

D5.2 DATA MANAGEMENT, GDPR AND ETHICS



Disclaimer

This document reflects only the author's view and the European Commission is not responsible for any use that may be made of the information it contains.

Document Information

Grant Agreement	101202581
Full Title	Waterborne federated systems and models for secure and resilient operations
Acronym	WARRANT
Deliverable	D5.2: Data Management, GDPR and Ethics
Deliverable Due Date	31.03.2026
Deliverable Submission date	31.03.2026
Work Package	WP5
Lead Partner	INLECOM GROUP
Leading Author	Bill Karakostas, Anargyros Mavrakos
Dissemination Level	Sensitive

Document History

Version	Date	Author	Description of change
0.1	31.10.2025	Argyris Mavrakos	Table of Contents
0.2	14.11.2025	Bill Karakostas, Anargyros Mavrakos	20% Draft Ready
0.5	12.12.2025	Bill Karakostas, Anargyros Mavrakos	50% Draft Ready
0.7	09.01.2026	Bill Karakostas, Anargyros Mavrakos	70% Draft Ready
0.7	23.01.2026	Georgia Tsiochantari	Version 0.7 Approved
0.8	06.02.2026	Bill Karakostas, Anargyros Mavrakos	80% Draft Ready
0.8	20.02.2026	Georgia Tsiochantari	Version 0.8 Approved
0.9	06.03.2026	Bill Karakostas, Anargyros Mavrakos	First Complete Draft Ready for internal Review
0.9	20.03.2026	Per Håkon Meland (SD), Gadi Benmoshe (AEL)	Complete Review Received
1.0	31.03.2026	Konstantinos Louzis (NTUA) Georgia Tsiochantari (INLE)	Quality Assurance Manager approval PM approval

Table of Contents

1 EXECUTIVE SUMMARY.....	6
2 INTRODUCTION	7
3 DATA GOVERNANCE, RESPONSIBILITIES	10
4 DESCRIPTION OF DATA GENERATED AND COLLECTED	13
5 FAIR AND OPEN SCIENCE STRATEGY	19
6 GDPR COMPLIANCE AND ETHICS FRAMEWORK	21
7 DATA SECURITY AND INTELLECTUAL PROPERTY	24
8 MONITORING, REVIEW AND UPDATES	27
9 CONCLUSIONS	29
10 ANNEX.....	30
11 REFERENCES	31

List of Figures

FIGURE 1: WARRANT APPROACH TO OPEN ACCESS FOR SCIENTIFIC PUBLICATIONS AND DATA7

FIGURE 2: WARRANT DATA LIFECYCLE 16

List of Tables

TABLE 1: *MAPPING OF WARRANT GRANT AGREEMENT COMMITMENTS TO D5.2 CONTENT..* 9

TABLE 2: WARRANT DATA GOVERNANCE ROLES AND RESPONSIBILITIES..... 11

TABLE 3: WARRANT DATA CATEGORIES 13

TABLE 4: REQUIRED METADATA ELEMENTS FOR WARRANT DATASETS..... 15

TABLE 5: WARRANT DATA SENSITIVITY CLASSIFICATION 15

TABLE 6: *WARRANT DATA LIFECYCLE STAGES* 16

TABLE 7: FAIR PRINCIPLES IMPLEMENTATION IN WARRANT 19

TABLE 8: DATA GENERATED AND FORMAT PER WP 30

Acronyms

AI	Artificial Intelligence
AI	Artificial Intelligence
AIV	Autonomous Inland Vessels
AML	Adversarial Machine Learning
DAMA	Data Management Association
DAL	Design Assurance Levels
DMBOK / DMBOK2	Data Management Body of Knowledge (2nd Edition)
DMP	Data Management Plan
DOI	Digital Object Identifier
DPO	Data Protection Officer
DPIA	Data Protection Impact Assessment
DT	Digital Twin
DTLF	Digital Transport and Logistics Forum
EU	European Union
GA	Grant Agreement
GDPR	General Data Protection Regulation
HAZOP	Hazard and Operability Study
HE	Horizon Europe
HIL	Hardware-in-the-Loop
IACS	International Association of Classification Societies
IEC	International Electrotechnical Commission
IPR	Intellectual Property Rights

ISO	International Organization for Standardization
KG LL	Knowledge Graph Living Lab
LL	Living Lab
MASS	Maritime Autonomous Surface Ships
ML	Machine Learning
MLOps	Machine Learning Operations
OA	Open Access
ORDP	Open Research Data Pilot
PLC	Programmable Logic Controller
RBAC	Role-Based Access Control
ROC	Remote Operations Centre
SCADA	Supervisory Control And Data Acquisition
SRODS	Safe, Secure and Resilient Operations of Digitalized Ships
STPA	System-Theoretic Process Analysis
WDS	Waterborne Digital Systems
WP	Work Package

1 Executive Summary

Deliverable D5.2 “Data Management, GDPR and Ethics” (INLE, M12) establishes the comprehensive governance framework for data management, personal data protection and ethical compliance within the Horizon Europe project WARRANT (Waterborne federated systems and models for secure and resilient operations, Grant Agreement No. 101202581). It operationalises Task T5.3 and Subtasks ST5.3.1-ST5.3.3 by defining structured procedures covering data classification, lifecycle management, FAIR implementation, GDPR compliance, ethical oversight and gender balance monitoring.

WARRANT integrates research, technological development and validation activities conducted within structured Living Labs (LLs). As such, the project generates heterogeneous datasets, including technical research data, software artefacts, operational validation data from Living Labs, stakeholder-related information and administrative records. This deliverable provides a structured categorisation of these datasets and defines proportionate safeguards according to their sensitivity level. In accordance with ST5.3.1, a Data Protection Officer (DPO) appointed at project start oversees compliance with Regulation (EU) 2016/679 (GDPR) and ensures that personal and critical data are processed lawfully and securely. The DPO also supports the implementation of ethical and legal guidelines under ST5.3.2, ensuring alignment with the AI Act, Data Act and Data Governance Act where relevant.

The deliverable integrates Innovation Management and Intellectual Property Rights (IPR) protection with Horizon Europe Open Science obligations. The project follows the principle “as open as possible, as closed as necessary,” ensuring that research outputs are Findable, Accessible, Interoperable and Reusable (FAIR), while safeguarding confidentiality, exploitation potential and personal data protection. Gender balance and inclusiveness are embedded within project governance structures in line with ST5.3.3, with periodic monitoring mechanisms ensuring equitable representation in decision-making bodies and stakeholder engagement activities.

As the first version submitted at Month 12, D5.2 establishes a robust baseline framework for responsible data governance. It will be reviewed and updated as Living Lab activities mature, additional datasets are generated and regulatory developments evolve.

