location where the data is stored and from where it is being made available.</p>	<p>Currently, data in ODIN is stored locally at the Data Owner’s facilities according to their individual procedures and requirements. Moving forward, data storage could either remain local or move to a central repository.</p> <p>In either scenario, the existing ODIN platform can be utilised as a “one-stop-shop” receiving, reviewing and approving/rejecting requests, while also providing a secure environment for making data available, where feasible.</p>
When	<p>Sets realistic timeframes and milestones with regard to data governance.</p>	<p>The related timeframes and milestones within the ODIN ecosystem could be identified as follows:</p> <ul style="list-style-type: none"> • M1 – Before the project’s end: Deciding upon how and with the collaboration of which partners to continue beyond the project; • M2 – Before the project’s end: Deciding upon the structure and architecture; • M3 – Before the project’s end: Identifying the datasets and solutions that can be

		<p>further made available and the conditions therein;</p> <ul style="list-style-type: none"> • M4 – Upon the finalization of M1-M3: Design the Data Policy based on information/requirements received. <p>Further milestones will be provided as the discussions progress.</p>
How	Establishes the procedures, standards, and rules to ensure compliance.	The baseline for the procedures, standards and rules to be considered when designing the further Data Governance framework have been provided in the context of this deliverable and the Data Management Plan.

According to the proposed framework described in the above table, the following figure visualises in a simple manner how the suggested model could operate in practice, in accordance with the roles and tasks discussed, focusing particularly on the data governance model.

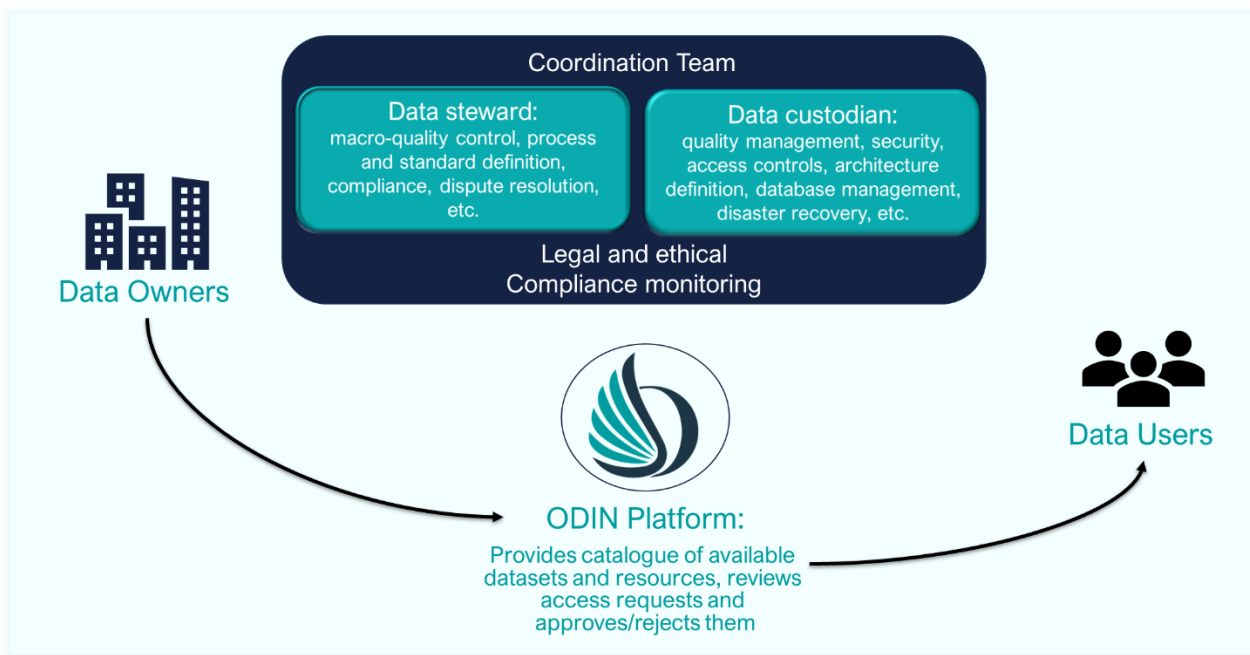


Figure 25. Data Governance Model Visualisation

As already clarified, the above-described recommendations are based on the ongoing discussions on governance beyond the ODIN project. The ODIN Consortium is already collecting and compiling the information on the datasets and solutions available, their quality, owners, and

conditions for reuse, so as to facilitate said discussions. Finally, the work of WP9 on Exploitation¹⁷ will further complement the analysis hereby presented and will facilitate the adoption of the necessary procedures and measures to enhance ODIN's impact, in accordance with legal and ethical requirements.

7.2 ODIN as an ethically compliant enabler of living labs and regulatory learning in healthcare

As noted in previous sections of this deliverable, Europe is currently at a crossroads of technological and regulatory developments which also impact organizational and administrative actions such as public procurement. The wide range of relevant regulatory frameworks, international and governmental oversight bodies and their intrinsic interconnection not only complexifies the process of compliance for organizations (such as public hospitals), but also makes it more difficult for regulators to properly communicate with regulated entities and learn from their experiences and feedback in order to further enhance and streamline the regulatory frameworks in the future.

Despite what could be perceived as an ever-expanding maze, several options and opportunities are available within the scope of current regulations and best practices¹⁸, which could serve to guide conversation of relevant stakeholders towards a mutually beneficial path. Regulatory learning is the process of acquiring and jointly expanding technical knowledge in alignment with (and in communication with) the regulatory agencies as a means to collaboratively develop better regulatory frameworks. This action can be performed in the context of healthcare through the alignment of research projects with regulator's needs, or by better integrating living labs¹⁹ (as tools for solution development and new technology testing) into the oversight and feedback process of relevant authorities.

In this context, UPM's living lab is a key enabler that could facilitate this alignment in the future, and ODIN could serve as a key enabler for this action. The integration and continuity of the ODIN toolset and enablers, both through the work of WP9 and by its deployment in the context of the UPM living lab could serve as an excellent demonstration of the project's potential for regulatory

¹⁷ The final WP9 deliverable on project legacy establishment will provide a more comprehensive report on the expected governance structure pursued by the project stakeholders.

¹⁸ An example of this is the inclusion of regulatory sandboxes in the AI Act, for example, which demonstrates willingness and disposition from the regulatory authorities towards controlled experimentation and regulatory learning processes.

¹⁹ In general, living labs are 'open innovation ecosystems in real-life environments using iterative feedback processes throughout a lifecycle approach of an innovation to create sustainable impact' (About us - Living Labs, 2017).

learning²⁰, especially if paired with a viable long-term governance strategy²¹ which addresses not only post-project data management and data sharing activities, but also issues associated with AI governance and IPR/licensing management towards sustainability²².

