

# Data Management Plan

August 2025

## Executive Summary

This report provides an initial version of the Data Management Plan (DMP) concerning the data processed, generated and preserved during and after the duration of the SystR project, as well as relative concerns generated from their usage. The deliverable aims to define a framework outlining the project policy for data management.

This document outlines key aspects such as data information, metadata structure, access and sharing policies, re-use guidelines, and long-term storage and management strategies. Throughout the project, the DMP will be continuously updated based on insights for all related Work Packages (WP). As such, the initial framework provided here will adapt over time serving as an evolving, living document.

## Report information

**Grant Number:** 101212761

**Acronym:** SystR

**Full project title:** Accelerating Systemic Climate Adaptation Across Europe through Integrated Ecosystems of Resilience Solutions

**Project duration:** 1 June 2025 – 31 May 2029

**Type of action:** HORIZON Innovation Action

**Deliverable:** D7.2 – Data Management Plan

**Work Package:** WP7 – Project Management and Coordination

**Submission date:** August 2025

**Type:** R- Document, Report (public)

**Authors:** Gianko Michailidis, AgroApps

**Reviewers:** Athanasios Sfetsos (NCSR), Dimitris Tzempelikos (EGL)

**Front page photo:** Photo by [Alina Grubnyak](#) on [Unsplash](#)

**Terms of use:** This publication has been produced as part of the SystR project and is licensed under a Creative Commons Attribution 4.0 International licence (CC BY 4.0), except where otherwise noted.

**Disclaimer:** The project is funded by the European Union. Views and opinions are however those of the author(s) only and do not necessarily reflect those of the European Union.

### Document history:

Version	Issue Date	Stage	Description	Contributor
V0.1	20/07/2025	Draft	1 <sup>st</sup> Draft of the Deliverable	
V0.2	18/08/2025	Draft	2 <sup>nd</sup> Draft of the Deliverable	
V0.3	22/08/2025	Draft	3 <sup>rd</sup> Draft of the Deliverable	

## Contents

1	Introduction.....	4
2	SystR Data Management Plan Overview .....	4
3	Participation to Open Research Data Pilot (ORDP).....	9
4	FAIR Data .....	13
5	Resource for Data Collection and Management.....	20
6	Data Security.....	21
7	Ethical and Legal Aspects .....	22
8	Summary.....	23
	About SystR.....	24
	Annex 1- Data Management Plan Questionnaire.....	Annex p. 1

## Index of Tables

Table 1. Types of Data.....	6
Table 2. SystR Data and Research Outputs .....	8
Table 3. Questionnaire for Classification of Research Outputs .....	11
Table 4. Revision History Table .....	15
Table 5. Metadata Template.....	16
Table 6. Project Documentation Related Metadata as Part of the Deliverables Template.....	17

ABBREVIATIONS AND ACRONYMS	
DMP	Data Management Plan
WP	Work Packages
DOI	Digital Object Identifier
IPR	Intellectual Property Rights
AI	Artificial Intelligence
EU	European Union
CA	Consortium Agreement
EC	European Commission
RIA	Research and Innovation Actions
IA	Innovation Action
CSA	Coordination and Support Actions

# 1 Introduction

This document presents the DMP for the SystR project. It outlines the types of data that will be collected, created, and maintained throughout the project's duration- and beyond its conclusion. This report serves as a basis for managing project data, covering aspects such as file formats, metadata standards, accessibility, sharing protocols, reuse conditions, and strategies for long-term preservation. Also, it addresses the legal and ethical obligation associated with data handling.

As an evolving document, this DMP will be reviewed and updated regularly to reflect new developments and consortium's growing understanding of its data requirements. Since SystR is currently in early stage (Month 3), many partners have yet to fully define their data workflows for future stages. A more detailed version is planned for the later months of the project, once there will be more information and insights from ongoing work across the consortium.

## 1.1 Scope

This deliverable sets out a structured approach to data management within the SystR project, aligning with the principles laid out in the European Commission's (EC) Guidelines<sup>1</sup> on Data Management in Horizon 2020. It seeks to address key questions, including:

- What categories of data will be produced or gathered?
- Which standards and protocols will be applied?
- In what ways will the data be shared, accessed, or reused, and how will transparency and validation be ensured?
- What measures will be in place for data preservation and long-term maintenance?