2 Introduction

2.1 Context of the Data Management Plan and the Research Data Pilot

The WARRANT Data Management Plan complies with and aligns to the objectives set by the Horizon Europe programme for responsible data management in publicly funded research. The European Commission has progressively strengthened its requirements for open access to research data, building upon the Open Research Data Pilot (ORDP) introduced under Horizon 2020 and now embedded as a standard obligation within Horizon Europe. The underlying rationale is to balance openness on one side, with protection of legitimate interests on the other, considering commercialisation aspects, Intellectual Property Rights (IPR), privacy concerns and security.

According to the Horizon Europe guidelines for Data Management Plans, the DMP aims to produce data so that researchers may benefit by their use directly, and to apply their methods based on data generated by EU-funded research that are Findable, Accessible, Interoperable and Reusable (FAIR). At the highest level, the context of the WARRANT DMP is set by the EU policy for Open Access (OA), which is about providing online access to scientific information free of charge to the end-user and in a reusable manner. In the context of research and innovation, scientific information refers to research data underlying publications, curated data and raw data.

The WARRANT consortium believes in the concepts of open science and in the benefits that the European innovation ecosystem and economy can draw from allowing the reuse of data at a larger scale. As regards the exploitation and sharing of project data, following the ORDP paradigm, data sharing may be desired and one of the project's means to create interest and to increase its reach and impact. At the same time, this can be restricted where there exists a legitimate reason for a specific dataset, to protect some patentable innovation or results that can reasonably be expected to be commercially or industrially exploited. This case is covered by the Innovation Management related tasks of WARRANT, and such restrictions are recognised within the Data Management Plan.

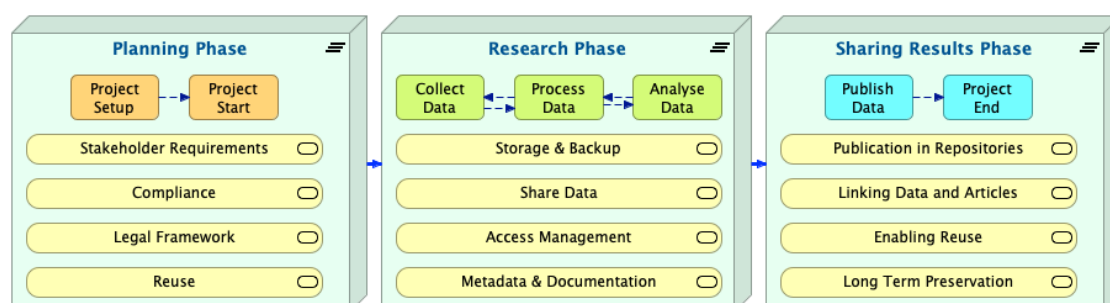


Figure 1: WARRANT approach to Open Access for Scientific Publications and Data

2.2 Overview and Mapping WARRANT outputs

This deliverable, D5.2 “Data Management, GDPR and Ethics” (INLE, M12), establishes the structured framework governing data management, personal data protection and ethical compliance within the WARRANT project. It constitutes the first version of the project’s Data Management Plan (DMP) and defines the procedures and safeguards applicable to all data generated, processed and shared during the project lifecycle, including data arising from Living Lab (LL) activities.

The objectives of this deliverable are to define the categories and characteristics of data generated within WARRANT, establish a clear governance and responsibility model for data handling, ensure compliance with Regulation (EU) 2016/679 (GDPR) and relevant ethical standards, operationalise the FAIR data principles, and align data management practices with Horizon Europe Open Science obligations. Emphasis is placed on Living Lab environments, where real-life validation activities may involve operational data streams and stakeholder engagement.

The preparation of this deliverable is based on inputs from all beneficiaries involved in data generation, system development, integration and validation activities. Contributions were provided by Work Package leaders, Living Lab leaders, technical partners responsible for system architecture and software development, and partners responsible for ethics and data protection oversight. The document reflects the commitments described in the Grant Agreement and the Description of Action (DoA), including the formal description of D5.2 and its associated task(s). It also considers dependencies with other project outputs, such as technical architecture deliverables, Living Lab implementation plans, dissemination and communication strategies, and exploitation and intellectual property management deliverables.

The main results of this deliverable include a structured classification of project datasets, a lifecycle-based data management model, a defined GDPR compliance framework, an ethics governance structure for research and Living Lab activities, defined technical and organisational security measures, and a FAIR-aligned Open Science and data sharing strategy. Together, these elements establish a coherent governance framework ensuring secure, lawful, ethical and impact-oriented data management. D5.2 is closely linked with technical and validation deliverables that define data flows and pilot configurations, as well as with dissemination and exploitation deliverables that regulate open access, intellectual property and access rights. The DMP is conceived as a living document evolving alongside project implementation.

This section maps the commitments described under Task T5.3: Data Management, GDPR and Ethics (Lead: INLE; Partners: ALL; M1-M36) and its associated subtasks in the WARRANT Grant Agreement against the content of this deliverable. The purpose of this mapping is to demonstrate clear traceability between the GA commitments and the structured framework presented herein. Table 1 provides a summary of this traceability, linking each GA component to the relevant sections of this document.

Table 1: Mapping of WARRANT Grant Agreement commitments to D5.2 content

GA Component	GA Description	Section(s)	Justification
D5.2 - Data Management, GDPR and Ethics	Structured framework for data management, GDPR compliance and ethical oversight across project activities.	Sections 1-8	Defines the DMP framework, dataset categorisation, GDPR mechanisms, ethics oversight, FAIR strategy, security safeguards, IPR management and monitoring procedures.
ST5.3.1 - Data Management and GDPR	DMP outlining data types, metadata and representation standards. DPO appointment, GDPR policies, FAIR principles and guidelines.	Sections 3-6	Defines data categories including Living Lab datasets, metadata standards, lifecycle management procedures, FAIR implementation, GDPR safeguards and DPO responsibilities.
ST5.3.2 - Ethics	DPO ethics responsibilities, consent forms for research experiments, alignment with AI Act, Data Act, Data Governance Act.	Sections 6-7	Ethics oversight structure, consent governance in Living Labs, RRI principles, EU regulatory alignment including AI Act and Data Act.
ST5.3.3 - Gender Analysis	Gender balance in decision-making structure, periodic assessment, equal opportunities for all stakeholders.	Sections 6, 8	Gender equality embedded in governance, periodic monitoring mechanisms, corrective actions at Steering Committee level.

3 Data Governance, responsibilities

3.1 Context

The “Data Management Body of Knowledge” V2.0 (DMBOK), published as a set of guidelines by DAMA (the Data Management Association), advances Data Management principles, guidelines, and best practices. DMBOK is a collection of processes, principles and knowledge areas about proper management of data, and can be used to develop strategies for data management, covering Data Architecture Management, Data Development, Database Operations Management, Data Security Management, Master Data Management, Data Warehousing and Business Intelligence Management, Document and Content Management, Metadata Management, and Data Quality Management.