The resulting information from this examination served to define and draft the Memorandum of Understanding presented to all consortium partners as part of the project legacy-oriented activities of WP9.

²⁰ Initial discussions with relevant data protection and AI authorities performed in the context of the 2024 editions of the Privacy Symposium, the IAPP Europe congress and the CPDP conferences have revealed the viability of this proposed approach. Furthermore presentations carried out towards the members of the International Accreditation Forum and the Global Privacy Assembly led to initial positive feedback on the project outputs and its relevance to new developments, both from a procurement and certification perspective.

²¹ Living labs usually involve multiple stakeholders which are involved in the decision-making project. Since stakeholders from various areas, such as academia or governmental organisations might be involved in such a living lab, a collaborative way of decision-making should be designed in order to account for feedback of these various stakeholders. In regard to ODIN, it is especially important to involve patients, as end-users in such a decision-making process and also the living lab as a whole.

²² UDGA is currently facilitating this action alongside with UPM, Mysphera, and other interested parties and will report with more detail on the final legacy deliverable for the project.

8 Conclusions and Way Forward

This deliverable presented both the regulatory requirements applicable to public procurement and the wider frameworks of relevance to the ODIN project, and has showcased the critical need for a simple, trustable and transparent ethical data procurement journey which better addresses the needs of smart hospital ecosystems and the difficulties associated with secondary processing of personal (health) data. It builds upon the work carried out in its previous iterations to generate operations-oriented recommendations and solutions (see annexes) whilst promoting responsible data handling and forward-thinking post-project sustainability actions to be considered and addressed in the final deliverables of the project.

The following are some of the key findings of this deliverable which should be considered as part of the ODIN legacy actions:

- Despite regulatory and technical developments, data procurement (and public procurement of health data) remains a challenge due to its intrinsically sensitive nature. This hinders policy development and transparency. Furthermore, the lack of a standardized approach to ethically compliant data and solution procurement presents barriers in an increasingly connected European Healthcare ecosystem.
- Feedback obtained from project stakeholders highlights key concerns regarding data security and personal data protection as reasons for the difficulties in data procurement (particularly as relevant to sensitive data from vulnerable groups). Bias in AI systems developed using available data within a single hospital is a significant risk, which in turn reinforces the need for viable ethical and legally compliant solutions for data procurement.

ODIN's outputs, past deliverables and key enablers shed further light on these issues, and may present us with some ways forward, such as better tailoring sustainability activities for the project to consider the regulatory and ethical requirements of innovative healthcare platforms, and the opportunities available in the regulatory landscape as of today. Furthermore, several general recommendations may be extrapolated:

- Bolster communication amongst national and international regulatory authorities and ethical boards, particularly in the context generated by an increasing number of regulatory frameworks and fast technological developments.
- Seek to standardize ethical procurement processes which better match international requirements on data and AI solutions whilst addressing national and international best practices for procurement.
- Prioritize transparency and stakeholder engagement across the ecosystem: Data governance and AI governance are two areas where ethical procurement should be considered. Centralization of information, increased accessibility, transparency and trust generation should be fundamental to ease data contribution by data subjects for research, and to ease compliance with data sharing requirements in those cases where data or solutions are to be procured externally.
- Data and solution certification may provide viable pathways to ease trustable sharing and procurement. In line with the results of D8.2, recent developments in regulatory compliance certification point towards the relevance of third-party certification as means to generate trust amongst international stakeholders for data sharing, particularly if performed in alignment with the requirements set by regulators and with close oversight by relevant accreditation authorities.

- EU standardization efforts on data (e.g.: quality, integrity, anonymization, federation, synthetic data generation, and privacy enhancing technologies) and AI (bias identification, trustability, and explainability), should be bolstered to align European best practices, provide technical clarity and mitigate legal uncertainty which may prevent broader adoption and divide procurement approaches amongst public hospitals.
- Development of compliance and self-assessment tools (such as the questionnaire presented in the annexes to this document) can help communication amongst the diverse stakeholders in an organization seeking to procure data or innovative solutions. These solutions should be further refined and developed to better meet both the needs of the various organizations and to better address evolving (and often diverging) recommendations from regulatory bodies.

Lastly, it is noted that the ODIN platform may serve as a key enabler for regulatory learning in the future, particularly if deployed in a secure processing environment such as a living lab with appropriate governance structures and regulatory support (e.g. approval as a regulatory sandbox). In this context, it is highly recommended that project partners consider adopting a Memorandum of Understanding (as prepared by WP8&9 partners) which clearly defines a project legacy roadmap and which continues to address the topics mentioned in this deliverable.

9 References

About us - Living Labs (2017) *European Network of Living Labs*. Available at: <https://enoll.org/about-us/> (Accessed: 17 September 2024).

Burrows, E. (2024) 'Public Procurement 2024'. Global Legal Group.

CloudFactory (no date) *The Essential Guide to Quality Training Data for Machine Learning*. Available at: <https://www.cloudfactory.com/training-data-guide> (Accessed: 11 July 2023).

Davenport, T. and Kalakota, R. (2019) 'The potential for artificial intelligence in healthcare', *Future Healthcare Journal*, 6(2), pp. 94–98. Available at: <https://doi.org/10.7861/futurehosp.6-2-94>.

Direccio General de Contractacio Publica (no date) 'Codi de Principis'. Available at: <https://contractacio.gencat.cat/web/.content/principis/transparencia-bones-practiques/bones-practiques/codis-bones-practiques/codi-principis-conductes-recomanables.pdf> (Accessed: 17 March 2022).

Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC Text with EEA relevance (no date).

EU model contractual AI clauses to pilot in procurements of AI | Public Buyers Community (2023). Available at: <https://public-buyers-community.ec.europa.eu/communities/procurement-ai/resources/eu-model-contractual-ai-clauses-pilot-procurements-ai> (Accessed: 19 June 2024).

European Commission (2017) 'COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Making Public Procurement work in and for Europe'. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A572%3AFIN> (Accessed: 16 March 2022).

European Commission (2020) 'WHITE PAPER On Artificial Intelligence - A European approach to excellence and trust'. Available at: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf (Accessed: 16 March 2022).

European Commission (2021) 'COMMISSION NOTICE Guidance on Innovation Procurement'. Available at: <https://ec.europa.eu/docsroom/documents/45975> (Accessed: 16 March 2022).

European Health Data Space - European Commission (2024). Available at: https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en (Accessed: 16 September 2024).