The document is dynamic and will be periodically updated in parallel with the development work taking place in other WPs. Overall, a common policy will be defined indicating the procedures for the data management during the project's lifecycle and beyond, as well as internal and external level.

# 2 SystR Data Management Plan Overview

In accordance with the Horizon 2020 Guidelines on FAIR Data Management<sup>2</sup>, which remain applicable under the Horizon Europe framework, the establishment of a DMP is considered essential for the proper handling of research data. Within this section, an overview is provided of the data types and research outputs expected to be generated, collected, or reused throughout the project. As the project advances, the types of data may be revised to incorporate any additional data types or outputs identified during implementation.

## 2.1 Data Management Plan in Horizon Europe

The EC requires that all project proposals related to "Research and Innovation Actions" (RIA), "Innovation Actions" (IA) and "Coordination and Support Actions (CSA)" incorporate research data management in

---

<sup>1</sup> European Commission, Directorate-General for Research & Innovation (2016) H2020 Programme Guidelines on FAIR Data Management in Horizon 2020, Version 3.0. Luxembourg, European Commission, Directorate-General for Research & Innovation 12pp. DOI: <http://dx.doi.org/10.25607/OBP-774>

<sup>2</sup> "Guidelines on Data Management in Horizon 2020", [http://ec.europa.eu/research/participants/data/ref/h2020/grants\\_manual/hi/oa\\_pilot/h2020-hi-oa-data-mgt\\_en.pdf](http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf)

their activity, which is being evaluated. Furthermore, a DMP is mandatory for projects which are part of the Open Research Data Pilot – which will be discussed in this document.

According to the Guidelines on FAIR Data Management, a DMP is defined as follows:

*“DMPs are a key element of good data management. A DMP describes the data management life cycle for the data to be collected, processed and/or generated by a Horizon 2020 project. The use of a Data Management Plan is required for projects participating in the Open Research Data Pilot. Other projects are invited to submit a Data Management Plan if relevant for their planned research.”*

The purpose of a DMP is to present the key components of the data management strategy to be applied throughout the project for all datasets that will be generated, processed, or preserved. With consideration given to the lawful processing of personal data, scientific research data should be made discoverable, accessible, comprehensible, and usable beyond their initial purpose, while also maintaining compliance with recognized quality and interoperability standards.

The SystR DMP has been developed in alignment with the Guidelines on FAIR Data Management in Horizon 2020<sup>3</sup> (EC, 2016) and the Horizon Europe DMP Template issued by the EC (European Commission, 2021)<sup>4</sup>. This template is intended for use in any Horizon Europe project involving the production, collection, or processing of research data. Under this framework, data management is to be guided by four core principles: findability, accessibility, interoperability, and reusability (FAIR). These principles are designed to ensure that research outputs can be effectively accessed, understood, shared, and reused within and beyond the original research context.

The FAIR principles<sup>5</sup> are to be interpreted as general guidelines and do not imply the use of any specific technologies, standards, or implementation tools. The template serves as a framework of structured questions to be answered with a level of detail appropriate to the project's maturity. The key topics addressed include: (a) Data Summary, (b) FAIR data, (c) Allocation of Resources, (d) Data Security, (e) Ethical Considerations, (f) Additional Issues, and (g) Support for DMP Development.

It is acknowledged that full responses to all areas are not expected by M3 of the project. Instead, the DMP is regarded as a dynamic document, intended to be revised as the project evolves and as significant changes arise. For SystR, regular updates will be facilitated through online documentation tools, and a comprehensive revised version of the DMP is scheduled for later months.

## 2.2 SystR Data Information

This section details the types of data that will be collected, generated, or reused throughout the SystR project to support the design, implementation, and evaluation of innovative solutions in climate adaptation settings. Data will be produced across various work packages and pilot sites, reflecting the project's cross-sectoral, multi-scalar approach and active stakeholder engagement in co-developing resilience strategies tailored to local environmental and socio-economic contexts.