Data Governance is central to all DMBOK-developed concepts and is concerned with planning, oversight, and control over data management and the use of data. Data Governance is responsible for setting policy rules on how data is used for decision making, reference and analysis within an organisation to deliver the overarching organisational strategy. As regards the standards related to Data Governance, the ISO 38505 series of governance of data standards provide guidance for the development of a data governance framework. These standards are centred around a data accountability map that identifies the areas in an organisation where data governance needs to be applied. Using the data accountability map, organisations proceed to develop data related strategies and decision-making models including the value, risks and constraints of data uses.

The WARRANT Data Governance classifies the project data assets based on their characteristics, their origin and use, their related stakeholders, any related restrictions or policies, their content, and their criticality. Furthermore, data quality is an important issue, as all research performed in the technical work packages and the Living Labs success is highly dependent on it. Data governance ensures proper management of important and sensitive data including information related to the Living Lab models and simulations. When necessary, data will be appropriately managed, anonymised, encrypted, and sanitised, whereas risks which may arise upon their access by third parties will be handled accordingly.

within their respective sites complies with the procedures described in this document.

3.2 Governance structure and roles overview

I The WARRANT project establishes a structured data governance framework to ensure that all data generated, processed, stored and shared within the project are handled in a secure, lawful and ethically responsible manner. This framework applies across all project activities, including research and development, system integration, dissemination, exploitation activities and Living Lab (LL) validation environments.

Overall responsibility for the implementation of Task T5.3 lies with INLECOM as task leader, in collaboration with all project partners. The governance structure ensures clear allocation of

responsibilities at consortium level, Work Package (WP) level and Living Lab level. Table 2 summarises the key governance roles and their responsibilities within the WARRANT data management framework.

Table 2: WARRANT Data Governance Roles and Responsibilities

Role	Responsibility	Scope
Project Coordinator	Ensures data governance procedures are aligned with the Grant Agreement and the Consortium Agreement. Overall project accountability.	Consortium-wide
Data Protection Officer (DPO)	Oversees GDPR compliance, advises on lawful processing, reviews data flows in Living Labs, monitors cross-border transfers, coordinates with institutional DPOs.	Consortium-wide
Work Package Leaders	Supervise data-related activities within their WPs, ensuring dataset creation, storage, documentation and sharing follow defined principles.	WP-level
Living Lab Leaders	Oversee data collection and processing within pilot environments, including operational data streams and stakeholder engagement data.	LL-level
Task T5.3 Leader (INLE)	Coordinates DMP implementation, monitors compliance, prepares deliverable updates, liaises between DPO and partners.	Consortium-wide
Individual Partners	Responsible for data they generate or process. Act as Data Controllers, Joint Controllers, or Data Processors depending on activity.	Partner-level

In accordance with Subtask ST5.3.1, a Data Protection Officer (DPO) has been appointed at project start. The DPO is responsible for overseeing compliance with GDPR and ensuring the protection of personal and critical data throughout the project lifecycle. The DPO's responsibilities encompass supervising compliance with Regulation (EU) 2016/679 (GDPR), advising partners on lawful processing of personal data, ensuring that appropriate technical and organisational safeguards are implemented, reviewing data flows within Living Labs to prevent unauthorised access or misuse, advising on the need for Data Protection Impact Assessments (DPIAs) where applicable, monitoring cross-border data transfers if relevant, and coordinating with institutional Data Protection Officers of partner organisations. The DPO acts independently in monitoring compliance and reports to the Project Coordinator and Steering Committee where necessary.

Data Governance in WARRANT serves two primary purposes. First, it provides a mechanism for controlling changes related to the data, data processes, and the data architecture, connectivity, storage, and data sharing. Governance is exercised and monitored by the appointed DPO, and all project partners have full control and decide about how the project data is managed, accessed, stored, and finally, how this data will be disseminated via the ORDP, as this will apply to specific datasets that will be identified. Second, it provides the rules and policies for identifying and handling data related issues, involving the processes, resources, specific content, and related stakeholders. As data can be shared and need to be interoperable, they will have to provide necessary metadata information including the data definitions, data types and change tracking, data compliance, data quality procedures and metrics.

3.3 Alignment With Innovation Management, IPR protection and open science

Data governance within WARRANT is closely aligned with Innovation Management and Intellectual Property Rights (IPR) protection strategies defined in the Consortium Agreement and related exploitation deliverables. Before any dataset is shared beyond the consortium, an assessment is conducted to determine whether the dataset contains confidential or commercially sensitive information, whether intellectual property protection measures are required, and whether personal or critical data are included. The DPO verifies that no personal data are disclosed without lawful basis and appropriate safeguards. This governance mechanism ensures that Open Science obligations are balanced with legitimate IPR protection and confidentiality requirements.

The data governance structure also supports the implementation of FAIR principles and Horizon Europe Open Science obligations. Metadata standards, documentation procedures and repository selection criteria are defined to ensure that datasets intended for sharing are Findable, Accessible, Interoperable and Reusable. However, data openness is subject to compliance checks: before publication or open access release, data sensitivity is assessed, IPR considerations are reviewed, and GDPR compliance is verified. The DPO ensures that personal data are anonymised or pseudonymised where required prior to sharing. There can also be used various techniques and methods to limit restrictions, including the anonymisation of data and the publishing of selected datasets where all important and sensitive information have been neutralised.

Living Labs constitute operational validation environments where real-life data may be generated, including system performance logs, operational parameters and stakeholder engagement data. For each Living Lab, a responsible partner is designated to oversee data flows, data categories are documented, personal data processing activities are identified, and consent procedures are implemented where required. The DPO reviews Living Lab data processing activities to ensure compliance with GDPR and ethical standards, particularly where stakeholder participation or experimental validation activities are involved.

Compliance with data governance procedures is monitored throughout the project. Periodic internal reviews ensure that data processing activities remain aligned with defined purposes, security safeguards are operational, and gender balance and equal opportunity principles are respected in governance structures. The DPO reports significant data protection issues to the Project Coordinator and, where necessary, to the Steering Committee.

4 Description of Data Generated and Collected

4.1 Overview

The WARRANT DMP applies to all data gathered in the Work Packages which develop the framework, the infrastructure and the knowledge hub, which are mostly data about models and processes, and the data from the Living Labs where innovations are being tested. Additionally, there are data and information related to innovation management, dissemination, commercialisation activities and administration. This information is mostly related to Privacy and Information Security Protection, IPR management, and has the form of documents (e.g. emails, presentations, document texts and deliverables), which mainly falls under the domain of GDPR compliance.