Events (2019) '4 Types of Tender and Tendering Processes', *Opus Kinetic*, 17 April. Available at: <https://www.opuskinetic.com/2019/04/4-types-of-tender-and-tendering-processes/> (Accessed: 25 June 2024).

Health Care Without Harm (2014) 'Sustainable Public Procurement in European Healthcare'. Available at: <https://noharm-europe.org/sites/default/files/Factsheet%20%7C%20Sustainable%20Public%20Procurement.pdf> (Accessed: 16 March 2022).

de Hond, A.A.H. *et al.* (2022) 'Guidelines and quality criteria for artificial intelligence-based prediction models in healthcare: a scoping review', *npj Digital Medicine*, 5(1), pp. 1–13. Available at: <https://doi.org/10.1038/s41746-021-00549-7>.

Kalamaras, I., Lolis, V. and Flevarakis, K. (2024) 'ODIN Platform D3.12'.

Lawton (2023) *What are AI Ethics (AI Code of Ethics)? | Definition from TechTarget, WhatIs.com.* Available at: <https://www.techtarget.com/whatis/definition/AI-code-of-ethics> (Accessed: 11 July 2023).

Naves, J. (2023) 'Proposal for standard contractual clauses for the procurement of Artificial Intelligence (AI) by public organisations'. European Commission. Available at: https://public-buyers-community.ec.europa.eu/system/files/2023-10/AI_Procurement_Clauses_template_High_Risk%20EN.pdf.

ODIN Partners (2020) 'ODIN Proposal - Leveraging AI based technology to transform the future of healthcare delivery in Leading Hospitals in Europe'. Horizon 2020 Call Innovation Action.

Perez, M. and Guillen, S. (2024) 'ODIN D9.9 Exploitation Report and Business Models'.

'Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space 2022/0140' (2022). European Commission.

Public procurement | EUR-Lex (no date). Available at: <https://eur-lex.europa.eu/EN/legal-content/summary/public-procurement.html> (Accessed: 12 July 2024).

Public procurement - European Commission (no date). Available at: https://single-market-economy.ec.europa.eu/single-market/public-procurement_en (Accessed: 25 June 2024).

Public tendering rules in the EU (no date) *Your Europe*. Available at: https://europa.eu/youreurope/business/selling-in-eu/public-contracts/public-tendering-rules/index_en.htm (Accessed: 25 June 2024).

Quesada, A. *et al.* (2023) 'D8.4Data Ethics Procurement for Public Hospitals'.

Shaher A. (2023) *Ethical Considerations for the Responsible Development and Use of AI" | LinkedIn.* Available at: <https://www.linkedin.com/pulse/ethical-considerations-responsible-development-use-ai-shaher-al-hroub/> (Accessed: 11 July 2023).

'Special report on Public procurement in the EU: Less competition for contracts awarded for works, goods and services in the 10 years up to 2021' (2023). European Court of Auditors.

Tomasi, C. (2023) 'The Principles of Ethical AI: 4 Examples to Follow', *MorphCast*, 15 March. Available at: <https://www.morphcast.com/the-principles-of-ethical-ai-what-you-need-to-know-in-this-transformative-year-2023/> (Accessed: 11 July 2023).

World Health Organisation (2021) *Ethics and governance of artificial intelligence for health.* Available at: <https://www.who.int/publications/i/item/9789240029200> (Accessed: 16 March 2022).

World Health Organization (2024) *Ethics and governance of artificial intelligence for health: Guidance on large multi-modal models*. Available at: <https://www.who.int/publications/i/item/9789240084759> (Accessed: 25 July 2024).

10 Annex 1: Simplified Questionnaire for Public Hospitals Considering Procurement of (Personal) Data (for AI training)

The following questionnaires seek to enable a high-level overview of the minimum applicable requirements to be considered, and documentation elements to be prepared by public hospitals in the process of procuring data (particularly concerning special categories of personal data), towards the development or training of AI-enabled solutions (such as LLMs). The resulting elements should serve to guide the discussions between technical teams in charge of the processing and the organization’s legal team so as to facilitate the viability assessment of the proposed actions.

Procuring and processing special categories of data under the GDPR		Art	
What are the justifications for processing?	Explicit Consent		9(2)(a) -(f)
	Employment, social security and protection		
	Protect the vital interests of the data subject Condition: Data subject is physically or legally unable to give consent		
	Pursuing legitimate purpose of the institution Condition: you must be not-for-profit Condition: personal data are NOT disclosed without the consent of the data subject		
	Personal data is made public by the data subject		
	Necessity for establishment, exercise, or defense of legal claims		
	Necessary for the public interest		
	Necessary for public health		
	Archiving, research, statistical purposes		
Is the data procured directly from the data subject?	Yes	No	12-14
	If no, then you must inform the data subject about 1. the holder that shared their data; 2. purpose of the procurement; 3. rights of the data subject		
Have you conducted a Data Protection Impact Assessment (DPIA*)?	Yes	No	35

Is the solution/dataset covered under a relevant Art. 42/46 GDPR certification?	Yes	No	43, 46
Procuring and processing electronic health data for secondary use under EHDSR			Art
Are you procuring electronic health data (EHD) for secondary use?	Yes	No	
In the context of secondary use, which purpose are you using the data for?	Public Interest	Statistics	34
	Support of public sector bodies	Scientific research for healthcare	
	Education or teaching activities	Development and innovation for products/services in healthcare	
	Training and testing AI systems and algorithms	Personalized medicine	
What type of data are you collecting/processing?	Electronic Health Records	Data impacting on health	33
	Pathogen genomic data	Health-related administrative data	
	Human genetic, genomic and/or proteomic data	Person-generated electronic health data	
	ID data related to health professionals treating natural persons	Population-wide health data registries	
	EHD from medical registries for specific diseases	EHD from clinical trials	
	EHD from medical devices, registries for medicinal products and medical devices	Research cohorts, questionnaires, and surveys related to health	
	EHD from biobanks and dedicated databases	Electronic data related to insurance, profession, education, lifestyle, wellness	
	EHD containing improvements such as correction, annotation, enrichment received by the data		

	holder following a processing based on a data permit		
	Other:		
Can the purpose be achieved with anonymized data?	Yes	No	10(5)(a)
	If yes, then it must be anonymized. If not, then you must provide clear reasons why. Connect the purpose of the procurement to the anonymity of the data		
In the context of processing EHD for secondary use, have you submitted a Data Access Application*?	Yes	No	45
Will you reuse the data?	Yes	No	5 DGA
	If yes: You may need to comply with additional requirements related to: <ol style="list-style-type: none"> 1. Specific conditions for the processing environment; 2. Provide mechanisms (tools and digital environments) to allow verification of any results of processing by the re-user; 3. Re-use of data must respect intellectual property rights and/or commercial confidentiality 		
Procuring and processing data in association with the AI Act			Art
Are you using the data to train AI systems*?	Yes	No	10, 27
Is the training taking place within a regulatory sandbox for AI?	Yes	No	56
In the case of training AI systems, have you conducted a Fundamental Rights Impact Assessment (FRIA)*?	Yes	No	27
Have you conducted assessments in the past (e.g. DPIA)?	Yes	No	27(2)
	If yes: previous assessments can be used to comply with the requirement for a FRIA		
Has any information from the assessment changed?	Yes	No	27(1)(2)
Have you updated the assessment to reflect latest and accurate activities?	Yes	No	27(2)