---

<sup>3</sup> European Commission, "H2020 Programme: Guidelines on FAIR Data Management in Horizon 2020" (2016). Guides. 4. <https://arrow.tudublin.ie/dataguide/4>

<sup>4</sup> [https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/temp-form/report/data-management-plan\\_he\\_en.docx&ved=2ahUKewiY2omQ0JuPAX-Whif0HHVzXN6MQFnoECB8QAQ&usg=AOvVaw0Dg2Ng62AKcLqa-SOAJhLe](https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/temp-form/report/data-management-plan_he_en.docx&ved=2ahUKewiY2omQ0JuPAX-Whif0HHVzXN6MQFnoECB8QAQ&usg=AOvVaw0Dg2Ng62AKcLqa-SOAJhLe)

<sup>5</sup> Wilkinson, M., Dumontier, M., Aalbersberg, I. et al. The FAIR Guiding Principles for scientific data management and stewardship. *Sci Data* 3, 160018 (2016). <https://doi.org/10.1038/sdata.2016.18>

### 2.2.1 Types of Data

The different types of data processed in the SystR project are clarified, which included on the DMP, according to the following table:

Types of Data	Description
Research Data	Research data is the evidence that underpins all research conclusions (except those which are purely theoretical) and includes data that has been collected, observed, generated, created or obtained from commercial, government or other sources for subsequent analysis and synthesis to produce original research results. These results are then used to produce research papers and submitted for publication.
Open Research Data	Research data that is publicly available and can generally be accessed, analyzed, utilized, replicated, and shared without any cost to the user.
Secondary Data	Secondary data refers to pre-existing information, independent of the current research study.
Metadata	Metadata refers to data that provides information about other data. It offers a summary of key details, making it simpler to locate and handle specific data instances.

Table 1. Types of Data

### 2.2.2 Data and Research Outputs

In alignment with the classification presented in Table 1 and following the EC FAIR Data Management Guidelines and template, a questionnaire was distributed during the first month of the project to the project's partners to identify the types of data to be collected, generated, or, where applicable, reused within the project. The questionnaire (Annex I) addressed various aspects, including the reuse of existing data, types and formats of data to be generated, the purpose and relevance to project objectives, anticipated data size, origin, and potential external utility. It also covered topics related to making data FAIR, such as persistent identifiers, metadata provisions, repository arrangements, data accessibility and restrictions, interoperability standards, and strategies for enhancing data reusability, while considering factors like resource allocation, data security, and legal and ethical concerns.

The questionnaire developed by the partner responsible for the DMP (AgroApps) was completed by all relevant project partners, with their responses compiled and summarized in this deliverable. It is worth noting that the input provided by the partners reflects the information available up to M3 of the project.

Partner	Type	Data/Research output
NCSR	Text, numeric data, geospatial, survey	Workflows, protocols, models

<b>CKIC</b>	Text, numeric data, survey	Workflows, protocols,
<b>IIASA</b>	Text, images, numeric data, geospatial, survey	Workflows, protocols, models
<b>E2050</b>	Text, images, numeric data, audio, video, geospatial, survey	Governance models, policy briefs, scenarios
<b>UVIGO</b>	Text, numeric data, survey	Not known yet
<b>ICLEI</b>	Text, numeric	Not known yet
<b>I4CE</b>	Text	Publications
<b>ACTIERRA</b>		
<b>AgroApps</b>	Text, Numeric, Survey	Software
<b>UA</b>	Text, images, numeric data, survey	Action plans
<b>EQY</b>		
<b>ADEME</b>	Text, images, video	workflows
<b>GAGNT</b>	Numeric data, geospatial, other	Not known yet
<b>BRGM</b>	Numeric data, geospatial	Protocols, models
<b>CCI</b>	Not Known yet	Not Known yet
<b>CMCC</b>	Text, numeric data, geospatial, survey	Software
<b>RM</b>	Not Known yet	Not Known yet

<b>ASUD</b>	Not Known yet	Not Known yet
<b>P&amp;W</b>	Text, numeric data, geospatial	Supporting documents for runoff analysis
<b>ABELOVA</b>	Text, images, numeric data, geospatial	Evaluation data of NBS implementations
<b>SUA</b>	Text, numeric data	Not Known yet
<b>UVL</b>	Not Known yet	Not Known yet
<b>EGL</b>	Not Known yet	Not Known yet
<b>EMS</b>	Text, numeric data, geospatial, survey	Protocols
<b>ACS</b>	Not Known yet	Not Known yet
<b>DXERCC</b>	Not Known yet	Not Known yet
<b>ACEA</b>	Not Known yet	Not Known yet
<b>BBSGR</b>	Not Known yet	Not Known yet

*Table 2. SystR Data and Research Outputs*

### 2.2.3 Purpose and Provenance of Data

The SystR project is committed to enhancing systemic climate resilience across Europe through the integration of advanced digital technologies and stakeholder-driven solutions. In alignment with the European Union’s (EU) Green Deal, Climate Adaptation Mission, and Digital Strategy, SystR seeks to address complex, interlinked climate risks by fostering sustainable, inclusive, and scalable adaptation pathways across coastal, urban, and rural regions.

