Ploto

D1.2

Data Management Plan

Project name

Deployment and Assessment of Predictive modelling, environmentally sustainable and emerging digital technologies and tools for improving the resilience of IWW against Climate change and other extremes

Horizon Innovation Actions | Project No. 101069941
Call HORIZON-CL5-2021-D6-01

Co-funded by
the European Union

Dissemination level	Public (PU) - fully open
Type of deliverable	R - Document, report
Work package	WP1 – Project Coordination and Ethics Management
Deliverable number	D1.2 Data Management Plan
Status - version, date	Final – V1.0, 28/02/2023
Deliverable leader	DBC
Contractual date of delivery	28/02/2023
Keywords	Data management strategy, FAIR, Data storage, Data processing, Data security, Quality control

Quality Control

	Name	Organisation	Date
Peer review 1	Dimitrios Liparas	INTRA	22/02/2023
Peer review 2	Inke Hussels	RISA	22/02/2023

Version History

Version	Date	Author	Summary of changes
0.1	25/10/2022	DBC	Initial ToC
0.2	09/12/2022	ALL	Updated ToC and first draft version
0.3	15/02/2023	DBC	Complete draft version for internal review
0.4	22/02/2023	INTRA	Internal review updates
0.5	22/02/2023	RISA	Internal review updates
1.0	28/02/2023	DBC	Final submitted version

Legal Disclaimer

The PLOTO project is co-funded by the European Union's Horizon Europe Innovation Actions under grant agreement No. 101069941. The views set out in this deliverable are those of the author(s) and do not necessarily reflect the official opinion of the European Union. The information in this document is provided "as is", and no guarantee or warranty is given that it is fit for any specific purpose. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use made of the information contained herein. The PLOTO project Consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law.

Table of contents

List of tables

List of abbreviations and acronyms

Abbreviation	Meaning
CNN	Convolutional Neural Network
DCAT	Data Catalog Vocabulary
DMP	Data Management Plan
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EC	European Commission
FAIR	Findability, Accessibility, Interoperability, Reusability
GA	Grant Agreement
GDPR	General Data Protection Regulation
IoT	Internet of Things
IRAP	Integrated Resilience Assessment Platform
IWAT	Inland Waterways Assessment Tool
IWW	Inland Waterways
ML	Machine Learning
WP	Work Package

Executive Summary

This deliverable presents the PLOTO project consortium's plan on handling research data during and after the end of the project, the types of data collected, processed and/or generated, the methodology and standards to be applied, sharing or open access and how the data will be curated/preserved in line with the Horizon Europe Guidelines and FAIR (findable, accessible, interoperable, and reusable) principles. The deliverable presents detailed information on the project data lifecycle, privacy, as well as the project's policies for data collection, storage, access, sharing, protection, retention, and destruction.

In more detail, the PLOTO Data Management Plan (DMP) consolidates and structures the project's processes, procedures and activities to support an effective and efficient data management methodology associated to the project schedule, needs and scope. This begins with a detailed examination of the data that are present and relevant to PLOTO activities, WPs, Tasks and pilots, as well as their lifecycle and all other related principles for complying to their FAIR treatment (conventions, openness, metadata, reusability etc.). Following this, the data management is positioned at a high operational layer, clarifying and positioning data management ownerships and responsibilities for each WP leader, partners etc., whilst also defining the data categories and special treatment for each. PLOTO will fully comply with and respect GDPR policies through an agreed holistic policy for handling all data within the project's activities and across the project's WPs and tasks.

1 Introduction

1.1 Document information

The PLOTO Data Management Plan (DMP) is considered as a key element of good data management. This DMP presents a plan for handling research data during and after the project's end, including types of data collected and processed, methodology and standards to be applied, etc. The DMP presents detailed information on the data lifecycle, privacy, and project's policies for the data collection and processing (including storage, access, sharing, retention, destruction) by PLOTO. In particular, as part of making research data findable, accessible, interoperable and re-usable (FAIR), this DMP includes information on:

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

The DMP is aligned with internal ethics for adequate ethical standards and adequate data protection measures. PLOTO collects data (including personal data) from different data sources and classifies the data into the following categories:

- **Qualitative and quantitative research data**, i.e. data from pilots.
- **Administrative data**, e.g. participants details, communications, identity management data.
- **Data from public sources**, e.g. legislation, government guidance, codes of practices, results of ethical horizon scanning.
- **Open-source data collected from publicly available sources.**
- **Publications and dissemination data**, e.g. data related to open peer-reviewed publications, interviews, reports, proceedings, stakeholders, capacity programme, contact details for webinars/workshops, dissemination contacts and enquiries.

The DMP is a living document and will be updated regularly, as new insights on data use are to be expected throughout the project.

The structure of this DMP is oriented towards the template provided by the European Commission:

https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/temp-form/report/data-management-plan_he_en.docx

1.2 Mapping PLOTO outputs

The purpose of this section is to map (Table 1) the PLOTO Grant Agreement (GA) commitments, both within the formal Deliverable and Task description, against the project's respective outputs and work performed.

Table 1: Adherence to the PLOTO GA Deliverable & Tasks Descriptions

PLOTO GA Component Title	PLOTO GA Component Outline	Respective Document Chapter(s)	Justification
DELIVERABLE			
D1.2 - Data Management Plan	DMP initial version (M6) including data definitions, management procedures, GDPR policies (T1.4)	Chapters 2-4	Data management plan as described in the GA, including all project data management procedures, templates, a GDPR policy and FAIR principles.
TASKS			
Task 1.4 Legal and ethical coordination	This task will make sure that all data are handled according to GDPR, while all the corresponding actions are followed, and the relevant procedures are in place towards this direction	Chapters 2-4	The document reports on the potential data assets that can be potentially generated from the PLOTO tasks, the methodology to make these data FAIR, and the way to protect the security and privacy of the data.

1.3 Document structure

The rest of this document is structured as follows:

- Section 2 describes the initial datasets that the project has identified at the beginning of the project.
- Section 3 describes how the project plans to make data FAIR, internally and externally.
- Section 4 defines the internal methods that the project uses to store, exchange, and follow the data.
- Section 5 concludes the document.

2 Data summary

In this section of the Data Management Plan, we define the concepts and purpose of data collection in relation to the working structure of the PLOTO project. After consultation with the leaders of the PLOTO WPs, we have described the following data points:

- Means of data collection.
- Types of data that will be collected (sensor information, source code, etc.).
- Formatting of the actual data.
- Data size and growth rate predictions.
- Data reproduction and re-usability (whenever applicable).
- Data versioning and control to align data following data modifications.
- Data handling software and tools to generate/modify/process.

What follows is a definition of the data that will be created/distributed for each of the PLOTO WPs. These are categorized as:

- Scientific data relating to data from the 3 PLOTO pilot sites.
- Source code and algorithm development and/or training.
- PLOTO project management and project-related documentation, reporting and management files.
- Dissemination and communication documents.

All PLOTO data files may include narrative texts, numbers, images, software codes, audio files, video files, internal/external reports. The structure of this Section complies with the FAIR data management template of the EC (DMP component 1). What follows is a data summary for each of the PLOTO WPs regarding the following:

- Data purpose
- Data format and types
- Re-used Information
- Data origin
- Data size
- Data utility

In the Sections that follow, we define the data collection for each of the PLOTO WPs, as well as the purpose of the data collected and how they relate to the project objectives. After the first round of analysis at the beginning of the project, we identified several potential data assets. These will be the initial input to the continual data management throughout the project. We will not only follow up the collection, storage and sharing of these data assets, but also use them as exemplars for identifying new data assets along the project work.

2.1 PLOTO data lifecycle

In this Section, we are examining the complete information life cycle that will take part in the PLOTO project, considering the diverse stages at which information will be made, overseen or utilized amid the total execution. What takes after is an examination of the information lifecycle as well as the ways to control, oversee and report the related information.

2.1.1 Data Creation/Collection

As implied by the title, this stage includes the data creation and/or collection, as it relates to the various data provided by the PLOTO pilots, as well as the project reports and other documents/spreadsheets. This includes the creation and collection of the data by each respective owner in appropriate formats and layouts that will enable their processing by the other project components/modules. Specific metrics at this stage relate to the following (Table 2):

Table 2: PLOTO Data Creation and Collection Indicators

Performance Indicator	Means of Verification	Target Values
Format	Compliance with existing standards of data exchange.	XLS, XML, etc.
Availability and Readability	Whole package of data available, non-corruption, whole percentage collected.	100% received 100% accessible
Fit for Use	Data follow data compliancy for proper processing and review.	100% usable by intended beneficiary/ies
Consistency and Competences	Data are consistent and complete for the intended purpose.	Including 100% of information for the intended purpose
Relation	Data processing follows a precise relation to their purpose of collection.	100% purpose precision

2.1.2 Data Processing and Analysis

This stage is related to the actual data processing by the various data processors, which are the partners that will be having access to the data for processing or dissemination activities, following the project needs and outcomes. During this stage we need to ensure that the suitable partners can perform data processing in a concise approach to fulfill the PLOTO needs. This stage includes all steps towards data verification, organization, transformation, integration and extraction for the intended use. Data analysis includes all the actions/methodology executed on the actual data that describe existing facts, identify outlines, develop data clarifications, etc. This stage is closely related to the processing stage previously described and forms as a consequent stage. Specific metrics at this stage relate to the following (Table 3):

Table 3: PLOTO Data Processing Indicators

Performance Indicator	Means of Verification	Target Values
Data logic	Data can be and are processed following a concise logic and approach.	New and processed data follow precise data logic
Organization and Utility	Suitable content organization of data under processing.	100% organized data

Validation	Ensuring that the data under processing are correct and relevant.	100% validated and relevant data
Aggregation	Whenever multiple data need to be aggregated ensure that this is done in a concise approach.	100% aggregate-able data
Transformation	Transformation of data to the proper format(s) for processing.	Capability of data for transformation (if needed)
Calibration	Calibration of data for their intended purpose.	Data properly calibrated