Have you set a timeframe for periodic revision and update of the assessment (e.g. 3 months, 6 months, etc.)?	Yes	No	
--	-----	----	--

Clarificatory compliments:

Data Protection Impact Assessment (Article 35 GDPR):

A mandatory process when dealing with large scale of special categories of personal data (e.g. medical/health data). The DPIA must contain information about:

- ✓ Description of the processing operations
- ✓ Purpose of processing
- ✓ Explain why the specific processing of the specific data in question is necessary
- ✓ Explain how the processing is proportionate to the purpose
 - Limit the processing only to what achieves the purpose
 - Place a time limit on processing the data (delete data after time limit or extend by going through the same process)
 - Limit the data to only what is necessary to achieve the purpose
 - AVOID collection of data that will NOT be needed
- ✓ Explain the risks that data subjects face in the process of handling their personal health data
- ✓ List in detail the technical measures to protect the data
 - Provide descriptions of the tools used
 - Provide descriptions and lists of the mechanisms (e.g. Authentication layers, Software security, etc.)
 - Explain how those work to provide protection to the data subjects' rights, freedoms, and personal data

Data Access Application (Article 45 EHDSR)

Under the EHDS, you must submit an application for accessing electronic health data for secondary use (e.g. scientific research). The application must be submitted to a health data access body (determined by State governments on a national level). It must contain the following information:

- ✓ a clear list of the purposes for which processing of electronic health data is sought;
- ✓ a description of the requested electronic health data, their format and data sources;
- ✓ an indication whether the data will be anonymized;
- ✓ an explanation of the reasons for seeking access to electronic health data in a pseudonymized format;
- ✓ a description of the safeguards that prevent any other use of the electronic health data;
- ✓ a description of the safeguards planned to protect the rights and interests of the data holder and of the natural persons concerned;
- ✓ an estimation of the period during which the electronic health data is needed for processing;
- ✓ description of the tools and computing resources needed for a secure environment.
- ✓ IF the data will be in pseudonymized format, you must add the following additional information:

- An assessment of ethical aspects of the processing
 - An explanation that prioritizes good will and protection of data subjects

Fundamental Rights Impact Assessment (Article 27 AI Act)

The FRIA is mandatory when deploying AI systems and using personal health data to train those systems. It must contain the following information:

- ✓ The processes in which the AI system will be used and the intended purpose;
- ✓ A description of the period of time for using the AI system
- ✓ A description of the frequency with which each AI system is intended to be used;
- ✓ The categories of natural persons and groups likely to be affected by the use in the specific context;
- ✓ The specific risks of harm to the categories of natural persons or groups of persons identified;
- ✓ A description of measures that include human oversight;
 - These must have instructions and detailed operation
 - How it works and how it will act against the risks identified
- ✓ Measures to be taken in the case of the risks coming to reality
 - Examples can be internal governance, notification mechanisms, complaint mechanisms, etc.

Training AI systems to detect and correct bias (Article 10(2) AI Act)

You must be able to prove and comply with the following requirements:

1. Explain why the bias correction cannot be effectively fulfilled by processing other data;
 - a. Explain why it cannot be fulfilled with the use of anonymous data
2. Explain what technical limitations are placed on the re-use of the personal data
 - a. This can include state-of-the-art security and privacy-preserving measures, including pseudonymization;
3. Explain what measures are used to ensure that the personal data processed are secured and protected
 - a. This can include strict controls and documentation of the access
 - b. The goal is to show how you avoid misuse and ensure that only authorised persons have access to those personal data with appropriate confidentiality obligations;
4. You must be able to explain how you keep track that data are not to transmitted, transferred or otherwise accessed by other parties;
5. You must delete all medical data once the bias has been corrected or the personal data has reached the end of its retention period, whichever comes first;
 - a. You must have a limit on the period of time that you are allowed to retain the data
 - b. After that period, you must delete the data
6. You need records of processing activities that include the reasons why the processing of special categories of personal data was strictly necessary to detect and correct biases, and why that objective could not be achieved by processing other data.

11 Annex 2: High-level Viability Assessment Questionnaire for Ethical Procurement of AI/LLM Solutions by Public Hospitals

The following questionnaire seeks to synthetically present the legal and ethical requirements and best practices to be considered by relevant staff members when proposing the potential adoption and/or procurement of AI/LLM solutions for use in a public hospital.

The contents of this questionnaire are not exhaustive, and should be considered as complementary procurement-oriented elements to dedicated questionnaires such as the [position paper / questionnaire on Artificial Intelligence on Medical Devices recently published by the European Association of Medical Devices Notified Bodies](#)

Completion of this questionnaire can guide the preparation of relevant documentation which will facilitate viability assessment from the technical, medical, legal and administrative teams of the organization.

1. Pre-Procurement Considerations

a. Needs Assessment and Definition

Question	Potential Answers	Regulatory Reference
Have we clearly defined the specific needs and objectives for the AI/LLM solution?	Yes / No	EU Procurement Directive 2014/24/EU, Article 40 - Prior information notices
Does the solution align with the hospital's mission and values, particularly regarding patient care and data protection?	Yes / No	N/A (Best Practice)

b. Stakeholder Engagement

Question	Potential Answers	Regulatory Reference
Have all relevant stakeholders been involved in the planning process (clinicians, IT professionals, data protection officers, legal advisors, ethics committees)?	Yes / No	N/A (Best Practice)
Have we gathered input on requirements, expectations, and potential concerns related to the AI/LLM solution?	Yes / No	N/A (Best Practice)

c. Risk Assessment

Question	Potential Answers	Regulatory Reference
Have we conducted a preliminary risk assessment focusing on data privacy, security, and ethical implications?	Yes / No	GDPR Article 35 - Data Protection Impact Assessment (DPIA)

Have we considered the impact on patient rights and hospital operations?	Yes / No	GDPR Recital 75 - Risks to the rights and freedoms of natural persons
--	----------	---