Furthermore, to conform with GDPR, mechanisms to protect sensitive information will be established and enforced as part of the data management actions. These mechanisms will be active throughout the project, applying to all activities including data deployment and the application of various algorithms developed in the technical work packages and tested in the Living Lab Application Scenarios.

WARRANT has applied an efficient approach where, during the project data lifecycle, internally data are treated in an organised manner per application need, with every partner keeping a record of the data managed by their activities, while all data definitions are collected by the DMP in the form of a master data management facility. The project has also investigated and detailed the methods and the relevant actions required for the preservation, enhancement and further exploitation of the data collected during the project.

4.2 Data Description, Categories and Stakeholders

WARRANT generates and processes heterogeneous datasets arising from research and development activities, system integration, validation within Living Labs (LLs), stakeholder engagement, project management and dissemination actions. The nature, volume and sensitivity of these datasets vary depending on the specific work package and activity phase. The project research activities both consume and generate datasets for the purpose of performing tasks such as analysis, simulation, experimentation, synthesis, training, test and validation of ship dependability models, concepts and methods. Table 3 provides a structured overview of the five primary data categories within WARRANT.

Table 3: WARRANT Data Categories

Category	Description	Typical Formats	Sensitivity
Technical and Research Data	Simulation outputs, modelling results, algorithm datasets, source code, system architecture documentation,	CSV, JSON, XML, domain-specific, source code, containers, databases	Consortium-restricted or Public

	performance metrics, test and validation datasets, benchmarking results.		
Living Lab Operational Data	System logs, operational parameters, infrastructure performance data, network metrics, sensor measurements, integration outputs, usage metrics.	CSV, JSON, time-series databases, log files	Consortium-restricted; GDPR assessment if identifiable
Stakeholder and Participant Data	Workshop records, survey responses, interview transcripts, feedback forms, usability results, contact details.	DOCX, XLSX, PDF, survey platform exports	Personal data - restricted access
Administrative and Management Data	Contact lists, meeting minutes, internal reports, financial documentation, progress monitoring records.	DOCX, XLSX, PDF, email archives	Personal/Confidential - authorised members only
Dissemination and Communication Data	Scientific publications, conference presentations, public deliverables, website content, social media material.	PDF, PPTX, HTML, media files	Public (after internal review)

Before publication, all dissemination materials undergo internal review to ensure that no confidential technical information is disclosed without authorisation, no personal data are disclosed without lawful basis, and intellectual property protection measures are respected. Datasets released as Open Access are aligned with FAIR principles and Horizon Europe Open Science obligations.

Secondary data users are those entities that are not directly involved in the project but can benefit from the data generated by the project, during its operation as well as after its end. These groups include researchers in ship dependability, ship digital systems and ship cybersecurity; shipping organisations; technical systems and service providers for ships such as system integrators; certification (e.g. classification) bodies; and legislation bodies pertinent to ship dependability matters. Additionally, such datasets can be reused and repurposed in other scientific experiments and studies related to ship dependability concepts, thereby contributing to the broader European research ecosystem.

4.3 Metadata Standards, Classification and Data Volumes

Metadata standards are applied to describe origin, version, ownership, format and intended use of the datasets. For metadata, standards like CWM and DCAT will be employed to facilitate discoverability, portability and reuse. Data standardisation is important and alignment will be sought to relevant domain standards. Every dataset metadata description will include its origin, nature, size and scale, to whom it brings value and how it is used, the method, algorithm and process applied, and integration

and reuse related information such as links to similar datasets. Raw data generated or used by the project must contain at least the metadata elements described in Table 4.

Table 4: Required Metadata Elements for WARRANT Datasets

Metadata Element	Description
Identification	Unique identifier, preferably in the form of a persistent identifier (e.g. DOI) or structured reference
Origin and Ownership	Specification of data source, contact information of administrator/owner, responsible partner
Entity Source	Information about the entity or system that generated the data
Terms of Use and Licence	Applicable terms of use, licensing conditions, access restrictions
Description	Narrative description of the dataset content, scope and purpose
Version and Timestamps	Data management related timestamps, version information, change tracking
Format and structure	Technical format (e.g. CSV, JSON, XML), schema definitions, variable descriptions
Sensitivity Classification	Classification level (Public, Consortium-restricted, Confidential, Personal/Critical)

For governance purposes, datasets are classified into four sensitivity levels, as summarised in Table 5. This classification determines access control mechanisms, storage requirements and sharing conditions. Most technical datasets are classified as consortium-restricted due to intellectual property considerations, or public where explicitly intended for Open Science dissemination. Operational datasets from Living Labs are classified based on content, with non-personal technical operational data typically being consortium-restricted, while data potentially containing identifiable operational actors or logs are restricted and subject to GDPR assessment. Prior to sharing or publication, datasets will be reviewed to ensure that no personal or commercially sensitive information is disclosed, using appropriate anonymisation and obfuscation techniques.

Table 5: WARRANT Data Sensitivity Classification

Level	Description	Access Control
Public	Intended for open access dissemination, aligned with FAIR principles.	Open - deposited in trusted repositories with persistent identifiers
Consortium-restricted	Accessible only to authorised project partners for project implementation.	Need-to-know basis within consortium, controlled by WP leaders
Confidential	Subject to contractual confidentiality obligations and IPR protection.	Restricted to specifically authorised personnel, NDA where required
Personal / Critical	Containing personal data or sensitive operational information requiring enhanced safeguards.	Enhanced access control, encryption, DPO oversight, DPIA where applicable

At Month 12, several Living Lab deployments are still under the initial stages of implementation, and therefore precise data volume estimation remains preliminary. It is anticipated that the largest data volumes will arise from simulation inputs, outputs and validation datasets, Living Lab operational logs, and system performance monitoring data. Due to the type (e.g. images) and method of generation (i.e. high frequency sensor-captured data), it is estimated that the volume of the datasets will be in the region of several hundreds of gigabytes. These estimates will be refined in future updates of this deliverable as pilots mature and detailed dataset inventories are compiled.

4.4 Data Lifecycle Management

WARRANT adopts a lifecycle-based data management approach covering all stages of data handling, from creation or collection to long-term preservation or secure deletion. This approach ensures traceability, integrity, security and regulatory compliance across research, development and Living Lab activities. The data lifecycle, as shown in Figure 2, defines the order of stages a piece of data goes through, from initial generation or capture to its eventual archival or deletion at the end of its useful life.

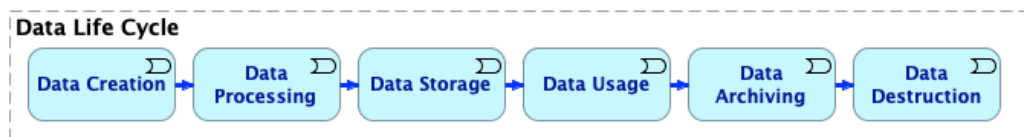


Figure 2: WARRANT Data Lifecycle

The lifecycle stages applied within WARRANT, together with their associated activities, are summarised in Table 6. Each stage is governed by the procedures described below and is subject to the data governance structure defined in Section 3.