2.1.3 Data Publication and Utilisation

Publication of data refers to the capability to share data openly to public, whereas utilization includes the steps towards data sharing (internally to PLOTO). This implies that data should be medium- and agent-independent, making sure that the transfer can be implemented in an automated approach. The purpose of this stage is to ensure that data is shared with the appropriate controlling mechanisms to ensure protection of proprietary data, as well as the data integrity itself. This stage is closely linked to the next stage (data storage and archiving) as far as metadata are related to ensure data searchability (as another feature of the FAIR data treatment). Specific metrics at this stage relate to the following (Table 4):

Table 4: PLOTO Publication and Utilization Indicators

Performance Indicator	Means of Verification	Target Values
Means-independent	Transferring of the data in a means-independent approach.	100% means independent transferability
Security (a)	Data stored in a secure enough repository.	At least access control provided

2.1.4 Data Storage, Archiving and Re-Use

The "storage and archiving" stage is very critical, as it relates to the data access, sharing, storage, archiving (including search capabilities) and re-usage. An important factor here is the updated status of the data so that no newer versions exist (or is clearly indicated if newer versions do exist). This should also involve actions and practices that safeguard data from accidental data losses, corruption and unauthorized access. Data storage and archiving is also strongly linked to data re-usability that is also within the scope of the FAIR data treatment. Specific metrics at this stage relate to the following (Table 5):

Table 5: PLOTO Storage and Re-use Indicators

Performance Indicator	Means of Verification	Target Values
Up to date	Ensuring that the stored data are up to date for the specific purpose and no later version exists.	100% updated
Security (b)	Access control provided.	Access control setup
Retention	Properly setting expiration dates for all data after which the data will be deleted.	Expiration date noted

2.2 Types of data assets

In the following paragraphs, the initial types of data assets identified, as most relevant to PLOTO, are presented.

2.2.1 Research data

Description. The research, development and evaluation activities within PLOTO will involve IoT devices and systems. Data about the IoT system will be collected, such as the architecture and design of the system, the metadata and identity information of IoT devices, the runtime monitoring and feedback from the IoT system, etc.

Why is the data needed? The various types of data from IoT devices will be used by PLOTO partners for the design, implementation and evaluation of trust and identity management techniques. Outside the project, the data can be useful for IoT system designers and researchers as reference for system design or benchmarking.

Data format. JSON and CSV files will be the common format for such data, but other formats will not be excluded.

2.2.2 Stakeholder-related data

Description. Part of the project work will involve end users & system requirements, training material for potential stakeholders, socioeconomic data and surveys/questionnaires. The materials and results will be collected during and after the studies and training courses. No personal or sensitive data will be included in the data assets.

Why is the data needed? The data will be used for the design and development of the PLOTO tools. They will also be the reference for the exploitation and dissemination activities of the project results. For external users, the data can be used for analyzing stakeholder involvement in IoT trust management and for designing cyber-security training courses.

Data format. Data will be stored in their original document format, together with generated PDF files for external distribution.

2.2.3 Project management data

Description. The project management team will reserve important management data, such as deliverables, meeting agenda and minutes, presentations, as well as key decisions.

Why is the data needed? The data will be used as reference for the day-to-day operation of the project.

Data format. Data will be stored as original document files, together with PDF files for external distribution (where applicable).

2.3 Data analysis per WP

This Section details the data summary from the viewpoints of all PLOTO WPs, as far as the following are concerned:

- Purpose of data collection/generation and relation to PLOTO activities.
- Types and formats of data collected/generated.

- Data utility.

Annex 1 provides a list of all datasets currently expected to be collected/generated and utilized in the PLOTO project and their planned accessibility. We recognize that this list will develop and grow as the project evolves.

WP1 – Project Coordination and Ethics Management

WP1 is responsible for the technical and administrative coordination of the project, including quality and ethical activities. These tasks include the creation and processing of various types of documents and files to ensure efficient and effective management of PLOTO. These types of data mainly consist of documents and spreadsheets or presentation files. This mainly includes documents and spreadsheet files for collection and progress/regular reporting (internal and/or to EC) by PLOTO. These are mainly MS Office documents (.doc/.docx, .xls/.xlsx, .pdf, etc.) that are distributed internally to the consortium or sent to the EC in their final version. At the same time, the WP is responsible for managing and processing meeting-related documents, such as meeting minutes and presentations. These files can also be MS Office- (or similar) related documents (.doc/.docx, .xls/xlsx, .pdf, .ppt/.pptx, etc.). All partners are expected to have access to them, but they are always considered as internal documents of the PLOTO consortium (not distributed outside of PLOTO).

Deliverables and different internal reviews are other forms of reports that this WP may be developing and managing/controlling. These documents may be mostly MS office (or related) documents (i.e., .doc/.docx, .pdf etc) and may be taken into consideration as internal or external, relying on their nature described within the PLOTO Grant Agreement.

Patenting files will also be considered as internal documents so they should fall into the above category and type of data. Other files that will be created in the framework of the WP consist of quality management and templates for all the above (and possibly more) purposes. These files will be mainly .doc, .docx, .pdf, .xls, .xlsx, .ppt, .pptx files, created by the quality manager and used and shared by the PLOTO partners.

All related files in WP1 will be stored in the PLOTO repository (PLOTO SharePoint), where all partners have personalised login details and therefore, we consider that access if fully controlled and safe. Links for exchanging these files internally will be circulated via email or the PLOTO SharePoint itself.

WP2 – End-User Requirements and Platform Design

The main objective of WP2 is to produce a list of end-users' requirements, PLOTO systems' specifications as well as the PLOTO integrated platform architecture, which will be the basis for the technical developments in WPs 3-6, as well as for the integration and piloting activities in WP7. The work in WP2 will be user-driven, and accordingly it will start with the analysis of the end users' current practices and needs, followed by the specification of the system requirements, and use cases, and finalized with the specification of the architecture itself. Since this WP constitutes the main interface with all the system stakeholders, its outputs will also be used by WP8, for awareness creation among all stakeholders, as well as for the definition of suitable business strategies.

In the tasks included in WP2, some major datasets are the end users' requirements, the PLOTO system requirements, asset taxonomies and pilot site regional and/or facility socioeconomic data. These include document and numerical data mainly in MS Office format (.doc/.docx, .xls/.xlsx, .pdf, etc.).

WP3 – Atmospheric Forcing Modelling, Weather Now/Fore-Casting and Data Processing

WP3 mainly deals with the reliable quantification and mapping of climate and atmospheric impacts for the targeted PLOTO sites. An optimal set of quantitative primary parameters and derivative impact indicators will be identified to quantify impacts in connection to the specific categories of hazards targeted by the project, including the WMO climate extreme indicators and several hydrological and soil quality indicators.

In the tasks included in WP3, some major datasets include medium- and long-term climate and atmospheric datasets, combined with two-way coupled multiscale numerical modelling systems and techniques. The data formats expected to be used in the relevant tasks are mainly csv, grib2, netCDF, geotiff, json, etc.

WP4 – Vulnerability and Resilience Assessment of the IWW and the connected hinterland infrastructures

The purpose of WP4 is to develop advanced modelling for natural and man-made hazards, design and develop the interfaces for the simulation tools, including hydrological, hydraulic, geotechnical, etc., deliver near-real-time post-event site-specific vulnerability assessment, support Infrastructure resilience assessment, as well as develop model-based organisational resilience and impact assessment.

Some of the datasets involved in WP4 include pilot site seismic hazard scenarios, weather and hydro hazard scenarios, traffic data, socioeconomic data, asset fragility and vulnerability curves. The data types of all different datasets will be text, numerical data and coordinates. The data formats anticipated are HDF5, json, csv and MS Office (.xls/.xlsx).

WP5 – Earth Observation, Sensor Data and Geospatial Services for Increased Resilience of the IWW

The work undertaken in WP5 is to develop an operational IWW corridor monitoring procedure and the connected infrastructure, involving degradation monitoring and damage assessment capabilities. For this purpose, the proposed system will ensure seamless monitoring and damage detection capability between open and closed transport sections, building on sensor-based solutions that will be optimized to the specific corridor/damage type combination.

Necessary input data will come from sources, such as passive, active instruments and satellite images. Data will be coupled with processing and data integration methods, such as Machine Learning (ML) and deep Convolutional Neural Networks (CNN). Taking under consideration that a wide number of datasets will be used in the WP5 tasks, the expected data format will also vary significantly. Some indicative data formats include SAR, shp, tif/png/jpg, Sentinel 1, hdr, etc.

WP6 – IWAT, Decision Support System and Enhanced Visualization Interface

In WP6, the IWAT platform for assessing the resilience of IWW and potential impacts due to various hazards will be developed, based on a modelling and simulation environment. The IWAT platform will support the identification of vulnerable elements and of cost-efficient adaptation measures.

To deliver all the tools and modules in WP6, a lot of datasets will be utilized, from real-time now-casting and forecasting data, current or future inland and other type of land infrastructure information systems (IoT – unattended sensors, systems – UAVs, devices, services) and external information systems, climate data and services, ground and space sensor data, simulated results, etc.

WP7 – On site Integration, Demonstration and Validation Activities

WP7 will ensure the system integration, according to the specified requirements and architecture to ease the development and testing of the PLOTO platform at different levels (functional, integration and system/end-to-end tests), to integrate all software components developed, delivering the produced PLOTO platform for experimental validation in the pilot sites.

The main types of data identified to be used during the implementation of WP7 are the results of the project pilots and the training material, while the expected format of these data will be MS Office documents (.doc/.docx, .xls/.xlsx, .pdf, etc.).