2. Procurement Specification Development

a. Legal and Regulatory Compliance

Question	Potential Answers	Regulatory Reference
Does the solution comply with the General Data Protection Regulation (GDPR)?	Yes / No	GDPR (Regulation (EU) 2016/679)
Does the solution meet the requirements of the EU AI Act, including provisions for high-risk AI systems used in healthcare?	Yes / No / Not Applicable	AI Act, Title III, Chapter 1, Article 6 - Classification of high-risk AI systems
If the solution involves electronic health data, does it comply with the European Health Data Space Regulation (EHDSR)?	Yes / No / Not Applicable	EHDSR, Article 33 - Secondary use of electronic health data

b. Ethical Requirements

Question	Potential Answers	Regulatory Reference
Does the solution incorporate privacy-enhancing technologies and follow the principles of data minimization and purpose limitation?	Yes / No	GDPR Article 5(1)(b)(c) - Purpose limitation and data minimization; Article 25 - Data protection by design and by default
Does the AI/LLM provide transparent operations and explainable outputs, especially in clinical decision-making contexts?	Yes / No	AI Act, Article 13 - Transparency and provision of information to users
Are there measures to detect and prevent biases that could lead to discriminatory outcomes?	Yes / No	AI Act, Article 10(2) - Data and data governance; GDPR Article 5(1)(a) - Lawfulness, fairness, and transparency
Does the solution include functionalities for managing patient consent where necessary, in accordance with legal requirements?	Yes / No / Not Applicable	GDPR Article 7 - Conditions for consent; Article 9(2)(a) - Explicit consent for processing special categories of data

c. Technical and Functional Specifications

Question	Potential Answers	Regulatory Reference
Is the solution interoperable with existing hospital systems and compliant with established data standards?	Yes / No	EHDSR, Article 5 - Interoperability requirements

Does it have robust cybersecurity features, including encryption, authentication protocols, and intrusion detection systems?	Yes / No	GDPR Article 32 - Security of processing; NIS Directive (EU) 2016/1148
Does the solution meet or exceed defined performance indicators and quality benchmarks?	Yes / No	AI Act, Article 15 - Accuracy, robustness, and cybersecurity

3. Supplier Qualification Criteria

a. Experience and Expertise

Question	Potential Answers	Regulatory Reference
Does the supplier have demonstrable experience in developing AI solutions for the healthcare industry?	Yes / No	EU Procurement Directive 2014/24/EU, Article 58 - Selection criteria
Can the supplier showcase technical competence and an innovation track record?	Yes / No	EU Procurement Directive 2014/24/EU, Article 58 - Selection criteria

b. Compliance Demonstration

Question	Potential Answers	Regulatory Reference
Can the supplier provide evidence of compliance through certifications such as ISO 27001 for information security management?	Yes / No	EU Procurement Directive 2014/24/EU, Article 62 - Quality assurance standards and environmental management standards
Does the supplier demonstrate an understanding of GDPR, the AI Act, and other relevant regulations?	Yes / No	EU Procurement Directive 2014/24/EU, Article 57 - Exclusion grounds

c. Ethical Commitment

Question	Potential Answers	Regulatory Reference
Does the supplier have clear corporate responsibility policies, including data protection practices and corporate social responsibility initiatives?	Yes / No	EU Procurement Directive 2014/24/EU, Article 18(2) - Compliance with environmental, social, and labor law
Is there a positive compliance record without past data breaches or regulatory infractions?	Yes / No	GDPR Article 83 - Administrative fines; EU Procurement Directive 2014/24/EU, Article 57(4)(c) - Exclusion grounds

4. Tendering Process Requirements

a. Transparent and Fair Procedures

Question	Potential Answers	Regulatory Reference
Is the tendering process open, transparent, and providing equal opportunity to all qualified suppliers, in line with EU public procurement directives?	Yes / No	EU Procurement Directive 2014/24/EU, Article 18 - Principles of procurement

b. Detailed RFP Documentation

Question	Potential Answers	Regulatory Reference
Does the Request for Proposal (RFP) detail all legal, ethical, technical, and functional requirements?	Yes / No	EU Procurement Directive 2014/24/EU, Article 42 - Technical specifications
Are the evaluation criteria and weighting clearly outlined, including compliance, ethical considerations, cost, and technical capabilities?	Yes / No	EU Procurement Directive 2014/24/EU, Article 67 - Contract award criteria

5. Proposal Evaluation

a. Compliance Verification

Question	Potential Answers	Regulatory Reference
Does the proposal comply with GDPR, the AI Act, EHDSR, and other applicable regulations?	Yes / No	GDPR; AI Act; EHDSR
Does the supplier effectively address ethical considerations, including data privacy and bias mitigation strategies?	Yes / No	AI Act, Article 9 - Risk management system

b. Technical and Functional Analysis

Question	Potential Answers	Regulatory Reference
Has a live demonstration or pilot implementation been requested and evaluated to assess real-world performance?	Yes / No	EU Procurement Directive 2014/24/EU, Article 44 - Technical capacity
Is the solution scalable and flexible to adapt to future needs and regulatory changes?	Yes / No	N/A (Best Practice)

c. Risk and Impact Assessments

Question	Potential Answers	Regulatory Reference
----------	-------------------	----------------------

Has a Data Protection Impact Assessment (DPIA) been conducted to identify and mitigate risks?	Yes / No	GDPR Article 35 - Data Protection Impact Assessment
For AI systems, has a Fundamental Rights Impact Assessment (FRIA) been evaluated?	Yes / No / Not Applicable	AI Act, Article 29 - Fundamental rights impact assessment

6. Contracting

a. Clear Legal Agreements

Question	Potential Answers	Regulatory Reference
Are specific Data Processing Agreements included in the contract, detailing data protection obligations, responsibilities, and liabilities?	Yes / No	GDPR Article 28(3) - Processing by a processor
Are confidentiality clauses robust and comprehensive to protect sensitive information?	Yes / No	GDPR Article 5(1)(f) - Integrity and confidentiality; EU Procurement Directive 2014/24/EU, Article 21 - Confidentiality

b. Compliance and Audit Clauses

Question	Potential Answers	Regulatory Reference
Does the contract require the supplier to maintain compliance throughout its duration?	Yes / No	GDPR Article 28(3)(h) - Processor's obligations
Is there a right to conduct audits or assessments to verify the supplier's compliance?	Yes / No	GDPR Article 28(3)(h); AI Act, Article 23 - Technical documentation

c. Termination Conditions

Question	Potential Answers	Regulatory Reference
Are conditions defined under which the contract can be terminated due to non-compliance or ethical violations?	Yes / No	EU Procurement Directive 2014/24/EU, Article 73 - Termination of contracts