Table 6: WARRANT Data Lifecycle Stages

Lifecycle Stage	Key Activities	Responsible
Creation / Collection	Define purpose, identify category and sensitivity, determine personal data involvement, ensure data minimisation.	Technical partners, LL leaders
Documentation / Metadata	Assign structured metadata (Table 4), document origin, version, format, sensitivity, retention period.	Data owners, WP leaders
Storage / Processing	Secure infrastructure, role-based access, encryption, regular backups, pseudonymisation where required.	IT partners, DPO oversight
Sharing / Dissemination	Verify classification, assess IPR, confirm GDPR safeguards, deposit in repositories.	WP leaders, DPO, Innovation Manager
Archiving / Preservation	Long-term deposit in institutional or certified repositories with documentation and metadata.	Data owners, repository operators
Retention / Deletion	Secure deletion at end of retention period, documented destruction, anonymisation where justified.	Data owners, DPO oversight

4.4.1 Data Creation and Collection

Data are generated through technical research and system development activities, simulation and modelling processes, Living Lab deployments and validation experiments, stakeholder engagement actions, and administrative and dissemination activities. At the point of creation or collection, responsible partners must define the purpose of data processing, identify the data category and sensitivity level, determine whether personal data are involved, and ensure compliance with data minimisation principles. For Living Lab activities involving stakeholders or participants, personal data collection is preceded by appropriate information notices and, where required, informed consent procedures, as further detailed in Section 6.

4.4.2 Storage and Secure Processing

Data are stored within secure infrastructures managed by consortium partners, including institutional secure servers, encrypted cloud-based platforms compliant with EU data protection requirements, and access-controlled repositories for software development. Storage environments implement role-based access control, strong authentication mechanisms, encryption for data at rest and in transit where appropriate, and regular backup procedures. Processing activities are limited to authorised personnel based on defined access rights. For datasets classified as confidential or personal, enhanced safeguards apply, including segregated storage environments, pseudonymisation where feasible, and logging and monitoring of access. Where personal data are processed, the DPO ensures that processing remains aligned with the lawful basis and purpose limitation principles. Personal data shall not be transmitted to non-EU countries and consequently cloud computing infrastructure will be based in an EU country.

4.4.3 Data Sharing

The Data Sharing DMP process involves the description of how data is shared, including access procedures, outlines of technical mechanisms for dissemination and necessary software and other tools for enabling re-use, and the definition of whether access is widely open or restricted to specific groups. Within the consortium, data sharing is governed by the Consortium Agreement, Intellectual Property Rights (IPR) provisions, confidentiality obligations and data sensitivity classification. Before sharing data internally, the responsible partner verifies the classification level, IPR implications are assessed, and personal data safeguards are confirmed. Living Lab datasets containing operational or stakeholder-related information are shared internally only on a need-to-know basis.

In line with Horizon Europe Open Science obligations, WARRANT commits to making research outputs openly accessible whenever possible. However, openness is balanced against confidentiality requirements, intellectual property protection, GDPR compliance, and security considerations. Before public release of datasets, data are reviewed for sensitivity, personal data are anonymised or removed, commercially sensitive elements are excluded, and appropriate licensing terms are defined. For the selected shareable datasets to the EU research public, an analysis will be performed to identify data appropriate for the ORDP. Publicly accessible repositories will be considered for storing the results of the project and providing access to the scientific community, such as OpenAIRE and Zenodo.

4.4.4 Data Retention, Archiving and Secure Deletion

According to the WARRANT DMP policies, raw or structured data, imported or generated including their related metadata from the project shall be preserved and archived. Retention periods are determined according to the purpose of data processing, legal and contractual obligations, funding programme requirements, and institutional policies of partners. Technical and research datasets relevant for scientific reproducibility may be retained for extended periods in secure archives. Personal data are retained only for as long as necessary to fulfil the purpose for which they were collected.

Datasets selected for long-term preservation are archived in institutional repositories, certified research data repositories, or trusted digital preservation systems. Archived datasets include sufficient documentation and metadata to ensure interpretability and reusability. The option for long-term preservation of specific datasets will be implemented via external data repositories. The WARRANT DMP information about these datasets will at minimum indicate how long the data of one dataset should be preserved. At the end of their retention period, datasets that are no longer required are securely deleted through permanent removal from storage systems, secure erasure methods preventing recovery, and destruction of physical storage media where applicable.

4.4.5 Risk Management Across the Lifecycle

Potential risks associated with data handling include unauthorised access, accidental loss, data breaches, misuse of personal data, and disclosure of commercially sensitive information. Mitigation measures include access control and encryption, backup and recovery mechanisms, periodic internal audits, breach response procedures, and DPO oversight of personal data processing activities. The consortium implements GDPR-compliant procedures to protect information over time, permitting a broad range of users to easily obtain, share, and properly interpret both active and archived information, ensuring that information is kept up to date in content and format, so it remains accessible and usable.

5 Fair and Open Science Strategy

5.1 Open Science and FAIR Principles

WARRANT is fully committed to the Horizon Europe Open Science principles, ensuring that research outputs are made openly accessible whenever possible, while balancing openness with legitimate constraints related to confidentiality, intellectual property protection, cybersecurity and personal data protection. The project implements a structured approach to FAIR data management, ensuring that datasets intended for sharing are Findable, Accessible, Interoperable and Reusable. At the same time, datasets generated within Living Labs or containing sensitive, personal or commercially exploitable information are subject to appropriate restrictions. Open Science implementation within WARRANT is therefore governed by proportionality: data are made “as open as possible, as closed as necessary.”

The DMP context aligns to the guidelines for the DMPs for projects running under the framework of Horizon Europe, in the direction to support European Research by selectively sharing data with the EU research community according to the FAIR principles. WARRANT aims to align to FAIR, and consequently, the DMP puts an emphasis into the handling of research data, on how such data are generated, collected, processed, shared, and deployed, on the definition of datasets that are shared and made available for open access, and on the methods to be used for data curation and preservation.

Table 7 provides a structured overview of how each FAIR principle is operationalised within the WARRANT project, together with the current implementation status at Month 12.