WP8 – Dissemination, Exploitation and Communication Activities

WP8 will ensure scale up through wide dissemination, exploitation actions and capacity building aiming at infrastructure sustainability, organisational development, and human capital development through training on the practical use of the PLOTO platform. A Dissemination and Communication Plan will be created to ensure that the project creates a strong awareness among the target groups and achieves its full potential impact. A strategy to exploit the results (in individual and collective way) and ensure that results are taken up by the relevant stakeholders during and after the project lifetime, will be also developed.

This WP will not produce any technical components but it will produce dissemination documents and will use data and documents generated from the other WPs. The data generated in the project can be grouped into source code, technical documentation, and formal reports. Deliverables and other formal internal reports are another type of data that this WP will create and manage/control. These files will be MS office (or related) documents (i.e., .doc/.docx, .pdf etc) and will be considered as internal or external, depending on their nature and character as defined in the PLOTO GA. The formal reports and deliverables will be stored in the PLOTO SharePoint.

2.4 DMP in PLOTO WPs, WP leaders' responsibilities and allocation of resources

Data management in PLOTO falls under Task 1.4 "Legal and ethical coordination" [M1-M42] (Leader: DBC). This includes the data management life cycle monitoring for all datasets to be collected, processed, or generated by the project. This task is responsible for the Data Management Plan (DMP, D1.2 & D1.3), including and respecting GDPR policies and procedures for personal/sensitive information protection. The plan will cover the rules of handling research data during and after the project, including the characterization of the data that will be collected, processed, or generated. Special attention will be paid to Regulation (EU) 2016/679 on the protection of natural persons with respect to the processing of personal data and repealing Directive 95/46/EC (GDPR).

To ensure compliance with all the previously described data management decisions as they relate to the DMP, the following overall PLOTO measures will apply in PLOTO:

- DBC is the leader of the task on Legal and ethical coordination.
- WP leaders will be responsible for adhering to the specifications above in their respective Work Packages.
- The project manager of each organization will be responsible for the DMP actions and will be accessible by the partner team in case of issues related to DMP.
- Data owners have the ultimate responsibility to comply with the specifics of the PLOTO Data Management Plan, as well as with the related GPDR policies.

- For the overall PLOTO project management activities, INTRA will be responsible for complying with the Data Management Plan.
- The project manager and main contact from each consortium partner should ensure that personnel working on the project have read the PLOTO DMP and apply/exercise all the principles as described in this document.

3 Making data FAIR

The FAIR principles describe how research outputs should be organised, so that they can be more easily accessed, understood, exchanged and reused. Major funding bodies, including the European Commission, promote FAIR data to maximise the integrity and impact of their research investment. Fair data management relates to the EC guidelines on the Data being Findable, Accessible, Interoperable, Reused. The structure of this Section complies with the FAIR data management template of the EC.

3.1 Making data findable

To make data finable within the PLOTO Sharepoint, **naming conventions** are laid out.

For facilitating common browsing and storage in different platforms, no spaces should be used in the document names, and instead the dash character "-" should be used. Project document names must start with the prefix "[PLOTO]" in order to facilitate quick identification and indexing. In particular, the following conventions are mandatory for certain types of documents. Names of deliverable documents should follow the convention:

"[PLOTO] Dw.n – Deliverable Name.vX.Y.ext"

here

- "Deliverable Name" is the name of the deliverable, as indicated in Part A of the GA
- "Dw.n[.m]" is the deliverable number
  - "w" is the WP number
  - "n" is the numbering within the specific WP
- "vX.Y" is the version number
  - "X" is the version
  - "Y" is the sub-version
- "ext" is the file extension pertaining to the format used. It is normally "doc" or "docx" during the preparation period and "pdf" for the formal submitted version

For instance, the name of (the final version of) deliverable D1.2 is

"[PLOTO] D1.2 – Title.v1.0.pdf"

The name of the PLOTO Technical Reports will follow the convention:

- "[PLOTO] TR.ddd – Technical Report Name.vX.Y.pdf"

where "ddd" is a three-digit decimal number that will be assigned automatically to a new Technical Report.

For other types of datasets that are not in the form of a single document, the folder, package, or online repository will follow the naming convention:

- "[PLOTO] Data – Data Asset Name.vX.Y.ext"

3.2 Making data openly accessible

3.2.1 Open Access to scientific publications

In accordance with the Grant Agreement, all peer-reviewed scientific publications related to the results of the PLOTO project will be published as open access.

This includes the obligation to:

- deposit a machine-readable electronic copy of the published version or final peer-reviewed manuscript accepted for publication in a repository for scientific publications, together with the research data needed to validate the results presented in the deposited scientific publication as soon as possible.

Open access to the deposited publication via the repository must be ensured at the latest:

- on publication, if an electronic version is available for free via the publisher, or
- within six months of the publication (twelve months for publications in the social sciences and humanities domains) in any other case.

Open access via the repository on the bibliographic metadata that identifies the deposited publication must be ensured. It must be provided in a standard format and must include:

- the terms “European Union (EU)” and “Horizon Europe”;
- the name of the action, acronym and grant number;
- the publication date and length of the embargo period, if applicable, and
- a persistent identifier.

3.2.2 Open Access to research data

In accordance with the Grant Agreement, research data will be made available to the highest possible extent. The research data will be made available to the project members via the PLOTO SharePoint during the project’s lifetime. After the end of the project, research data will be made available via Zenodo.

- Data from technical research: Data used by the research partners or generated from the research work related to the development and evaluation of the prototype tools will be opened as much as possible.
- Use case-specific data: As it is not yet exactly clear which data will be generated throughout the use cases, at this point it cannot be stated which of the retrieved data will be made publicly available. Some use cases involve (sensitive) personal data, which are protected by the GDPR and therefore, will not be shared publicly or within the entire consortium. Some other data that are sensitive to the business of the use case providers will also be protected.
- Stakeholder-related data: Most of the stakeholder data contain personal information, which is why they will not be made openly available. However, anonymized results from workshops and other stakeholder engagement events will be made openly available through related deliverables.

3.2.3 How will the data be made available?

The data will be made available using Zenodo. Zenodo is an open-access repository developed under the European OpenAIRE program operated by CERN, which provides researchers the sharing, curation and publication of data and software. The OpenAIRE project was commissioned by the EC to support their nascent Open Data policy, by providing a catch-all repository for EC-funded research.

Zenodo allows to create an own collection and accept or reject uploads submitted to it. It is possible to update all research outputs from all fields of science. In the upload form, it is possible to choose between different types of files: publications, posters, presentations, datasets, images, software, videos/audio and interactive materials, such as lessons. Zenodo assigns to all publicly available uploads a Digital Object Identifier (DOI) to make the upload easily and uniquely citeable.

3.3 Making data interoperable

All data will be stored as standard formats (e.g. pdf, doc, JSON, blockchain record, etc.). The documents and reports created by PLOTO will contain the executive summary in the beginning of the document, summarizing the contents, target readers, as well as the expected way to use the document. All source code repositories will contain a README file under the root path, with instructions on how to build, run and contribute to the code base. For other types of data assets, the metadata will be created, using as much as possible the format and vocabularies, as defined in the Data Catalog Vocabulary (DCAT) standard[1].

3.4 Making data re-usable

- **How will data be licensed to permit the widest reuse possible?** The project aims to enable open access to all research data via CC-BY licence. However, as it is yet to emerge which data exactly will be generated by the use cases, this might be adapted throughout the project.
- **When will the data be made available for re-use?** The data will be made available for re-use at the soonest moment possible, however it is not yet clear, when this will be, as it depends on which data will be generated throughout the use cases.
- **Which data quality assurance process will be in place?** Data related to deliverables will go through the same internal review processes and the quality of the data will be part of the criteria for internal review.

[1] https://www.w3.org/TR/vocab-dcat/

4 General Data Protection Regulation (GDPR)

This Section summarizes the GDPR compliancy of PLOTO, as the GDPR was formally introduced in May 2018 and has been applicable in all Member States in the European Union, as well as in the countries in the European Economic Area (EEA).

4.1 GDPR compliancy

Data confidentiality is an overriding concern throughout the PLOTO project and beyond, as the solution to be developed in PLOTO will continue to be used afterwards, to this end PLOTO aims to be fully compliant with the GDPR. All data to be collected from stakeholders in the project will be done in accordance with applicable ethical standards and requirements in the respective countries of the data collection, as well will be processed and handled in a secure way and in line with applicable rules and regulations on privacy and data protection. Table 6 summarises the PLOTO GDPR comliancy matrix where the first column presents the overall data description, in the second column it is determined who has access to the particular data (internal, external to consortium), the third column describes the storage places of the actual data, the intended purpose of data and reasons for keeping is described in the fourth column and finally the duration of stored data (until when they will be kept) is presented in the fifth column.

Table 6: PLOTO GDPR Compliancy

Personal Data Description[2]	Access[3]	Storage[4]	Purpose[5]	Duration[6]
XLS list of PLOTO contacts	Internal to PLOTO (project partners only)	PLOTO Sharepoint (folder: *Contacts Directory*)	PLOTO internal communications	28 February 2026
Meeting related material (agendas, presentations, signature lists, minutes)	Internal to PLOTO (project partners only)	PLOTO Sharepoint (folder: *Meetings - Telcos*)	PLOTO meetings-related	28 February 2026
Workshops/Conferences and Training sessions	Internal and external to PLOTO	PLOTO Sharepoint (folder: *External Events*)	Large event dissemination	28 February 2026

[2] Overall data description.
[3] Determines who has access to the particular data (internal, external to consortium).
[4] Storage places of actual data.
[5] Intended purpose of data and reasons for keeping
[6] Duration of stored data (until when they will be kept).