7. Implementation and Integration

a. Data Governance Framework

Question	Potential Answers	Regulatory Reference
----------	-------------------	----------------------

Are clear roles and responsibilities established for data stewardship, including data access controls and accountability mechanisms?	Yes / No	GDPR Article 24 - Responsibility of the controller
Is there a process to ensure the accuracy and integrity of data used by the AI/LLM solution?	Yes / No	GDPR Article 5(1)(d) - Accuracy; AI Act, Article 10 - Data and data governance

b. Staff Training and Awareness

Question	Potential Answers	Regulatory Reference
Is comprehensive training provided for staff on using the new system, focusing on compliance and ethical use?	Yes / No	GDPR Article 39 - Tasks of the data protection officer; AI Act, Article 14 - Human oversight
Have ethical use guidelines been developed for interacting with the AI/LLM solution?	Yes / No	AI Act, Article 14 - Human oversight

c. Monitoring and Evaluation

Question	Potential Answers	Regulatory Reference
Is there continuous monitoring of the system's performance against predefined metrics?	Yes / No	AI Act, Article 61 - Post-market monitoring
Are regular compliance verifications scheduled to ensure legal and ethical boundaries are maintained?	Yes / No	GDPR Article 24 - Responsibility of the controller; AI Act, Article 61

8. Post-Implementation Review

a. Continuous Improvement

Question	Potential Answers	Regulatory Reference
Are feedback mechanisms established for users to report issues, biases, or unintended consequences?	Yes / No	AI Act, Article 62 - Reporting obligations of providers and users
Does the supplier provide updates to address vulnerabilities, regulatory changes, or performance improvements?	Yes / No	AI Act, Article 61 - Post-market monitoring; GDPR Article 32 - Security of processing

b. Reassessment of Risks

Question	Potential Answers	Regulatory Reference
----------	-------------------	----------------------

Are periodic DPIAs and FRIAs conducted to identify new risks or changes in the operational environment?	Yes / No	GDPR Article 35(11) - Data protection impact assessment review
Is the hospital staying informed about changes in laws and regulations that may affect compliance?	Yes / No	N/A (Best Practice)

9. Data Lifecycle Management

a. Data Retention Policies

Question	Potential Answers	Regulatory Reference
Are data retention schedules defined and justified, specifying how long data will be stored?	Yes / No	GDPR Article 5(1)(e) - Storage limitation
Are procedures established for the secure deletion or anonymization of data when no longer needed?	Yes / No	GDPR Article 17 - Right to erasure ('right to be forgotten')

b. Data Subject Rights

Question	Potential Answers	Regulatory Reference
Are mechanisms in place to facilitate data subjects' rights, such as access, rectification, erasure, restriction, and objection?	Yes / No	GDPR Articles 12-22 - Rights of the data subject
Is there a process that allows data subjects to withdraw consent where applicable?	Yes / No / Not Applicable	GDPR Article 7(3) - Conditions for consent withdrawal

10. Ethical Oversight and Governance

a. Ethics Committee Involvement

Question	Potential Answers	Regulatory Reference
Is an ethics committee or board engaged to oversee the AI/LLM solution's deployment and operation?	Yes / No	N/A (Best Practice); AI Act, Recital 70 - Human oversight
Are ethical guidelines developed and updated in response to new challenges or insights?	Yes / No	AI Act, Article 14 - Human oversight

b. Transparency and Accountability

Question	Potential Answers	Regulatory Reference
----------	-------------------	----------------------

Are transparency reports on the AI/LLM solution's use and impact considered for publication?	Yes / No / Planned	AI Act, Article 60 - Transparency obligations
Is there open communication with patients and staff about the system's role and benefits?	Yes / No	GDPR Article 12 - Transparent information; AI Act, Article 13 - Transparency

Alignment with EU Procurement Requirements - Assessment of Compliance:

Adherence to EU Public Procurement Directives

Question	Potential Answers	Regulatory Reference
Does the procurement process emphasize transparency and fairness, ensuring equal opportunity for all qualified suppliers, in line with Directive 2014/24/EU?	Yes / No	EU Procurement Directive 2014/24/EU, Article 18 - Principles of procurement
Are the principles of equal treatment and non-discrimination being followed in the procurement process?	Yes / No	EU Procurement Directive 2014/24/EU, Article 18
Are the requirements proportionate to the objectives, avoiding unnecessary burdens on suppliers, in line with EU procurement principles?	Yes / No	EU Procurement Directive 2014/24/EU, Article 18

Compliance with Legal and Regulatory Frameworks

Question	Potential Answers	Regulatory Reference
Is compliance with GDPR specified for data protection and privacy?	Yes / No	GDPR (Regulation (EU) 2016/679)
Are the provisions of the EU AI Act considered, especially regarding high-risk AI systems in healthcare?	Yes / No / Not Applicable	AI Act, Article 6 - Classification of high-risk AI systems
Is the handling of electronic health data meeting EU standards per EHDSR?	Yes / No / Not Applicable	EHDSR, Article 33 - Secondary use of electronic health data

Ethical and Social Considerations

Question	Potential Answers	Regulatory Reference
Does the procurement include ethical requirements such as data protection by design, transparency, and bias prevention?	Yes / No	GDPR Article 25 - Data protection by design and by default; AI Act, Article 9 - Risk management system

Are environmental sustainability considerations included, reflecting the EU's commitment to green procurement?	Yes / No	EU Procurement Directive 2014/24/EU, Recital 95; Article 68 - Life-cycle costing
--	----------	--

Supplier Qualification and Exclusion Criteria

Question	Potential Answers	Regulatory Reference
Are suppliers evaluated based on their legal compliance, ethical commitment, and technical capabilities?	Yes / No	EU Procurement Directive 2014/24/EU, Article 58 - Selection criteria

Contractual Requirements and Clauses

Question	Potential Answers	Regulatory Reference
Are specific data processing agreements and confidentiality clauses included to ensure legal certainty and protection of sensitive information?	Yes / No	GDPR Article 28 - Processor; EU Procurement Directive 2014/24/EU, Article 21 - Confidentiality
Does the contract include compliance and audit clauses to enforce ongoing adherence to obligations?	Yes / No	GDPR Article 28(3)(h); EU Procurement Directive 2014/24/EU, Article 70 - Conditions for performance of contracts

Risk Management and Impact Assessments

Question	Potential Answers	Regulatory Reference
Are Data Protection Impact Assessments (DPIAs) mandated in line with GDPR requirements?	Yes / No	GDPR Article 35 - Data Protection Impact Assessment
Is the impact on fundamental rights assessed, especially for AI applications, aligning with ethical considerations promoted by the EU?	Yes / No / Not Applicable	AI Act, Article 29 - Fundamental rights impact assessment