A core aspect of the project is the responsible collection, generation, and reuse of data across diverse pilot sites and work packages. This data—ranging from environmental observations and socio-economic indicators to system-level performance metrics and stakeholder engagement inputs—will be managed in full compliance with EU data protection regulations, including the General Data Protection Regulation

(GDPR)<sup>6</sup>. In instances involving personal or sensitive information, anonymized or synthetic datasets will be employed to safeguard privacy, particularly during the testing, validation, and upscaling of adaptation solutions.

SystR places strong emphasis on data transparency, provenance, and ethical use. All data workflows will be accompanied by detailed metadata and provenance records to ensure traceability and reproducibility. This includes documentation of data sources, processing methodologies, modeling tools, and governance frameworks applied in developing the Integrated Ecosystems of Resilience Solutions.

By adhering to robust data management principles, SystR not only supports trustworthy, evidence-based decision-making but also contributes to the EU's vision for responsible digital innovation, collaborative climate governance, and sustainable territorial development.

### **2.2.4 Expected Size of Data**

The SystR project is anticipated to produce a variety of research outputs, including datasets, scientific publications, software tools, methodologies, dissemination materials, and other relevant resources. At this stage, it is not yet possible to accurately estimate the size of the datasets. However, this information will be included and specified in the updates of DMP.

## **3 Participation to Open Research Data Pilot (ORDP)**

As part of SystR's commitment to Open Science and in line with the EU's Open Research Data guidelines under Horizon Europe, the project ensures that all research data is managed in accordance with the FAIR principles. By promoting transparency and responsible data sharing, the consortium aims to foster cross-sectoral collaboration and maximize the societal and scientific impact of its outcomes.

The Open Research Data framework applies to datasets and metadata that are essential for validating findings reported in scientific publications, as well as to curated and raw data identified in the project's DMP. To ensure long-term preservation and accessibility, all relevant data generated or collected during SystR will be deposited in trusted, OpenAIRE-compliant repositories.

To enhance discoverability and reusability, standardized metadata will be provided for all datasets. This will facilitate integration across climate adaptation, urban planning, environmental monitoring, and governance domains, thereby supporting data-driven policymaking and innovation across regions and stakeholder groups. Where feasible, persistent identifiers (e.g., DOIs) will be assigned to datasets to ensure stable referencing and citation.

The DMP will be regularly updated throughout the project's lifetime to reflect evolving practices in data generation, processing, and sharing. It will also clearly define access conditions, particularly where ethical, legal, or confidentiality constraints apply, such as when handling sensitive stakeholder input or regional policy data.

Where feasible, SystR will provide open access to its data, along with any tools or documentation necessary to enable third parties to reproduce results, analyze findings, and further exploit the information for climate resilience, regional development, and digital governance applications. To ensure interoperability and reusability, the project will adopt recognized standards and community-endorsed practices, such as ISO 19115 for geospatial metadata, and the NetCDF/CF conventions and CSV formats for climate and

---

<sup>6</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) <http://data.europa.eu/eli/reg/2016/679/2016-05-04>

environmental datasets, and the use of controlled vocabularies (e.g., Dublin Core, SKOS) for consistent terminology.

### 3.1 Publishing Infrastructure for Open Access

The project will establish a system for making all its research outputs publicly and permanently available. This infrastructure includes a defined procedure and specific publication platforms. The project’s execution will comply with all relevant national and European regulations, particularly the GDPR, to ensure the protection of personal data. The details of this process and the chosen platforms are further elaborated in the subsequent sections.

#### 3.1.1 Publishing Process

A clear and structured process will be followed within the SystR project to determine whether a given research output should be made publicly available. All project-generated outputs—such as datasets, scientific reports, peer-reviewed publications, methodologies, and anonymized stakeholder data—are treated as “results” under the Horizon Europe framework.