		LinkedIn, twitter, PLOTO website		
Reporting (C forms)	Internal to PLOTO (project partners only)	PLOTO sharepoint	PLOTO reporting and consolidation of financial reports	5 years after the project end (in case of audit)
Deliverables, internal documents and other PLOTO reports	Depending on deliverable type could be public or consortium restricted	PLOTO Sharepoint (folder: *Submitted Deliverables*)	PLOTO documents and deliverables	28 February 2026
Publications	Internal and external to PLOTO	PLOTO Sharepoint (folder: *WP8 Dissemination, Exploitation and Communication*)	Dissemination and publication of research results	Internal: 28 February 2026 External: Depending on publisher
List of stakeholders (external to PLOTO)	Internal and external to PLOTO	PLOTO Sharepoint (folder: *WP8 Dissemination, Exploitation and Communication*)	PLOTO mass-dissemination, list of potential users, exploitation	28 February 2026

4.2 General Data Protection Policy

4.2.1 Introduction

This General Data Protection Policy (the “**Policy**”) is drafted by INTRA (the “**Project Coordinator**”) with regard to the EU HE Project PLOTO Grant agreement ID 101069941 (the “**Project**”) executed by the list of partners included therein (the “**Project Partners**”) in order to:

- Comply with the policy and legal requirements of the EU General Data Protection Regulation (Regulation EU 2016/679, the “**GDPR**”)[14], as in effect since 25 May 2018;
- Comply with all other applicable national and EU regulations and guidelines on personal data processing;
- Comply with applicable regulations and best practices with regard to research projects within the EU HE Research Programme;

- Raise awareness and improve knowledge among the Project Coordinator, the Project Partners, as well as their employees and/or agents and/or contractors (collectively, the "**Policy Recipients**").

Because the field of data protection is a dynamic legal field of constant change, new developments, in the form of new regulations, official reports and/or guidelines, are issued by EU and national legislators, as well as competent national authorities at a constant pace. In this context, this Policy may need to be periodically updated by the Project Coordinator, in order to remain relevant to legislative change. Accordingly, Policy Recipients will be duly informed, and will be asked to provide their renewed consent upon any such updates.

4.2.2 Definitions

For the purposes of this Policy the GDPR definitions, as set in Article 4, apply. In addition,

"**Personal data**" means any information relating to an identified or identifiable natural person that is processed by any Project Partner and Policy Recipient during execution of the Project.

"**Controller**" means the owner of the personal data (usually the creator of the data itself), unless otherwise expressly clarified in this Policy or elsewhere in Project deliverables and/or reports.

"**Processor**" means each Project Partner, unless otherwise expressly clarified in this Policy or elsewhere in Project deliverables and/or reports.

"**Consent**" of the data subject means any freely given, specific, informed, unambiguous and **in writing** indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

"**Supervisory authority**" means the competent Data Protection Authorities within the Project Partners' jurisdictions.

Aim of the above definitions is to particularise and complement the definitions of Article 4 of the GDPR. Policy Recipients are advised to consult both texts in order to formulate the applicable definitions each time.

4.2.3 Policy Scope

The Controller determines in advance what is the law applicable to the processing of personal data in a particular case, considering that according to EU law such determination comes from legal principles and cannot be derogated by the parties.

4.2.3.1 Establishment

Each Project Partner is established on the territory of EU Member States. In the event of any change in establishment, the respective Project Partner shall notify the Project Coordinator duly and in writing.

Unless otherwise expressly specified, each Project Partner is considered the controller in that Member State.

4.2.3.2 Processor outside the EU

In the event of any subcontracting to an organization not established on EU territory (such as subsidiaries pertaining to the same corporate group) that processes personal data of people staying on EU territory, on behalf of a Project Partner, that organization qualifies as Processor and ensures the fulfilment of the obligations imposed by the GDPR for that specific part of processing.

4.2.4 Personal data processing

4.2.4.1 Personal data

Personal data means any information relating to natural persons, which is or can be identified, even indirectly, by reference to any other information including a personal identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of data

Special categories of personal data include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or data concerning a natural person's sex life or sexual orientation as well as the processing of genetic data and biometric data for the purpose of uniquely identifying an individual.

In the event of such processing the Controller and/or Processor respectively comply with specific rules related to the processing of such data of special categories, as collecting specific informed consent from data subject and applying stricter safeguards.

When the Controller and/or Processor relies on data subject's consent as a legal ground for processing special categories of data, it will meet all legal consent requirements; otherwise, they are only processed if and to the extent it is based on one of the legal grounds listed in the GDPR for the processing of such data.

Data anonymization

Whenever possible, including non-detrimental to Project execution purposes, Controller and Project Partners shall undertake efforts to keep personal data processed by them for Project purposes anonymous or pseudonymous.

According to the GDPR, "*anonymous information*" is information which does not relate to an identified or identifiable natural person, or personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. In this context, the GDPR does not apply to the processing of such anonymous information, including for statistical or research purposes.

Similarly, "*pseudonymisation*" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Newsletters, social media and other dissemination material

Unless otherwise expressly specified in Project contract, Controller shall be responsible for the personal data processing carried out for Project dissemination purposes. To this end, Controller shall:

- Collect and keep all relevant personal data (including lists of contact details), or copies thereof;
- Monitor relevant communications;
- Address to Project Partners instructions and guidelines on Project dissemination activities (including any EU or other state guidelines, whenever available);
- Inform Project Partners of any policy or legal requirements reviews and changes.

4.2.4.2 Personal data

Minors

Processing of children's personal data requires a special legitimate basis. In the event of such processing the Controller shall be informed in advance and in writing by Project Partners.

4.2.4.3 Data processing

Data processing means any operation, or set of operations, carried out with or without the help of electronic or automated means, concerning the collection, recording, organization, keeping, interrogation, elaboration, modification, selection, retrieval, comparison, utilization, interconnection, blocking, communication, dissemination, erasure and destruction of data whether the latter are contained or not in data bank.

4.2.4.4 Principles for legitimate processing

European Union data protection law set forth the following specific principles which have to be complied with for the processing to be legitimate.

Pertinence and necessity - The Controller should implement management practices to fulfil the obligation to collect only relevant and necessary data for a specified purpose.

Purpose limitation - Personal data is collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. The Controller has a clear overview of all purposes for which personal data is processed. Personal data is not processed for purposes besides the original purposes, unless the (secondary) use is compatible.

Data minimization - Personal data collected by the Controller must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are collected and further processed; if the same purposes can be realized in a less data intensive way a preference is given to that method.

Data update - Personal data is accurate, and, where necessary, kept up to date. Every reasonable step is taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Data retention - Personal data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. The Controller and/or Processing concerned should have processes and policies in place to:

1. determine what the applicable (minimum and maximum) retention periods are for the personal data that is being processed;
2. ensure that relevant retention periods are monitored.

4.2.5 Data protection legal roles

4.2.5.1 Controller

By determining the purposes and means of the processing of personal data, unless otherwise expressly specified in this Policy, the Controller is considered by law as the "Controller" and it is the primary target of the provisions of the law.

Identification

The data controller previously identifies itself as such and ensures an effective implementation of data protection measures in order to comply with the principle that personal data are processed fairly and lawfully. The legal role of controller implies specific responsibilities because provisions setting conditions for lawful processing are essentially addressed to the controller.

Accountability

The GDPR provides full accountability of the company/controller regarding the compliance of its processing of personal data with the law. To ensure the effectiveness of that obligation, it prompts the Controller to follow an overall approach, achieving a genuine system of control and management of its pertinent information. So, accountability and compliance system are elements of the framework for the protection of personal data, in the cause / effect relationship: to be compliant and able to prove it (accountability), the Controller needs to put in place a comprehensive compliance system.

Data protection by design

The Controller considers data protection issues from the outset and from the design of the Project, within the whole lifecycle of processing, in order to manage the issues in a proactive way, to reduce costs and improve efficiency.

Data protection by default

The Controller standardizes data protection principles in personal data processing, products and services. The measures adopted ensure that:

- personal data is processed for purposes not different from the original purposes,
- only data necessary for these purposes are collected, and
- data are not disclosed without human intervention.

4.2.5.2 Joint controller

If at any time during Project execution the Controller processes personal data in conjunction with a third party, by jointly determining the purposes and means of the processing, they both act as joint controller. Both joint controllers determine the mutual responsibilities with a specific arrangement.

4.2.5.3 Processor

Unless otherwise specified expressly in this Policy, all Project Partners act as Processors during Project execution.

A processor processes personal data on behalf of the Controller – that is, the Controller delegates all or part of the processing activities to them. In such event the Project contract assumes the role of the relevant required written agreement as per GDPR requirements.

The processor warrants that it shall provide sufficient guarantees to ensure compliance with the GDPR, has implemented appropriate controls to meet data protection requirements defined by the agreement, instructions and/or legal requirements and ensures the protection of the rights of data subjects.

Auditing

The Controller ensures the commitment of the Processor(s) to enable and contribute to any review activities, including inspections, conducted by the Controller or other (EU authorities') auditors and/or reviewers, as appropriate.

Security

Each Project Partner undertakes that it adopts appropriate security measures to ensure the security, integrity and confidentiality of personal information and electronic communications at an adequate level with regard to Project purposes, and at any event at no lower lever than processing of similar data within its own organisation.

4.2.5.4 DPO

Whenever required, following applicable GDPR and Member State respective legal requirements, the Controller and each Processor, may designate a Data Protection Officer ("DPO") for assistance in monitoring internal compliance with the GDPR.

Identification

Each Processor appoints a DPO in accordance with the criteria and the requirements set forth in the GDPR, as applicable to it. In such event, it shall notify the Controller in writing accordingly.

Designation compulsory vs. voluntary

Each Processor documents the reasons supporting the designation of the DPO or, rather, the reasons why such designation is deemed not necessary. This documentation forms part of the data protection documentation system of that Processor.

Professional requirements

The DPO has sufficient authority, professional qualities and independence to ensure success in his role, according to the GDPR provisions.

Tasks

The organization assigns to the DPO at least the tasks listed in the GDPR.

Notification to Supervisory Authority

Whenever a DPO is appointed, the organization notifies the Supervisory Authority of such designation and publishes DPO's contact details.