Table 7: FAIR Principles Implementation in WARRANT

Principle	Implementation Approach	Status (M12)
Findable	Structured metadata (Table 4) assigned to all shared datasets. Persistent identifiers (DOI) via recognised repositories. Public deliverables referenced on project website. Internal catalogue for consortium datasets.	Metadata framework defined; repository selection underway
Accessible	Public datasets in trusted repositories. Consortium-restricted via controlled platforms. Access conditions in metadata. DPO verification before public release. Justified opt-outs documented.	Access classification defined (Table 5); repository agreements pending
Interoperable	Standard formats (CSV, JSON, XML, PDF/A). Structured data schemas for technical datasets. Common vocabularies and domain standards. Documented APIs for software components.	Format guidelines established; domain standard alignment in progress
Reusable	Detailed documentation and methodology descriptions. Quality control before release. Clear licensing (e.g. Creative Commons). Internal documentation for non-sharable datasets.	Licensing framework defined; quality procedures under development

For Living Lab datasets that are eligible for publication, metadata are prepared to ensure traceability without exposing sensitive operational details. Internal consortium datasets are catalogued within project documentation systems to ensure internal traceability, even when not publicly released. Living

Lab datasets intended for reuse are structured to ensure compatibility with relevant technical standards while avoiding disclosure of sensitive operational configurations.

5.2 Open access, repositories and provisions

WARRANT ensures that peer-reviewed scientific publications resulting from the project are made openly accessible in accordance with Horizon Europe requirements. This includes immediate open access through trusted repositories, deposition of the Author Accepted Manuscript or final published version where required, and inclusion of appropriate funding acknowledgements. Publication strategies are coordinated with Innovation Management and exploitation objectives to ensure that intellectual property is protected prior to disclosure. The publication of data within WARRANT is carried out in full alignment with the Intellectual Property and the Innovation Management activities.

Public datasets are deposited in recognised repositories that provide persistent identifiers, ensure long-term preservation, comply with FAIR principles, and operate within the EU or under adequate data protection safeguards. The selection of repositories considers domain relevance, sustainability and accessibility. Publicly accessible repositories considered for storing the results of the project and providing access to the scientific community include OpenAIRE and Zenodo. Advertisement for the data, public distribution, will be disseminated through scientific announcements, papers, and interest groups created by the partners of the project.

Given the operational nature of Living Labs, most LL-generated datasets will remain consortium-restricted due to sensitivity and security considerations. However, aggregated and anonymised validation results may be shared, benchmarking results may be published, and lessons learned and methodological insights will be disseminated. This ensures that Open Science commitments are met without compromising security, GDPR compliance or IPR protection.

In accordance with Horizon Europe provisions, certain datasets may be excluded from open access where disclosure would compromise intellectual property protection, data contain personal information that cannot be sufficiently anonymised, security or critical infrastructure concerns apply, or commercial exploitation would be jeopardised. Such decisions are documented and justified internally, and the DPO is consulted where personal data considerations are involved. After the end of the project, every partner will be able to have a copy of the data produced, per the consortium agreement and specific updates to the access rights of each partner to specific datasets.

6 GDPR Compliance and Ethics Framework

6.1 Legal Framework and GDPR compliance

WARRANT ensures full compliance with Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR) for any activity involving the processing of personal data. This compliance framework applies across all project activities, including research and development, Living Lab (LL) deployments, stakeholder engagement, dissemination actions and administrative management. In addition to GDPR, the project considers relevant national data protection legislation applicable to consortium partners. Ethical and regulatory alignment is further ensured in accordance with the AI Act, the Data Act and the Data Governance Act, particularly where innovative digital technologies and data-sharing mechanisms are involved.

It is essential to consider that the project is being undertaken under a contract with the EC. According to GDPR definitions, the management and processing of personal data should comply with the applicable regulations. Processing shall mean any operation or set of operations which is performed upon personal data, whether by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

Each partner participating in personal data processing activities determines its role under GDPR as either Data Controller (where determining purposes and means of processing), Joint Controller (where purposes are jointly determined), or Data Processor (processing data on behalf of another entity). Role allocation is assessed at activity level, particularly within Living Labs where operational validation may involve stakeholder participation. Where joint controllership applies, arrangements are defined in accordance with Article 26 GDPR, and where processing is delegated, appropriate Data Processing Agreements (DPAs) are established in accordance with Article 28 GDPR.

Personal data within WARRANT are processed only where a valid lawful basis exists under Article 6 GDPR. Depending on the context, lawful bases may include:

- Informed consent (Article 6(1)(a)) - for Living Lab participation, surveys, interviews or experimental validation activities.
- Legitimate interest (Article 6(1)(f)) - for professional stakeholder engagement, where balanced against data subject rights.
- Legal obligation (Article 6(1)(c)) - for administrative or reporting requirements.

Where special categories of data are not intended to be processed, safeguards are in place to avoid accidental collection. The DPO verifies that each processing activity is supported by a clearly documented lawful basis. Personal data collection within WARRANT is strictly limited to what is necessary to achieve defined project objectives. No excessive or unrelated data are collected. Each

processing activity is documented with defined purpose, identified lawful basis, specified retention period, and designated responsible partner.

Where Living Lab activities involve identifiable participants, informed consent procedures are implemented. Consent forms clearly describe the purpose of data processing, specify the categories of data collected, define retention periods, inform participants of their rights under GDPR, and provide contact details for data protection queries. Consent is freely given, specific, informed and unambiguous. Withdrawal of consent is facilitated at any time without negative consequences. The DPO reviews consent templates and ensures compliance with GDPR and ethical requirements.

While in the project context, any collection of personal data might take place through interaction with individuals that may provide personal information during interviews or evaluation sessions, or through collection of data regarding stakeholders in the maritime domain where personal information is recorded. With respect to these cases, participants must be asked to sign a relevant form for their consent, conforming to legal requirements clarifying the intention for the data gathered, describing how the information is used and how the person concerned may review or amend their data. All partners who collect personal data must inform the DPO prior to any data being collected.

WARRANT ensures that data subjects can exercise their rights under GDPR, including the right of access (Article 15), right to rectification (Article 16), right to erasure (Article 17), right to restriction of processing (Article 18), right to data portability (Article 20), and right to object (Article 21). Procedures are established to respond to requests within the legally prescribed timeframes. The DPO coordinates the handling of data subject requests and ensures timely and compliant responses.

Where processing activities are likely to result in a high risk to the rights and freedoms of individuals, a Data Protection Impact Assessment (DPIA) is conducted in accordance with Article 35 GDPR. This may apply particularly where innovative technologies are deployed in Living Labs, systematic monitoring of participants occurs, or large-scale processing of identifiable data takes place. In the event of a personal data breach, partners must immediately notify the Project Coordinator, inform the DPO without undue delay, assess risk to affected data subjects, notify the competent supervisory authority within 72 hours where required, and inform affected data subjects where high risk is identified. All breaches are documented, including root cause analysis and corrective measures.