Each result will be systematically assessed and categorized as either “public” or “non-public.” In accordance with Article 17 of the Horizon Europe Model Grant Agreement (GA), results intended for dissemination—particularly peer-reviewed scientific publications—must be made openly accessible, following open science and FAIR principles<sup>7</sup>.

Conversely, results classified as “non-public”—for example, those involving confidential stakeholder contributions, commercially sensitive insights, or those pending intellectual property rights (IPR) protection—will not be disclosed or published unless appropriate safeguarding measures (e.g., patent filings or confidentiality protocols) are in place. This approach ensures that the project strikes a balance between fulfilling its open science obligations and protecting valuable or sensitive outcomes.

To guide the classification of results, a decision matrix will be applied, evaluating key factors such as dissemination value, stakeholder impact, ethical or legal constraints, and potential for exploitation. This transparent assessment process supports both the responsible dissemination of knowledge and the strategic management of SystR’s innovations and findings.

Research Output	Description
Is the result beneficial to other, or is it required for understanding a scientific conclusion?	If the question about a result is answered with "yes," then the result is classified as public. If the answer is "no," then the result is classified as non-public.
Besides the author’s identity, does the result include anyone else’s personal data?	If the question about a result is answered with "yes," then the result is classified as non-public. To publish such a result, any personal information beyond must be removed. This illustrates how the publishing process can be iterative, with results initially deemed unsuitable for publication becoming publishable after these privacy-related details are addressed.

<sup>7</sup> Open Access to Scientific Publications and Open Data Access to Research Data in H2020

<p>Can individuals be identified from the result, even if their names are not used?</p>	<p>If the question about a result is answered with "yes," then the result is classified as non-public. If the answer is "no", the result classified as public.</p> <p>Sometimes, data inference can be used to combine different user data and indirectly reveal a single user's identity. Therefore, to make a result publishable, the included information must be reduced to a level where individual users cannot be identified. This can be done using established anonymization techniques, such as abstraction, dummy users, or non-intersecting features, to conceal a single user's identity. This illustrates how the publishing process can be iterative, with results initially deemed unsuitable for publication becoming publishable after these privacy-related details are addressed.</p>
<p>Does the result contain any confidential business information belonging to SystR partners?</p>	<p>If the question about a result is answered with "yes," the outcome will be considered non-public by default, unless the involved partners have explicitly agreed otherwise. Any business-sensitive or proprietary information must be removed in accordance with the requirements of all partners before any publication or disclosure of the result can take place.</p>
<p>Does the result disclose technology that is the subject of a project-related patent application?</p>	<p>If this question is answered with "yes," the result will be treated as non-public. However, it may be published once a patent application has been submitted.</p>
<p>Could project results be misused in a way that harm society or violate ethical principles?</p>	<p>If the question about a result is answered with "yes," then the result is classified as non-public.</p>
<p>Does a result pose a national security risk to any project participant?</p>	<p>If the question about a result is answered with "yes," then the result is classified as non-public.</p>

*Table 3. Questionnaire for Classification of Research Outputs*

### 3.1.2 Publishing Platforms

To ensure accessibility and compliance with open research principles, the project will utilize multiple publishing platforms for data and research outputs. These platforms collectively support FAIR data principles, maximizing the project's scientific and social impact.

### 3.1.3 Website

The official SystR project website will be launched in M6 of the project to serve as a central platform for disseminating research findings and project-related information. It is designed to remain a long-term digital resource, continuing to support knowledge sharing beyond the project's duration.

The website will play a vital role in facilitating communication and knowledge exchange among key stakeholders, including researchers, climate policy experts, public authorities, community organizations, and civil society actors. It will serve as an accessible interface for engagement with the wider public, media, and interested third parties—amplifying the visibility, reach, and impact of the project.

The SystR website will provide access to publicly available documents, project materials, and deliverables marked with a public dissemination level. Any personal data shared through website interactions (e.g.,

contact forms or event registrations) will be submitted voluntarily and handled securely, ensuring that individual user data is not accessible to other visitors.