4.2.5.5 People in charge of processing

Individuals who process personal data under the authority of the Controllers or Processor(s) must receive specific formal instructions. Hence, the Controller gives specific instructions, relating also to the implementation of security measures and safeguards, to all its personnel in charge of processing personal data.

Training and awareness

All Project Partners’ employees should be well informed and aware of data protection implications and be able to carry out their obligations in their work. A data protection education and communication program should be in place and supported by a monitoring system that confirms all employees and/or contractors are appropriately trained on their data protection responsibilities.

Policies and procedures

Data protection policies and procedures exist, are documented in writing, are formally approved by management, implemented, reviewed, updated and approved when there are changes to applicable laws and regulations.

All Project Partners understand, and the Controller may ask them to overview all their personal data processing, the data protection risks and the applicable rules and procedures. In such event, they shall provide it with all requested information to the best of their ability without undue delay.

4.2.6 Notice and consent

4.2.6.1 Notice

Each Controller and/or Processor, as appropriate, provides the information required by law to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

The data protection notice informs data subjects about the processing of personal data relating to them, even when the personal data is not collected from them as well as of their rights, in order to let them verify in particular the accuracy of the data and the lawfulness of the processing.

4.2.6.2 Free and informed consent

Personal data is processed if and to the extent that the data subject has given valid consent to the processing for one or more specific purposes, or another legal basis for processing exists.

Systems or applications are able to document the explicit consent of the data subject so that it can be evidenced at any time.

Other legal grounds for a legitimate personal data processing are the following:

- performance of a contract;
- legal obligation;
- vital interest of data subject;
- public interest;
- legitimate interest of the controller or third party.

If "legitimate interest" is used as a basis, the interests that have preceded to the decision, need to be documented as well as any possible mitigating measures which will be taken to be able to proceed with personal data processing based on the defined interests.

4.2.6.3 Withdrawal of consent

Data subject’s consent can be withdrawn at any time; even though it will not affect the lawfulness of processing based on consent before its withdrawal.

4.2.7 Rights of data subjects

The individual whom the data refers to (data subject) is entitled with specific rights set forth by the law. The GDPR requires that each Controller and/or Processor, as appropriate, must facilitate the exercise of the data subject’s rights, take action on the request within a specific time frame and must communicate the information requested in an intelligible and easy to access form.

4.2.7.1 Right of accessdrawal of consent

Any individual must be able to exercise the right of access to data relating to him which are being processed.

4.2.7.2 Right to rectification

Each Controller and/or Processor, as appropriate, should have a procedure in place for data subjects to request rectification of their personal data. The procedure specifies in which cases rectification is legitimate.

If a data subject’s request for rectification is legitimate, this is executed across all relevant data storage facilities, including those managed by third parties.

4.2.7.3 Right to erasure

Each Controller and/or Processor, as appropriate, should have a procedure in place for data subjects to request erasure of their personal data. The procedure specifies in which cases erasure is legitimate.

If a data subject's request for erasure is legitimate, this is executed across all relevant data storage facilities, including those managed by third parties.

4.2.7.4 Right to restriction of processing

Each Controller and/or Processor, as appropriate, should have a procedure in place for data subjects to request restriction of processing of their personal data. The procedure specifies in which cases restriction is legitimate.

If a data subject's request for restriction of processing is legitimate, this is executed across all relevant data storage facilities, including those managed by third parties.

4.2.7.5 Right to data portability

Each Controller and/or Processor, as appropriate, determines which processes are subject to the right of data portability as well as when the requirements for such right are met.

Data subject can request the organization to receive a machine-readable copy of the personal data the organization holds about them and where possible, enable the transfer of this data to another data controller.

Portability right can be exercised when:

- processing operations are based on data subject's consent or on contract
- personal data concerns the data subject and are the same that the latter has provided to the organization
- the right does not adversely affect rights and freedoms of others
- the processing is carried out by automated means.

Each Controller and/or Processor, as appropriate, implements appropriate measures and procedures to provide data subject, who is entitled to, with a structured, commonly used and machine-readable copy of the personal data it holds about him and where possible, to enable the transfer of this data to another data controller indicated by data subject.

4.2.7.6 Right to object

Where personal data are processed for scientific or historical research purposes or statistical purposes, the data subjects have the right to object on grounds relating to their particular situation (unless the processing is necessary for the performance of a task carried out for reasons of public interest). The right to object is explicitly brought to the attention of the data subject at the latest at the time of the first communication with the data subject, presented clearly and separately from any other information. Measures should be in place to assess such objections and to ensure that such processing ceases when the request is legitimate and needs to be respected.

Data subjects have right to object, on request and free of charge, to the processing of personal data relating to them for purposes of direct marketing.

4.2.7.7 Automated decision making

Data subject has the right to object to any automatic decision-making (including profiling).

Each Controller and/or Processor, as appropriate, will have determined which processes entail automated decision-making (including profiling) and will have established measures to allow data subjects to object to such automated decision making and profiling. Suitable measures are in place to safeguard the data subject's rights and freedoms and legitimate interest, at least the right to obtain human intervention on the part of the Company/controller, to express his or her point of view and to contest the decision.

4.2.7.8 Timely response to exercise of rights

Each Controller and/or Processor, as appropriate, must confirm to data subjects without delay whether data relating to them are processed and communicate the data to them in an intelligible form. Each Controller and/or Processor, as appropriate, should implement internal procedures in order to be able to provide a timely response to the requests of data subject for the exercise of his rights.

Measures have to be implemented in a way that effectively allows an individual to exercise his or her right to personal data, and that enables Each Controller and/or Processor, as appropriate, to respond to such request appropriately within the required timeframes.

Notification to recipients

In case of a legitimate exercise of rights to rectification, erasure or restriction of processing recipients of the personal data should be informed of the rectification, erasure of that data or of the restriction of processing.

Each Controller and/or Processor, as appropriate, should have a procedure in place for communicating any rectification or erasure of personal data or restriction of processing to the recipients to whom the personal data has been disclosed and for disclosing these recipients to the data subject, if so requested.

4.2.8 Data protection documentation system

4.2.8.1 Register of processing

Each Controller and/or Processor, as appropriate, regarding their processing activities must set up a relevant record, maintained in writing (including in electronic form) and made available easily and swiftly to the supervisory authority on request, as per applicable legal requirements within their respective Member States. The record of processing activities shall contain all the information required by GDPR.

Consequently, the Controller shall have an up-to-date overview of all personal data processing activities and shall maintain records within the Project, that meet the legal requirements posed by the GDPR. By so doing, the Controller will be able to demonstrate compliance to any Supervisory Authority or other state or EU authority concerned.

For the avoidance of doubt, each Project Partner carries the same responsibility above within its own respective organisation.

4.2.8.2 Register of data breaches

A specific register where the breaches have to be recorded together with other information specified by the law, must be maintained by the Controller and shown to the Supervisory Authority upon request. This register is an important element of the data protection documentation system.

Project Partners need to notify immediately and in writing the Controller of any personal data breach within their respective organisations that affects execution of the Project in any way, and to cooperate with the Controller while applying relevant GDPR legal requirements.

4.2.9 Data protection assessment

4.2.9.1 Assessment

In the event that a Data Protection Impact Assessment (“DPIA”) is carried out under the Project, the Controller shall ensure that personal data receives the appropriate level of protection in accordance with the assessed data protection risk.

The decision whether to carry out a DPIA under the Project, unless undertaken in respective Project contract, will be made by the Controller upon prior written consultation with the Project Partners.

Adequacy of protection

The Controller, assisted by Project Partners, should have a process in place in order to assess for all processing the risks of varying likelihood and severity for the rights and freedoms of natural persons, taking into account the nature, scope, context and purposes of personal data processing.

Impact assessment in case of high risk (DPIA)

When the preliminary assessment highlights that processing represents high risks, a formal and documented DPIA is carried out by ascertaining possible impact on data subject.

DPIA is conducted in such a way to meet all the requirements set forth by the GDPR (art. 35) in order to confirm the quality and validity of the findings.

Prior consultation to Supervisory Authority

The Controller has a process in place and roles are assigned in order to ensure that when a DPIA determines that the processing represents high risks, the competent Supervisory Authority is consulted prior to the processing.

4.2.10 Technical and organizational measures

The Controller and each Project Partner, as appropriate, adopts appropriate technical and organisational measures with regard to Project execution (the “Measures”), and reviews and updates them where necessary, to ensure and to be able to demonstrate that processing is in compliance with GDPR.

Each Project Partner shall notify relevant Measures to the Controller in writing. In the event of any queries or further requests by the Controller, each Project Partner undertakes to address them duly and in writing.

In the event that any Project Partner has notified the Measures to its competent Supervisory Authority, it shall inform the Controller thereof, and shall provide respective copies thereof.

4.2.11 Data breach

According to GDPR, the Controller and/or Processor, as appropriate, has to implement adequate Measures in order to prevent personal data breaches.

In addition, the Measures should be able to minimize the adverse effects, in case a security breach to personal data relating in any manner to the Project occurs anyhow.

Should a data breach occur, GDPR sets forth that the Controller and/or Processor, as appropriate, has to notify it to the Supervisory Authority providing specific information, without undue delay and in any case no later than 72 hours from the time of knowledge.

When the breach leads to significant risk of serious adverse effects on the data subject(s) or serious adverse consequences for the protection of personal data, also the latter must be informed without undue delay.

4.2.12 Data transfers to third countries

No international transfers of personal data are expected to take place under the Project.

In the event that any Project Partner wishes to carry out such personal data processing in a third country, it shall notify the Controller in writing and in advance. Unless otherwise expressly specified, any international data transfers carried out by any Project Partner for any reason during Project execution take place at its own exclusive liability and responsibility; same Project Partner shall hold all other Project Partners (including the Controller) harmless from any legal or other claims arising for such personal data processing.

4.2.13 Data transfers to third countries

In case of violation of data protection principles and rules, each Project Partner (including the Controller) is responsible for damages and is subject to sanctions. Possible violations may involve civil liability and sanctions in order to ensure that any relevant damage is compensated.