6.2 Ethics, responsible research and regulatory alignment

WARRANT integrates ethical oversight into its governance framework in accordance with Task T5.3 and Subtask ST5.3.2. Ethical compliance is embedded across research, system development, Living Lab validation activities, stakeholder engagement and dissemination actions. Ethical supervision is coordinated under the responsibility of the Data Protection Officer, who is responsible for identifying, monitoring and managing ethical issues that may arise during project implementation, including reviewing research protocols, assessing ethical risks associated with innovative technologies and ensuring that experimental activities respect fundamental rights and EU regulatory standards.

Ethical risks within WARRANT may arise from deployment of innovative digital technologies within Living Labs, processing of stakeholder-related data, potential bias in algorithmic or data-driven components, unequal participation or representation in validation activities, and misuse or unintended secondary use of collected data. To address these risks, the project applies prior ethical assessment of Living Lab experimental activities, review of data collection instruments, application of data minimisation and purpose limitation principles, documentation of processing activities, and periodic internal review of emerging risks.

In accordance with ST5.3.2, ethical and legal guidelines provided at project start ensure alignment not only with GDPR but also with the AI Act (for AI-based or automated decision-support components), the Data Act (for data access and sharing obligations), and the Data Governance Act (for trusted data-sharing mechanisms). Where digital technologies are deployed within Living Labs, the project evaluates transparency of algorithmic processes, explainability where automated outputs influence decision-making, risk classification under the AI Act if applicable, and responsible data-sharing mechanisms. The DPO monitors regulatory developments and advises the consortium on necessary adaptations to maintain compliance.

WARRANT integrates Responsible Research and Innovation (RRI) principles across project activities, ensuring that technological development aligns with societal values and fundamental rights. Key principles include transparency in data processing and validation activities, accountability in system design and deployment, inclusiveness in stakeholder engagement, sustainability and proportionality in data usage, and continuous reflection on societal impact. Living Lab deployments are conducted in a manner that ensures respect for human dignity, autonomy and privacy.

In line with Subtask ST5.3.3, gender balance and equal opportunity are embedded within the governance and operational structure of the project. The project decision-making structure, including the Steering Committee and other governance bodies, prioritises gender balance in representation. Partners commit to promoting equitable participation in technical activities, Living Lab deployments and stakeholder engagement events. Gender considerations are addressed through periodic assessment of gender balance within governance bodies, monitoring of participation in Living Lab activities, promotion of inclusive language and practices in dissemination, and equal opportunity principles in recruitment and task allocation. Where imbalances are identified, corrective measures are discussed at Steering Committee level.

7 Data Security and Intellectual Property

7.1 Security plan and measures

WARRANT implements a risk-based security framework to ensure the confidentiality, integrity and availability of data processed within the project. Security measures are proportionate to the sensitivity classification defined in Section 4 and are applied consistently across research, development, Living Lab (LL) deployments and administrative activities. Security implementation aligns with Article 32 GDPR (Security of Processing), Consortium Agreement confidentiality provisions, Innovation Management and IPR protection requirements, and Horizon Europe obligations regarding responsible data handling. Security is embedded across the full data lifecycle described in Section 4.

Where appropriate and proportionate to risk, data in transit are protected using secure communication protocols (e.g., TLS/HTTPS), sensitive datasets are encrypted at rest using recognised cryptographic standards, and encryption keys are managed securely with restricted access. Personal and confidential datasets stored within Living Lab environments are subject to enhanced encryption measures where feasible. Access to project data is governed by role-based access control (RBAC) mechanisms, with access rights granted based on role within the consortium, necessity for task execution, and sensitivity level of the dataset. Authentication mechanisms may include strong password policies, multi-factor authentication where available, and secure credential management systems. Access rights are reviewed periodically and revoked when no longer necessary.

Software components developed within WARRANT are maintained using controlled repositories with version control mechanisms, access restrictions, and logging of code modifications. Secure development practices aim to prevent vulnerabilities that could compromise system integrity or expose data within Living Lab deployments. Access to sensitive datasets, particularly those containing personal or operational data, may be logged where appropriate, with monitoring mechanisms helping detect unauthorised access attempts, unusual activity patterns and potential misuse of data.

All consortium members are bound by confidentiality clauses under the Consortium Agreement, applying to confidential technical data, personal data, commercially sensitive information and Living Lab operational configurations. Partners ensure that personnel involved in project activities are aware of confidentiality and data protection obligations. Where relevant, partners provide internal training or guidance to staff involved in personal data processing, Living Lab deployments, and data management and storage activities.

Living Labs may introduce additional operational security risks due to real-world deployment of systems, interaction with external stakeholders, and integration with existing infrastructures. To mitigate these risks, network segmentation may be applied where feasible, test environments are separated from production systems, access to operational systems is limited to authorised personnel,

and sensitive configuration details are not publicly disclosed. Before publishing aggregated results from Living Labs, datasets are reviewed to ensure that no critical infrastructure or sensitive operational information is exposed.

To ensure data availability and resilience, regular backups are performed for critical datasets, backup copies are stored securely, and recovery procedures are defined to restore data in case of accidental loss, corruption or system failure. Backup strategies are proportionate to data sensitivity and operational criticality. In the event of a security incident, partners must immediately contain and assess the incident, notify the Project Coordinator without undue delay, inform the DPO where personal data may be affected, conduct a risk assessment regarding potential impact on data subjects or system integrity, and implement corrective measures to prevent recurrence. Where a personal data breach is confirmed, notification to the competent supervisory authority within 72 hours is required, along with communication to affected data subjects if high risk is identified. All incidents are documented and retained for audit purposes.

7.2 Intellectual Property, Access Rights and Confidentiality

Intellectual Property Rights (IPR) management within WARRANT is governed by the Grant Agreement, the Consortium Agreement and the project's Innovation Management framework. Data governance, exploitation strategy and Open Science obligations are implemented in a coordinated manner to ensure that research outputs are protected where necessary while maximising impact and knowledge dissemination. IPR considerations apply to technical research data and validation datasets, software components and algorithms, Living Lab operational outputs, exploitable foreground results, and confidential information exchanged within the consortium.

Background refers to data, software, tools, methodologies and know-how owned by partners prior to their participation in WARRANT and made available for project implementation. Ownership of background remains with the respective partner, and access to background is granted only to the extent necessary for project implementation under the conditions defined in the Consortium Agreement. Foreground refers to results generated within the project, including software modules and system components, validation datasets and performance results, integration methodologies, aggregated Living Lab outcomes, and documentation and technical deliverables. Ownership of results follows the provisions of the Grant Agreement and Consortium Agreement, and where results are jointly generated, joint ownership arrangements are defined contractually.