Post-Implementation Monitoring

Question	Potential Answers	Regulatory Reference
Is there regular evaluation of the solution's performance and compliance to ensure ongoing adherence to contractual obligations and EU regulations?	Yes / No	AI Act, Article 61 - Post-market monitoring; GDPR Article 24 - Responsibility of the controller

Data Subject Rights and Data Lifecycle Management

Question	Potential Answers	Regulatory Reference
----------	-------------------	----------------------

Are mechanisms in place for data subjects to exercise their rights under GDPR, such as access and erasure?	Yes / No	GDPR Articles 12-22 - Rights of the data subject
Are data retention and disposal policies defined according to data minimization and storage limitation principles under GDPR?	Yes / No	GDPR Article 5(1)(c)(e) - Data minimization and storage limitation

Additional Considerations

International Data Transfers

Question	Potential Answers	Regulatory Reference
Are safeguards in place for any transfer of personal data outside the EU, such as Standard Contractual Clauses or adequacy decisions, complying with GDPR requirements?	Yes / No / Not Applicable	GDPR Chapter V - Transfers of personal data to third countries or international organizations

Incident Response Planning

Question	Potential Answers	Regulatory Reference
Are breach notification procedures developed, including clear timelines and protocols for responding to data breaches or security incidents?	Yes / No	GDPR Article 33 - Notification of a personal data breach to the supervisory authority; Article 34 - Communication of a personal data breach to the data subject

Environmental Sustainability

Question	Potential Answers	Regulatory Reference
Is the environmental impact of the AI/LLM solution considered, promoting energy-efficient technologies where possible?	Yes / No	EU Procurement Directive 2014/24/EU, Article 68 - Life-cycle costing; Recital 95

12 Annex 3: High-level Self-Assessment Questionnaire for Providers Offering AI/LLM Solutions to Public Hospitals in the EU

The following questionnaire seeks to synthetically present the legal and ethical requirements and best practices to be considered by AI/LLM solution providers towards offering them for eventual adoption in a public hospital.

Completion of this self-assessment can guide the preparation of relevant documentation (such as DPIAs & FRIAs) which in turn will facilitate associated certification processes and ulterior viability assessment by the technical, medical, legal and administrative teams of the adopting organization.

1. Legal and Regulatory Compliance

a. General Data Protection Regulation (GDPR) Compliance (technical)

Question	Potential Answers	Regulatory Reference
Have we ensured and documented full compliance with the GDPR, including data protection by design and by default?	Yes / No	GDPR (Regulation (EU) 2016/679), Articles 25, 5(1)(b)(c)
Do we have documented procedures in place for lawful processing of personal data, especially special categories like health data?	Yes / No	GDPR Articles 6, 9
Have we established and documented processes for obtaining and managing consent where necessary?	Yes / No / Not Applicable	GDPR Articles 7, 9(2)(a)

b. EU AI Act Compliance (technical)

Question	Potential Answers	Regulatory Reference
Does our AI/LLM solution comply with the EU AI Act requirements for high-risk AI systems in healthcare?	Yes / No / Not Applicable	AI Act, Articles 6, 10, 14, 15
Have we conducted a Fundamental Rights Impact Assessment (FRIA) if applicable?	Yes / No / Not Applicable	AI Act, Article 29
Does our solution meet international or regional standards for accuracy, robustness, and cybersecurity?	Yes / No	AI Act, Article 15

c. European Health Data Space Regulation (EHDSR) Compliance (technical)

Question	Potential Answers	Regulatory Reference
----------	-------------------	----------------------

Is our solution compliant with EHDSR when handling electronic health data, if applicable?	Yes / No / Not Applicable	EHDSR, Articles 5, 33
Do we facilitate interoperability and secure data exchange according to EHDSR standards, if applicable?	Yes / No	EHDSR, Article 5

2. Ethical Requirements

a. Privacy and Data Protection (technical)

Question	Potential Answers	Regulatory Reference
Have we incorporated and documented privacy-enhancing technologies in our solution?	Yes / No	GDPR Article 25
Do we adhere to data minimization and purpose limitation principles?	Yes / No	GDPR Articles 5(1)(b)(c)
Have we implemented anonymization or pseudonymization where appropriate? Following which standard or technical methodology?	Yes / No	GDPR Article 32(1)(a)

b. Transparency and Explainability (technical)

Question	Potential Answers	Regulatory Reference
Does our AI/LLM provide transparent operations and explainable outputs? Specify	Yes / No	AI Act, Article 13
Have we provided documentation and user guides that clarify how the AI/LLM functions?	Yes / No	AI Act, Article 13(2)

c. Bias and Discrimination Prevention (technical)

Question	Potential Answers	Regulatory Reference
Have we implemented measures to detect and prevent biases in our AI models? Specify	Yes / No	AI Act, Article 10(2); GDPR Article 5(1)(a)
Do we use diverse and representative datasets for training? Specify	Yes / No	AI Act, Article 10(3)
Do we regularly test and audit algorithms for potential biases? Specify the methodology	Yes / No	AI Act, Article 9

d. Consent Management (technical)

Question	Potential Answers	Regulatory Reference
Does our solution include functionalities for managing patient consent? Specify the methodology	Yes / No / Not Applicable	GDPR Articles 7, 9(2)(a)

Can data subjects easily withdraw consent within our system? Specify the methodology	Yes / No	GDPR Article 7(3)
Do we keep records of consents obtained? Specify the methodology	Yes / No	GDPR Article 7(1)

3. Technical and Functional Specifications

a. Interoperability (technical)

Question	Potential Answers	Regulatory Reference
Is our solution interoperable with existing hospital systems?	Yes / No	EHDSR, Article 5
Do we comply with established data standards (e.g., HL7, FHIR)?	Yes / No	EHDSR, Article 5

b. Cybersecurity (technical)

Question	Potential Answers	Regulatory Reference
Have we implemented encryption for data at rest and in transit? Specify	Yes / No	GDPR Article 32(1)(a); AI Act, Article 15(2)
Do we have secure authentication and authorization mechanisms? Specify the methodology	Yes / No	GDPR Article 32(1)(b)
Do we conduct regular security assessments and penetration testing of the solution? Specify the methodology	Yes / No	NIS Directive (EU) 2016/1148

c. Performance and Quality Assurance (technical)

Question	Potential Answers	Regulatory Reference
Does our solution meet defined performance indicators and quality benchmarks? Document and specify	Yes / No	AI Act, Article 15(1)
Have we trained and validated the AI/LLM against relevant, sufficiently representative, complete and to the best extent possible error-free datasets?	Yes / No	AI Act, Article 10(3)
Do we provide evidence of testing and quality assurance processes?	Yes / No	AI Act, Article 11