For dissemination and outreach purposes, the platform may collect basic personal information, such as name, surname, email address, and organizational affiliation, from external stakeholders. This information will be used solely to share project-related updates, foster stakeholder engagement, and facilitate direct communication, always with informed consent and in adherence to applicable data protection standards (GDPR, EU Regulations 2016/679; Horizon Europe FAIR Data Guidelines) .

### **3.1.4 Zenodo Repository**

SystR's research outputs will be made easily discoverable via the Zenodo platform, an open-access repository used to archive and share publicly available datasets, peer-reviewed publications, methodologies, and project deliverables. All publicly accessible outputs will be deposited and assigned a unique Digital Object Identifier (DOI), ensuring persistent findability and facilitating integration within the OpenAIRE ecosystem.

A dedicated SystR Zenodo community will be established by the project coordinator, NCSR D, to organize and showcase the project's open outputs in one accessible location. The consortium will ensure compliance with Zenodo's terms of use, access rules, and metadata standards.

All datasets shared via Zenodo will be accompanied by standardized metadata to support discoverability, citation, and reuse. However, users should note that while metadata will be published alongside datasets, its availability may not be guaranteed if the corresponding data becomes inaccessible in the future (e.g., due to legal, ethical, or technical reason).

This repository-based dissemination approach reinforces SystR's commitment to open science, data transparency, and long-term accessibility of research results, in alignment with Horizon Europe guidelines.

### **3.1.5 Open Access Repositories and Directory of Open Access Repositories**

As part of its strong commitment to Open Science, the SystR project will make extensive use of Open Access Repositories to maximize the visibility and accessibility of its research outcomes. By sharing peer-reviewed articles, datasets, technical reports, and methodological frameworks through platforms such as Zenodo and participating institutions' repositories, SystR aims to foster interdisciplinary collaboration and knowledge exchange across climate adaptation, urban and regional planning, policy design, and systems innovation.

To further support broad access to its findings, SystR will follow a Green Open Access publication strategy following Horizon Europe recommendations<sup>8</sup>. This includes depositing preprints or accepted versions of scientific manuscripts in trusted repositories (e.g., Zenodo or institutional archives), in full compliance with copyright agreements and publisher embargo policies.

This approach is fully aligned with SystR's knowledge management and IPR strategy, which promotes open dissemination of publicly shareable results while protecting confidential, sensitive, or commercially valuable information. Through this open access strategy, SystR will support innovation in climate adaptation and multi-level governance across Europe.

---

<sup>8</sup> [https://ec.europa.eu/research/participants/data/ref/h2020/grants\\_manual/amga/h2020-amga\\_en.pdf#page=245](https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/amga/h2020-amga_en.pdf#page=245)

## 4 FAIR Data

SystR fully supports the re-use of research data and is strongly committed to implementing the FAIR principles. The project emphasizes high data quality and clear documentation to support transparency, knowledge sharing, and future reuse across disciplines and regions.

Each FAIR principle is applied in the context of SystR as follows:

- **Findable:** All datasets will be assigned a unique and persistent identifier (e.g., DOI) and deposited in searchable, open-access repositories such as Zenodo. Each dataset will include rich and standardized metadata to enhance discoverability across sectors including climate adaptation, regional planning, and public policy.
- **Accessible:** Research data will be made retrievable using standard, open protocols. Where data access must be restricted—due to privacy, ethical, or legal considerations—corresponding metadata will remain openly available, preserving transparency and discoverability.
- **Interoperable:** SystR will use commonly accepted data formats, vocabularies, and metadata standards to ensure seamless integration across domains such as environmental science, urban governance, and socio-economic modeling.
- **Reusable:** Each dataset will be published with clear licensing terms and include comprehensive metadata documenting its origin, structure, and intended use. This ensures the data can be accurately interpreted and repurposed by other researchers, policymakers, and practitioners.

By embedding these principles into its data management practices, SystR aims to ensure that its research outputs remain accessible, useful, and impactful beyond the project's duration—supporting future work in climate resilience, digital governance, and territorial sustainability.

### 4.1 Making Data Findable

This document outlines the DMP for the SystR project, detailing procedures for the structured collection, secure storage, integration, and responsible sharing of project-related data. Internal data exchange among consortium partners will be facilitated using collaborative platforms such as Sharepoint or equivalent secure cloud services, ensuring efficient and traceable access to shared materials and data processing workflows. All project data will remain accessible to consortium members for two years after the official conclusion of the project.