Access rights to background and foreground are granted for implementation of project tasks and exploitation of results after project completion, on a need-to-know basis and in accordance with confidentiality and IPR provisions. Before dissemination of project outputs, partners assess whether protection measures (e.g., patent filing, copyright registration, trade secret protection) are necessary. The preferred means through which to protect confidential information exchanged are non-disclosure-agreements (NDAs), and these are included in the Consortium Agreement which has been signed by all partners.

While data exchange is important for the project objectives to be accomplished, the issue of confidentiality is of critical importance to the success of WARRANT. Confidential information within WARRANT includes technical specifications and source code that are not designated as open source, operational Living Lab configurations, commercial strategies, personal data, and enterprise commercial secrets. Such information is clearly labelled where appropriate, stored in secure environments, shared only with authorised personnel, and protected under contractual confidentiality clauses. Disclosure of confidential information outside the consortium requires prior written consent from the owner.

WARRANT balances IPR protection with Horizon Europe Open Science requirements. Before public dissemination of datasets or publications, IPR assessment is conducted, confidential elements are removed, personal data are anonymised or excluded, and licensing terms are defined. Where results are suitable for open release, appropriate open licences are applied. Where datasets cannot be made openly available due to IPR, confidentiality or GDPR constraints, a justified opt-out is documented in accordance with Horizon Europe provisions.

8 Monitoring, Review and updates

8.1 Document updates and continuous improvement

Deliverable D5.2 constitutes the first version of the project's Data Management framework. In accordance with Horizon Europe requirements and Task T5.3, this document is conceived as a living document that evolves alongside project implementation. As research activities progress, Living Lab deployments mature and new datasets are generated, this document will be reviewed and updated to ensure continued compliance with legal, ethical and technical obligations. The WARRANT Data Management Plan is a public document, made to evolve through the project lifespan, capable of capturing and reflecting evolution in the form of dataset updates and changes in consortium policies.

Monitoring of data management, GDPR compliance and ethical governance is conducted through continuous oversight by Task T5.3 lead (INLE), periodic internal reviews within the consortium, Steering Committee discussions where relevant, Living Lab-level monitoring of operational data flows, and documentation of processing activities and dataset inventories. The DPO plays a central role in monitoring compliance with personal data protection requirements and ethical safeguards.

Periodic review of this deliverable will be conducted at major project milestones, upon significant changes in Living Lab configurations, when new categories of data are introduced, and when regulatory developments require adaptation. Reviews assess whether new datasets require updated classification, whether security measures remain adequate, whether GDPR lawful bases remain valid, whether ethical risks have evolved, and whether gender balance commitments are being upheld. The forthcoming monitoring actions will perform detailed analysis per work package for the related datasets, following and complying with the format of the DMP template.

Updates to D5.2 may be triggered by deployment of new technical components in Living Labs, introduction of AI-based or automated decision-support functionalities, expansion of stakeholder engagement activities, changes in data sharing strategy, identification of new ethical risks, personal data breach incidents requiring procedural revision, or amendments to relevant EU regulatory frameworks (e.g., AI Act, Data Act, Data Governance Act). In such cases, appropriate sections of this deliverable will be revised to reflect updated safeguards and procedures.

Given the evolving EU regulatory landscape, particularly concerning digital technologies and data governance, the project monitors developments related to GDPR guidance and supervisory authority decisions, the AI Act, the Data Act, the Data Governance Act, and national data protection legislation affecting partners. The DPO monitors regulatory developments and advises the consortium on necessary adjustments to policies and procedures. Gender balance within project governance and stakeholder engagement is subject to periodic assessment throughout the project lifecycle.

All procedures described in this deliverable are supported by documented internal processes, ensuring traceability of data processing activities, transparency of decision-making regarding data classification

and sharing, and audit readiness in case of review by funding authorities or supervisory bodies. Records of processing activities, consent documentation, DPIAs (where applicable), breach reports and dataset inventories are maintained by responsible partners.

9 Conclusions

Through the structured governance framework described in this deliverable, WARRANT ensures that its data management, GDPR compliance and ethical governance framework remains robust, adaptive and aligned with both project evolution and regulatory requirements. As the first version delivered at Month 12, D5.2 establishes a comprehensive governance baseline that will be refined as Living Lab activities mature and additional datasets are generated. The DMP will define per work package and per Living Lab the related datasets, while the data in these datasets will be cleansed, integrated, and further enhanced and curated to ensure their value and their suitability to be reused in Open Research.

10 Annex

For the WARRANT project, a dedicated ZENODO repository will be established and continuously updated with all relevant outputs. Furthermore, any revisions to the Data Management Plan (DMP) will be included in the second version (D5.3, M36), providing detailed dataset inventories per Work Package and per Living Lab.

The table below provides an overview of the data expected to be generated, including estimated size and format, organised per Work Package.

Table 8: Data Generated and Format per WP

WP	Data generated (& Estimated size of the data)	Format of data
WP1	Hazard and risk analysis data, AI models, ship subsystem models, cybersecurity risk assessment data, results from simulations, and fault injection tests. (1-2 TB)	CSV, JSON, XML, HDF5, Matlab files (.mat), Text Documents (.docx/.pdf) for reports and guidelines, Graph databases.
WP2	Digital twin data, cybersecurity tool outputs, dependability models, identity management data, vulnerability assessment data, and data from federated learning 500 GB - 1 TB)	CSV, JSON, XML, SQL databases, Docker containers for tool deployment, Log files (.log), Graph databases, Text .docx/.pdf).
WP3	LL experimental data, HIL testing data, ship operation logs, dependability performance metrics, data from LLs. (1-2 TB)	CSV, JSON, XML, SQL databases, Excel files (.xlsx), Video recordings (.mp4/.mkv),
WP4	Dissemination materials, publications, stakeholder engagement records, training materials, 100-500 GB)	Text .docx/.pdf), .pptx, Video recordings (.mp4), (HTML/CSS/JS), posts (.json/.csv).
WP5	Project management documents, quality assurance reports, risk management data, GDPR compliance documentation, and ethics records. (50-200 GB)	Text Documents (.docx/.pdf), Excel files (.xlsx), Management databases (SQL), Project management (MS Project, Jira).

11 References

- [1] How to comply with Horizon Europe mandate for RDM. Retrieved from <https://www.openaire.eu/how-to-comply-with-horizon-europe-mandate-for-rdm>
- [2] HORIZON Europe. Data Management Plan Template. Retrieved from https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/temp-form/report/data-management-plan_he_en.docx
- [3] General Data Protection Regulation (GDPR) - Legal Text. Retrieved from <https://gdpr-info.eu/>
- [4] Open Science. Retrieved from https://rea.ec.europa.eu/open-science_en
- [5] DAMA International, Data Management Body of Knowledge (DMBOK2), 2nd Edition.
- [6] ISO/IEC 38505-1:2017, Information technology - Governance of IT - Governance of data - Part 1: Application of ISO/IEC 38500 to the governance of data.