4. Demonstrating Compliance

a. Certifications and Standards (technical)

Question	Potential Answers	Regulatory Reference

Have we obtained relevant certifications (e.g. MDR, CE, ISO 27001, ISO 13485, EU Data Protection Seal)?	Yes / No	EU Procurement Directive 2014/24/EU, Article 62
Have we prepared technical documentation as required by regulations?	Yes / No	AI Act, Article 11; GDPR Article 30

b. Regulatory Knowledge (organizational)

Question	Potential Answers	Regulatory Reference
Does our organization stay updated on GDPR, AI Act, EHDSR, and other relevant laws?	Yes / No	EU Procurement Directive 2014/24/EU, Article 57
Is regulatory compliance reflected in our organizational policies and procedures?	Yes / No	GDPR Article 24; AI Act, Article 9

5. Ethical Commitment

a. Corporate Responsibility (organizational)

Question	Potential Answers	Regulatory Reference
Have we established clear ethical policies for AI development?	Yes / No	EU Procurement Directive 2014/24/EU, Article 18(2)
Do we engage in corporate social responsibility initiatives?	Yes / No	N/A (Best Practice)
Is there transparency in our operations and decision-making processes?	Yes / No	GDPR Article 5(1)(a); AI Act, Article 13

b. Compliance History (organizational)

Question	Potential Answers	Regulatory Reference
Do we have a positive compliance record without significant regulatory infractions?	Yes / No	GDPR Article 83; EU Procurement Directive 2014/24/EU, Article 57(4)(c)
Have we addressed any past compliance issues with corrective measures?	Yes / No / Not Applicable	GDPR Article 24; AI Act, Article 61

6. Contractual Readiness

a. Data Processing Agreements (organizational)

Question	Potential Answers	Regulatory Reference
Are we prepared to enter into Data Processing Agreements detailing obligations?	Yes / No	GDPR Article 28(3)

Do our DPAs comply with GDPR requirements?	Yes / No	GDPR Article 28(3)
--	----------	--------------------

b. Confidentiality and Security Clauses (organizational)

Question	Potential Answers	Regulatory Reference
Do our contracts include robust confidentiality clauses?	Yes / No	GDPR Article 5(1)(f); EU Procurement Directive 2014/24/EU, Article 21
Have we defined protocols for handling data breaches?	Yes / No	GDPR Articles 33, 34

c. Compliance and Audit Rights (organizational/technical)

Question	Potential Answers	Regulatory Reference
Are we willing to maintain compliance and allow for audits during the contract period?	Yes / No	GDPR Article 28(3)(h); AI Act, Article 23
Do we have procedures to cooperate fully with compliance checks?	Yes / No	GDPR Article 31; AI Act, Article 61

7. Implementation Support

a. Data Governance Assistance (organizational/technical)

Question	Potential Answers	Regulatory Reference
Do we offer guidance on best practices for data management?	Yes / No	GDPR Article 24; AI Act, Article 10
Can we assist clients in setting up data access controls and accountability mechanisms?	Yes / No	GDPR Articles 24, 32

b. Training and User Support (organizational/technical)

Question	Potential Answers	Regulatory Reference
Do we provide comprehensive training materials and sessions for hospital staff?	Yes / No	GDPR Article 39; AI Act, Article 14
Are user manuals and technical support channels available?	Yes / No	AI Act, Article 13(2)

8. Post-Implementation Obligations

a. Monitoring and Updates (organizational/technical)

Question	Potential Answers	Regulatory Reference

Do we have processes for post-market surveillance of our AI/LLM solution?	Yes / No	AI Act, Article 61
Will we provide timely updates to address vulnerabilities or regulatory changes?	Yes / No	GDPR Article 32; AI Act, Article 61

b. Issue Reporting Mechanisms (organizational/technical)

Question	Potential Answers	Regulatory Reference
Have we established channels for users to report problems or concerns?	Yes / No	AI Act, Article 62
Do we respond promptly and effectively to reports?	Yes / No	AI Act, Article 62(2)

9. Data Lifecycle Management

a. Data Retention Policies (organizational/technical)

Question	Potential Answers	Regulatory Reference
Have we defined clear data retention schedules specifying how long data will be stored?	Yes / No	GDPR Article 5(1)(e)
Do we have secure deletion or anonymization processes when data is no longer needed?	Yes / No	GDPR Articles 17, 32

b. Facilitating Data Subject Rights (organizational/technical)

Question	Potential Answers	Regulatory Reference
Do we provide tools and processes for data access, rectification, erasure, and restriction?	Yes / No	GDPR Articles 12-22
Do we ensure timely responses to data subject requests?	Yes / No	GDPR Article 12(3)

10. Transparency and Accountability

a. Transparency Reporting (organizational/technical)

Question	Potential Answers	Regulatory Reference
Do we document data processing activities and decisions related to our AI/LLM solution?	Yes / No	GDPR Article 30; AI Act, Article 11
Are we willing to share relevant information with clients, regulators and stakeholders?	Yes / No	AI Act, Article 60

b. Open Communication (organizational/technical)

Question	Potential Answers	Regulatory Reference
Do we provide clear explanations of AI functionalities to clients?	Yes / No	AI Act, Article 13
Are we responsive to concerns or questions from users and stakeholders?	Yes / No	GDPR Article 12; AI Act, Article 13(2)

11. Additional Considerations

a. International Data Transfers (organizational/technical)

Question	Potential Answers	Regulatory Reference
Have we ensured lawful international data transfers in compliance with GDPR?	Yes / No / Not Applicable	GDPR Chapter V
Do we use Standard Contractual Clauses, Binding Corporate Rules, or valid Certifications for international data transfers (under GDPR Art. 46) where necessary?	Yes / No / Not Applicable	GDPR Articles 46, 47

b. Incident Response Planning (organizational/technical)

Question	Potential Answers	Regulatory Reference
Do we have robust incident response plans for data breaches or security incidents?	Yes / No	GDPR Articles 33, 34
Have we established protocols for detecting, reporting, and managing incidents?	Yes / No	GDPR Article 32(1)(c); AI Act, Article 61(4)

c. Environmental Sustainability (organizational/technical)

Question	Potential Answers	Regulatory Reference
Have we considered the environmental impact of our solution, promoting energy-efficient technologies?	Yes / No	EU Procurement Directive 2014/24/EU, Article 68; Recital 95
Do we implement environmentally friendly practices in development and deployment?	Yes / No	N/A (Best Practice)