The Project Partner (including the Controller) that is liable for said damages and/or sanctions shall hold all other Project Partners harmless from any claims, costs, and expenses arising from relevant GDPR infringement.

4.2.14 PLOTO Repository Personal Data Protection and Privacy policy

The following Personal Data Protection and Privacy Policy is uploaded onto the Project website and Sharepoint:

1. Introduction. This Personal Data Protection and Privacy Policy (the “**Policy**”) aims at providing details of the processing, and related methods of use, of personal data referred to users/visitors (the “**User(s)**”) of this website that can be reached at the address [teamwork.com] (the “**Website**”).

This Policy refers to EU Project [PLOTO, 101069941], (the “**Project**”).

Web users and visitors are recommended to read carefully this Privacy Policy before sending any personal information and/or filling in any electronic form posted on this website.

This information is given in accordance with applicable EU data protection law, in particular the EU General Data Protection Regulation, and EU applicable Privacy law.

2. Controller. The Controller is the actual data owner per data case i.e., it is expected to be an PLOTO partner that has full ownership or is the creator of the dataset.

3. Scope. This Policy covers this web site only, and no other personal data processing under the Project or any other websites owned or run in any manner by the Controller or Project Partners.

4. Policy and information notice. This site has been designed with the main function of providing information on the activities of the Project. Therefore, in most cases, the collection of the user's personal data is not required.

In certain instances, such as the "newsletter" section and in order to allow the transmission of our newsletter, the interested user is required to fill out a data collection form. In these cases, the user is always free to provide his/her own data and consent to relevant processing. We recommend reading this Policy before providing the data.

In addition, should it be necessary in limited cases to collect personal information for other purposes, this will be clearly shown in the information privacy notices required by law, in order to enable transparency and user awareness. Consent forms and other documentation will be used each time, as appropriate.

The above information aims to define limits and methods of personal data processing of each service, according to which the visitor can freely express his consent and eventually allow the collection of data and its subsequent use.

5. Traffic data. The computer systems and software procedures used to operate this website acquire, during their normal operation, some personal data whose transmission is implicit in the use of Internet communication protocols.

This category of data includes: IP addresses, browser type, operating system, the domain name and website addresses from which you are logged in or out, the information on pages visited by users within the site, the time of access, time period of user's staying on a single page, the internal path analysis and other parameters regarding the user's operating system and computer environment.

This technical / IT data is collected and used only in an aggregated and not immediately identifiable manner; they could be used to ascertain responsibility in case of hypothetical crimes against the site or upon public authorities' request.

6. Cookies. No cookies are used by this repository.

7. Redirects to other websites. From this website, you can connect through special links to other websites of Project Partners within the Project, or of third parties as applicable each time. Controller hereby assumes no responsibility regarding the possible processing of personal data by third-party sites and in respect of the management of authentication credentials provided by third parties.

8. Purposes of processing and data retention. The processing of personal data is carried out mainly by using electronic procedures and media for the time strictly necessary to achieve the purposes for which the data were collected. The User, however, has the right to obtain the cancellation of his data for legitimate reasons.

9. Optional supply of personal information. The supply of personal data required from the User, unless otherwise noted, is optional, but in case of refusal it could be impossible to fulfill the request, or the related activity mentioned.

10. Place of personal data processing. Data processing related to web services of this website takes place, unless otherwise expressly stated, at Controller's establishment, which provides for the corresponding repository management. Personal data are only handled by technical personnel of the Controller, specifically in charge of processing, or others charged with occasional maintenance operations. These persons have received specific instructions on the confidentiality of this data.

11. Scope of data flow and dissemination. The data may be used by Controller and/or Project Partners' employees, as persons in charge of processing, to whom appropriate operating instructions have been given, as well as by third parties who perform operating activities on behalf of them and who act as data processors, in order to fulfill contractual obligations with regard to the Project. Personal data are not disseminated to unspecified recipients. Detailed information on the names of the data processors can be requested by writing to the project coordinator.

12. Data protection rights. With regard to the processing of personal data, User has the right, at any time, to obtain confirmation of whether or not the data exists and to have it communicated to him/her in an intelligible format. Users also have the right to know the content and the origin of the data, to check its accuracy or to ask that it be integrated, updated or adjusted. Finally, Users have the right to ask that the data be deleted or made anonymous or to request the blocking of data processed in violation of the law; moreover, they may oppose the processing of the data for legitimate reasons. Requests should be addressed to the project coordinator.

13. Policy updating. The possible entry into force of new laws, as well as the evolution and updating of User services or developments in the Project could make it necessary to vary the method of processing of personal data. It is therefore possible that our policy may be modified over time and therefore we invite the visitor to periodically visit this page. To this end, the policy document highlights the date of last version.

4.2.15 PLOTO Day-to-Day Data Usage and Related Processes

Despite the fact that PLOTO does not use any direct personal data (in the form of data coming out or processed during its research activities), it recognises the needs for creating some process related policies so that there is overall agreement of the usage/storage/retention/opt-out etc of data from every-day (day-to-day) project activities. A list of such matters is included below where the means that the consortium will tackle them reflects the whole consortium agreed approach.

4.2.15.1 PLOTO list of contacts

The PLOTO list of contacts relates to a single XLS file that includes the names of all the consortium partners and persons and their email address. It also indicates the purposes of contacting each person per organisation (admin, technical, legal etc) and the emailing lists that each belongs to. Only PLOTO consortium partners have access to this list of contacts. The purpose of this list is to keep a well organised list of contacts for the PLOTO communications. The data will be erased after the project end (28/02/2026) and not kept or maintained after the project end. This list is being stored at the POTO sharepoint. Any person has the right to opt out of this list by direct email to the project coordinator.

4.2.15.2 Meetings' related material

This relates to any document created and used for the purposes of project meetings. These may relate to agendas, presentations, minutes, signature lists or any other internal document created for the purposes of PLOTO meetings. All these documents will be created and maintained for internal purposes of PLOTO and only PLOTO partners will have access to them at the PLOTO teamwork under the meetings section. They will be kept for 5 years after the project end (for auditing reasons, ie 28/02/2026). Any person has the right to opt out of being mentioned in these by direct email to the project coordinator before or after the meeting.

4.2.15.3 Workshops/Conferences and Training sessions

These data relate to the creation of workshops, agendas, programmes, participants' lists etc and in general dissemination material related to PLOTO organised workshops. Regarding the external publication of this material, we consider that this material can be fully anonymized so that it excludes personal information from the presenters/participants in the related programmes/agendas that will be shared publicly. For the parts of the related material that will be used for the workshop organisation internally to PLOTO, the related files will be stored in the PLOTO sharepoint under the section meetings. The data will be kept for 5 years after the project end for auditing reasons (i.e., 28/02/2026). Any person has the right to opt out of being mentioned in these by direct email to the project coordinator before or after the event.

4.2.15.4 Reporting

Reporting refers to internal and external (EC) documents including PLOTO progress of activities, technical overviews etc. Related files will be including documents (reports with no personal identifiable information) and financial data (C forms) sometimes including personal data. The purpose of these data is financial so that partners can claim budget requests for their related effort in PLOTO. C forms will be maintained by the project coordinator only and stored at internal and secure sharepoint. These (per partner) data are not to be shared with anyone internally or externally to PLOTO, will be kept for 5 years after the project end (for audit purposes, i.e., 28/02/2026) and will be deleted after this date. Opting out of these data will be possible but will require an updated Form C to be submitted by the project partner.

4.2.15.5 Deliverables, internal documents and other PLOTO reports

During the PLOTO project run-time, a large series of documentation and reporting will be provided relating to the project deliverables and/or internal documents etc. These files will be used for the project contractual obligations and shared to: PLOTO partners, EC, everyone (depending on deliverable type). In these documents, the name or email of authors may be included. Following this, as far as the internal (to PLOTO) and EC distributed documents are related, they will be used only for the purposes of reporting and stored in the PLOTO teamwork under the deliverables section. Reports that will be shared publicly (public deliverables) will mention only the partner name and not any other personal information. All reports will be kept for 5 years after the project end for auditing reasons (i.e., 28/02/2026).

4.2.15.6 Source codes

As far as the inclusion of personal information inside source codes is concerned, PLOTO intends to not use any such information into actual source code files produced in the framework of PLOTO foreground. In case that any partner wishes to include any personal information, a related consent form will have to be created, used and signed by the data owner(s).

4.2.15.7 Usage of cookies (in PLOTO sites)

In the cases that in any PLOTO application (web) requires the usage of cookies, a related pop-up window informing the user must be present, prompting the user to accept (or not) the conditions under which her/his personal information are stored. The cookie policy of the PLOTO website can be found here. PLOTO will maximize efforts to reduce the usage of cookies in its web developments.

4.2.15.8 Lists of stakeholders and PLOTO contacts

This list refers to internal to PLOTO lists of external stakeholders including potential technology/results up-takers, major links with end-users and other stakeholders. This list will be used for communication purposes of PLOTO, no external access will be allowed (restricted to PLOTO partners) and will be stored in the PLOTO teamwork (contacts section). When people are being registered to this list, a consent by email will have to be sent by the data owner. The data will be kept until the PLOTO end, i.e. 28/02/2026. Any person has the right to opt out of being mentioned in these by direct email to the project coordinator.

4.2.15.9 Project related research data

Any data circulated internally to PLOTO for research purposes must be fully anonymized by the data owner (in this case the data controller) and not relating in any case to personal information as stated in the Sections above.

4.2.15.10 Any other PLOTO related data

In case that personal information needs to be added in any other document in PLOTO, the controller (document creator) will have to notify the data owners of their personal details being included into the related document, purpose, retention, storage etc.

5 Conclusions

This document contributes to the PLOTO project management processes and policies, by providing a complete Data Management Plan (as part of WP1). The report starts with a description of the data that will be used in all technical, project management, administrative and pilot activities of PLOTO. This provides the PLOTO data lifecycle overview and the types of data assets that range from IoT-related data to trust-related data, stakeholder-related data and project management data. In addition, an analysis of the data in each WP and task is included, together with extensive descriptions of their properties. Furthermore, the PLOTO policy and overall overview for respecting the General Data Protection Regulation (GDPR) is presented. This includes also the PLOTO GDPR policy that is agreed within the consortium. This document also includes the potential data that can be generated or collected during the PLOTO project's lifetime, how the project plans to make the data FAIR, as well as how to ensure the security and privacy of personal and sensitive data.

This deliverable is the first version of the Data Management Plan (DMP) and will be updated in the second and final version of the report (D1.3 "Data Management Plan version 2"). This will be updated towards the project's end, including latest updates on data, actual data shared, metadata provided, as well as information on their public sharing and related platforms.

6 Annexes

6.1 Annex 1: Initial data assets

The folowing table (Table 7) lists the potential data assets that have been identified in the beginning of the PLOTO project. This list will be updated at later stages of the project and reported in the next versions of the Data Management Plan. The data below have been structured per WP and task and are referenced with IDs (1st column).

Table 7: Initial data assets in PLOTO

Name of dataset	Relevant project task(s)	Type of data	Format of data	Expected size of data[i]	Storage of data[ii]	Stakeholders that may find meaningful utility for the dataset[iii]	Describe the utility of the dataset[iv]	Includes personal data? (Y/N)	Data availability (Open/Closed)	If data will be closed (or can be shared under restrictions), please provide a justification	Data accessibility for open data[v]	Please indicate the expected time that data will be made open through Zenodo, OpenAIR, etc.	Responsible partner / collaborating partners
Meeting Presentations, minutes, and internal reports	All	Document	PDF; DOCX; DOC	1-2MB each	Project SharePoint	Consortium	Internal documents to monitor project progress	Y	Closed	Information useful only for internal project management purposes.	N/A	N/A	INTRA, all consortium partners
Deliverables	All	Document	PDF; DOCX; DOC	1-20MB each	Project SharePoint	Consortium	Delivery and presentation of project results	Y	Open (Sensitive data will be removed)	N/A	Project website	After submission to the EC	Deliverable leaders/main authors
End users' requirements	T2.1	Document	XLSX; PDF; DOCX; DOC	~5MB	Local storage, Project SharePoint	Academic institutions/research centres, technology companies	Requirements from end-users for the development of the PLOTO integrated system	N	Open (Sensitive data will be removed)	N/A	Zenodo	August 2023	RISA, end user partners
PLOTO system requirements	T2.2	Document	XLSX; PDF; DOCX; DOC	~5MB	Local storage, Project SharePoint	Academic institutions/research centres, technology companies	Functional and non-functional requirements of the PLOTO integrated system	N	Open (Sensitive data will be removed)	N/A	Zenodo	August 2023	RISA

Hungarian River Information Services data (pannonris.hu)	T2.2	Text, numerical data, coordinates	NtS 4.0 xml, JSON	TBD	Central repository	Academic institutions/research centres, technology companies	Specification of pilot use case	N	Open (Sensitive data will be removed)	N/A	Zenodo	August 2023	RSOE
Minimum effective depths in harbour basins and berths	T2.4	Hydrological data	XLSX	100KB	Local storage	Academic, research, technology companies	Hydrological studies, usefull information for logistic and port operation	N	Open	N/A	Zenodo	August 2023	RRT
Euro-CORDEX Episodic Periods	T3.1	Data of "episodic" periods	CSV	30 MB	Central repository	Academic institutions/research centres	NTUA will use them to evaluate climate and weather-related risks on chosen pilot sites	N	Open	N/A	Zenodo	June 2023	FMI
Pilot site weather & hydro hazard scenarios	T3.1	Numerical data	HDF5 file	6GB per site	TBD	Academic institutions/research centres & end users	Needed for IRAP	N	Open (Sensitive data will be removed)	N/A	Zenodo, Github	August 2023	FMI, AUTH
LES Wind Timeseries	T3.3	Dataset of wind speed time series obtained from high-resolution LES model simulations over the chosen pilot sites	NETCDF 4	10 GB	Central repository	Academic institutions/research centres, technology companies	Datasets of atmospheric turbulence which will be used by NTUA to evaluate climate and wind related risks on chosen pilot sites	N	Open	N/A	Zenodo	August 2024	FMI
ICON-EU	T3.3	Text	JSON & Excel file	4MB per site	TBD	Research & end users	Needed for IRAP	N	Open	N/A	Zenodo, Github	December 2024	AUTH
Pilot site wind simulation dataset	T3.3	Numerical data	netCDF	3GB per site	TBD	Academic institutions/research centres & end users	Needed for IRAP	N	Closed	Confidential site information	N/A	N/A	FMI
Pilot site mesoscale model nowcasting timeseries	T3.4, 3.5	Numerical data	netCDF or CSV	500MB per site	Local storage	Academic institutions/research centres & end users	Needed for IRAP	N	Closed	Confidential site information	N/A	N/A	AUTH
Pilot site weather station timeseries	T3.4	Text, numerical	CSV	5MB per site	TBD	Academic institutions/resear	Needed for IRAP	N	Closed	Confidential site information	N/A	N/A	AUTH

		data, coordinates				ch centres & end users							
Daily nowcasting & forecasting mesoscale predictions	T3.4	Text, numerical data, coordinates	geotiff, netcdf	10GB per site	TBD	Academic institutions/research centres & end users	Needed for IRAP	N	Closed	Confidential site information	N/A	N/A	AUTH
Pilot site seismic hazard scenarios	T4.1	Numerical data	HDF5 file	2GB per site	TBD	Academic institutions/research centres & end users	Needed for IRAP	N	Open	N/A	Zenodo, Github	August 2024	NTUA
Pilot site traffic data	T4.1	Text, numerical data, coordinates	Excel, CSV	10MB per site	Local storage	Research & end users	Needed for IRAP	N	Open (Sensitive data will be removed)	N/A	Zenodo	August 2024	End users, associated partners
Inundation modelling outcomes	T4.1	Numerical data	CSV	TBD	Local storage	Research & end users	Needed for IRAP	N	Open (Sensitive data will be removed)	N/A	Zenodo	August 2024	ULiege
IWW asset fragility & vulnerability curves	T4.2, 4.3	Text, numerical data	JSON & Excel file	1MB per site	Local storage	Academic institutions/research centres & end users	Needed for IRAP	N	Open	N/A	Zenodo, Github	February 2025	SORECC, NTUA
Pilot site socioeconomic consequence dataset	T4.5	Text, numerical data	Excel or JSON	10MB per site	Local storage	Academic institutions/research centres & end users	Needed for IRAP	N	Open (Sensitive data will be removed)	N/A	Zenodo	June 2025	SORECC
WISE Large rivers and large lakes	T5.1, 5.3, 5.5	Vector data	.shp	TBD	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	June 2023	NTUA, STWS, UM, SoReCC
Rivers of Romania EN	T5.1, 5.3, 5.5	Vector data	arcgis	TBD	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Closed	Only available for arcgis users	N/A	N/A	NTUA, STWS, UM, SoReCC
JRC Data Catalogue	T5.1, 5.3, 5.5	Vector data	.shp	TBD	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	June 2023	NTUA, STWS, UM, SoReCC
JRC Data Catalogue Floods	T5.1, 5.3, 5.5	Vector data	WKT (Polygon) etc.	TBD	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	June 2023	NTUA, STWS, UM, SoReCC
River flood hazard maps for Europe	T5.1, 5.3, 5.5	Raster	.tif	TBD	Local storage	Academic institutions/resear	IWW corridors monitoring	N	Open	N/A	Zenodo	June 2023	NTUA, STWS, UM, SoReCC

						ch centres & end users							
River flood hazard maps for Europe and the Mediterranean Basin region	T5.1, 5.3, 5.5	Raster	.tif	TBD	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	June 2023	NTUA, STWS, UM, SoReCC
Flood hazard map of the World - 500-year return period	T5.1, 5.3, 5.5	Raster	.tif	TBD	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	June 2023	NTUA, STWS, UM, SoReCC
Flood hazard map of the World - 50-year return period	T5.1, 5.3, 5.5	Raster	.tif	TBD	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	June 2023	NTUA, STWS, UM, SoReCC
Flood hazard map of the World - 20-year return period	T5.1, 5.3, 5.5	Raster	.tif	TBD	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	June 2023	NTUA, STWS, UM, SoReCC
Flood hazard map of the World - 10-year return period	T5.1, 5.3, 5.5	Raster	.tif	TBD	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	June 2023	NTUA, STWS, UM, SoReCC
Corine Land Cover	T5.1, 5.3, 5.5	Raster	.tif	TBD	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	June 2023	NTUA, STWS, UM, SoReCC
Catchment Characterisation and Modelling (CCM)	T5.1, 5.3, 5.5	Vector data	.shp	TBD	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Closed	Only available on request	N/A	N/A	NTUA, STWS, UM, SoReCC
Synthetic flood imagery for image segmentation	T5.1, 5.3, 5.5	Raster (aerial)	.png, .jpg etc.	TBD	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	June 2023	NTUA, STWS, UM, SoReCC
RIWA Dataset	T5.1, 5.3, 5.5	Raster (aerial)	.png, .jpg etc.	TBD	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	June 2023	NTUA, STWS, UM, SoReCC
Louisiana flood 2016	T5.1, 5.3, 5.5	Raster (aerial)	.png, .jpg etc.	TBD	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	June 2023	NTUA, STWS, UM, SoReCC

AIDER	T5.1, 5.3, 5.5	Raster (aerial)	.png, .jpg etc.	TBD	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	June 2023	NTUA, STWS, UM, SoReCC
SEN12-FLOOD: a SAR and Multispectral Dataset for Flood Detection	T5.1, 5.3, 5.5	Satellite images	SAR	TBD	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Closed	Only available for IEEE members	N/A	N/A	NTUA, STWS, UM, SoReCC
Lake Image Classification	T5.1, 5.3, 5.5	Raster	.png, .jpg etc.	TBD	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	June 2023	NTUA, STWS, UM, SoReCC
Satellite water yolo	T5.1, 5.3, 5.5	Satellite images	Sentinel 2	TBD	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	June 2023	NTUA, STWS, UM, SoReCC
Flood Area Segmentation	T5.1, 5.3, 5.5	Raster (aerial)	.png, .jpg etc.	TBD	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	June 2023	NTUA, STWS, UM, SoReCC
Flood Area Segmentation | DeepLabV3+	T5.1, 5.3, 5.5	Raster (aerial)	.png, .jpg etc.	TBD	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	June 2023	NTUA, STWS, UM, SoReCC
Satellite Images of Water Bodies	T5.1, 5.3, 5.5	Satellite images	.jpg	TBD	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	June 2023	NTUA, STWS, UM, SoReCC
Water Segmentation Dataset	T5.1, 5.3, 5.5	Raster	.png, .jpg etc.	TBD	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	June 2023	NTUA, STWS, UM, SoReCC
AFO - Aerial dataset of floating objects	T5.1, 5.3, 5.5	Raster	.png, .jpg etc.	TBD	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	June 2023	NTUA, STWS, UM, SoReCC
Water Classification	T5.1, 5.3, 5.5	Raster	.png, .jpg etc.	TBD	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	June 2023	NTUA, STWS, UM, SoReCC
Water Bodies Dataset	T5.1, 5.3, 5.5	Satellite images	Sentinel 2	TBD	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	June 2023	NTUA, STWS, UM, SoReCC

Test Data for Segmentation - Land and Water plots	T5.1, 5.3, 5.5	Raster	.png, .jpg etc.	TBD	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	June 2023	NTUA, STWS, UM, SoReCC
Sen1Floods11	T5.1, 5.3, 5.5	Satellite images	Sentinel 1 and Sentinel 2	TBD	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	June 2023	NTUA, STWS, UM, SoReCC
Western-europe-flooding	T5.1, 5.3, 5.5	Raster	.tif	TBD	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	June 2023	NTUA, STWS, UM, SoReCC
Flooding events from 2010 to 2022	T5.1, 5.3, 5.5	Raster	.tif	TBD	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	June 2023	NTUA, STWS, UM, SoReCC
Satellite Image Segmentation for Flood Damage Analysis	T5.1, 5.3, 5.5	Satellite images	Sentinel	TBD	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	June 2023	NTUA, STWS, UM, SoReCC
Detect Flood Water	T5.1, 5.3, 5.5	Satellite images	Sentinel 1	TBD	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Closed	Competition	N/A	N/A	NTUA, STWS, UM, SoReCC
Flood Segmentation	T5.1, 5.3, 5.5	Raster	mobile phone	TBD	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	June 2023	NTUA, STWS, UM, SoReCC
Dynamic World	T5.1, 5.3, 5.5	WebGIS	TBD	TBD	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Closed	Competition	N/A	N/A	NTUA, STWS, UM, SoReCC
Semantic-Segmentation-of-Flood-Water-Imagery	T5.1, 5.3, 5.5	Raster	RADAR	TBD	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	June 2023	NTUA, STWS, UM, SoReCC
Learning Deep Models from Weak Labels for Water Surface Segmentation in SAR Images	T5.1, 5.3, 5.5	Raster	.npy	TBD	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	June 2023	NTUA, STWS, UM, SoReCC
RescueNet Dataset	T5.1, 5.3, 5.5	Raster (aerial)	.shp	TBD	Local storage	Academic institutions/resear	Disaster management and IWW	N	Open	N/A	Zenodo	June 2023	NTUA, STWS, UM, SoReCC

						ch centres & end users	performance monitoring					
SAR Sentinel 1A images	T5.3, 5.4	Raster dataset	Sentinel product (safe,.zip), JPEG2000(.jp2), GeoTIFF (.tif)	10TB (depending on the time span of the time series)	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	August 2024	NTUA, STWS, UM, SoReCC
SAR Sentinel 1B images	T5.3, 5.4	Raster dataset	Sentinel product (safe,.zip), JPEG2000(.jp2), GeoTIFF (.tif)	10TB (depending on the time span of the time series)	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	August 2024	NTUA, STWS, UM, SoReCC
Multispectral very high resolution images (World View, QuickBird)	T5.3, 5.4	Raster dataset	JPEG2000(.jp2), GeoTIFF (.tif)	10TB (depending on the time span of the time series)	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Closed	Very high-resolution multispectral satellite images will be purchased and are subject to public access restrictions	N/A	N/A	NTUA, STWS, UM, SoReCC
Multispectral (RGB) images	T5.3, 5.4	Raster dataset	JPEG2000(.jp2), GeoTIFF (.tif), JPEG (.jpg)	1TB per acquisition	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	August 2024	NTUA, STWS, UM, SoReCC
Hyperspectral images	T5.3, 5.4	Raster dataset	ENVI data product (.hdr), PCIDSK (.pix), TIFF (.tif)	500GB per acquisition	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	August 2024	NTUA, STWS, UM, SoReCC
Thermal images	T5.3, 5.4	Raster dataset	TIFF (.tif)	100MB per acquisition	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	August 2024	NTUA, STWS, UM, SoReCC
Geographic Data	T5.3, 5.4	Dataset	(.json)	TBD	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	August 2024	NTUA, STWS, UM, SoReCC

Geographic Data	T5.2, 5.3, 5.4	Dataset	Shapefiles (.shp), TIFF (.tif), GeoTiFF (.tif), (.prj), (.dbf), (.shx), (.csv), (.json), (.xls)	500MB per pilot site	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	November 2023	NTUA, STWS, UM, SoReCC
Spectral Library (SL)	T5.3, 5.4, 5.5	Report	(.pdf), (.doc), (.tiff), (.png), (.jpg)	200MB per pilot site	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	August 2024	NTUA, STWS, UM, SoReCC
GPS Measurements	T5.3, 5.4	Dataset	(.txt), (.csv), (.dxf), (.dwg), (.pdf)	100MB per acquisition	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	August 2024	NTUA, STWS, UM, SoReCC
Digital Elevation Models (DEMs)	T5.2, 5.3, 5.4	Raster dataset	(.tiff)	500MB per pilot site	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	November 2023	NTUA, STWS, UM, SoReCC
3D representations	T5.3, 5.4	Point cloud	(.ply), (.obj), (.wrl), (.dxf)	4-8GB per pilot site	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	August 2024	NTUA, STWS, UM, SoReCC
3D representations	T5.3, 5.4	Mesh (3D surface)	(.ply), (.obj), (.nxs), (.nxz)	4-8GB per pilot site	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	August 2024	NTUA, STWS, UM, SoReCC
UAV Flight Plans	T5.2, 5.3, 5.4, 5.5	Report	(.json), (.lz), (.csv	100MB per acquisition	Local storage	Academic institutions/research centres & end users	IWW corridors monitoring	N	Open	N/A	Zenodo	November 2023	NTUA, STWS, UM, SoReCC
European Flood Database	T6.8	Hydrological time series data	CSV	~700 KB	TBD	Academic institutions/research centres & end users	Development of the IWW Digital Twin	N	Open	N/A	Zenodo	June 2025	EXUS
Global Flood Monitoring System	T6.8	Hydrological time series data	TBD	TBD	TBD	Academic institutions/research centres & end users	Development of the IWW Digital Twin	N	Open	N/A	Zenodo	June 2025	EXUS
The Flood Observatory	T6.8	Hydrological time series data, GIS	TBD	TBD	TBD	Academic institutions/resear	Development of the IWW Digital Twin	N	Open	N/A	Zenodo	June 2025	EXUS

						ch centres & end users							
The European Space Agency (ESA)	T6.8	Satellite imagery data	TBD	TBD	TBD	Academic institutions/research centres & end users	Development of the IWW Digital Twin	N	Open	N/A	Zenodo	June 2025	EXUS
The United States Geological Survey	T6.8	Elevation model and geospatial data	TBD	TBD	TBD	Academic institutions/research centres & end users	Development of the IWW Digital Twin	N	Open	N/A	Zenodo	June 2025	EXUS
Open Steet Map	T6.8	Vector data of buildings and roads	TBD	TBD	TBD	Academic institutions/research centres & end users	Development of the IWW Digital Twin	N	Open	N/A	Zenodo	June 2025	EXUS
IWW exposure dataset	T6.8	Text, numerical data, coordinates	XLSX & shapefile	100MB per site	TBD	Academic institutions/research centres, end users	Needed for IRAP	N	Closed	Confidential site info	N/A	N/A	EXUS, end users, associated partners
Pilot site regional and/or facility socioeconomic data	T7.3	text, numerical data	XLSX	1MB per site	Local storage	Academic institutions/research centres, end users	Needed for IRAP	N	Open (Sensitive data will be removed)	N/A	Zenodo, Github	February 2026	UDG, BME, associated partners
Results of Pilots	T7.3	Document	XLSX; DOCX; DOC	TBD	TBD	Research and tech partners	Needed for IRAP	N	Open	N/A	Zenodo	February 2026	EXUS
Training materials and results of training	T7.4	Document	PDF; DOCX; DOC	5-10MB each	TBD	Research and tech partners	Needed for IRAP	N	Open	N/A	Zenodo	February 2026	DBC

[i] (Refers to estimated expected size of the data based on similar past experiences of the project partners unless otherwise indicated)

[ii] (e.g. local storage, central repository, etc.)

[iii] (e.g. academic institutions/research centres, technology companies, etc.)

[iv] (for the indicated stakeholders group)

[v] (e.g. Zenodo, OpenAIRE, etc.)