For public dissemination, curated datasets, updates, and key research outputs will be made available through the official SystR project website and appropriate open-access repositories such as Zenodo.

To enhance findability, all datasets will follow a standardized naming convention that includes a brief description of the dataset's contents, the contributing partner organization, and the month and year of submission or publication.

SystR adheres to established disciplinary and general metadata standards, including but not limited to Dublin Core<sup>9</sup> (general metadata description), DataCite Metadata Schema<sup>10</sup> (dataset citation and persistent identifiers), and where appropriate, ISO/IEC 1117<sup>11</sup> (for structures data element definitions and

---

<sup>9</sup> Dublin Core Metadata Initiative (DCMI). Dublin Core Metadata Element Set, Version 1.1. 2023

<sup>10</sup> DataCite. DataCite Metadata Schema Documentation. 2023

<sup>11</sup> ISO/IEC 11179: Information technology – Metadata registries (MDR)

interoperability), to ensure that data is well-documented, discoverable, and reusable across domains relevant to climate adaptation, regional governance, and sustainability science.

#### **4.1.1 Discoverability of the Data**

In alignment with the FAIR data principles, SystR ensures that all datasets and their accompanying metadata fulfill the following key criteria:

- Each dataset will be assigned a globally unique and persistent identifier to ensure consistent referencing, traceability, and long-term accessibility.
- Comprehensive metadata will be provided for each dataset, offering sufficient context and detail to enable accurate interpretation, replication, and meaningful reuse by researchers, policymakers, and other stakeholders.
- All data will be indexed in trusted, searchable repositories to maximize discoverability and visibility within the wider scientific and policy communities focused on climate adaptation and systemic resilience.

In parallel, authentication and access control measures will be implemented as needed to protect sensitive or restricted data. Through these combined practices, SystR will ensure its data is not only well-structured and secure, but also reliably retrievable and usable by authorized users in compliance with ethical and legal standards.

#### **4.1.2 Data Identification Mechanisms**

All documents produced within the SystR project will follow a standardized naming convention to ensure clarity and consistency. Each file will include the project acronym (SystR), a distinct and persistent identifier that reflects the documents type, and a unique number assigned by the project coordinator for reporting to the EC.

Furthermore, the document version will be clearly indicated in both the file name and title. For materials related to specific project activities or deliverables, identifiers such as the relevant task or deliverable number will be included, followed by a concise title that captured the document's focus.

The specifying naming conventions adopted for documentations are detailed in the following sections.

#### **4.1.3 Naming Convention Used**

To ensure clarity, traceability, and consistency across all project outputs, SystR adopts a standardized naming convention for all documentation. This convention supports streamlined collaboration within the consortium and compliance with EC reporting standards.

Each document file name will include the following elements in its file name:

- The project acronym: SystR
- The relevant WP identifier (e.g., WPx)
- The specific deliverable or task reference (e.g., Dx.x or Tx.x)
- A two-digit numeric suffix indicating the version number.

Example naming convention for deliverables:

Systr\_WP1\_D1.1\_v0.1.docx

For presentations and communication materials, the following format will be used:

- The project Acronym: SystR
- The name of the event or meeting (e.g., KOM, Review1)
- The relevant WP
- The version information

Example for presentation files:

SystR\_KOM\_WP1\_v0.1.pptx

This structured naming system facilitated efficient document tracking, internal collaboration, and alignment with SystR’s dissemination, quality assurance, and EC reporting protocols.

#### 4.1.4 Clear Versioning of Documents

All documents produced within the SystR project will be clearly versioned. Each document will include a version control table on the cover or first pages, containing the following descriptors:

- Version
- Date
- Partner responsible
- Description of changes

This practice ensured full transparency in document evolution, allowing all partners and reviewers to track revisions and status over the course of the project, as depicted in the table below:

Version	Issue Date	Stage	Description	Contributor
x.y				

Table 4. Revision History Table

#### 4.1.5 Standards for Metadata Creation

SystR recognizes the critical role of metadata in ensuring the discoverability, reusability, and clarity of all project documentation and datasets. Therefore, every document—especially public deliverables and datasets—must contain key metadata fields, prominently displayed on the initial pages. These include:

- Title and versioning
- Lead partner and contributors
- Associated WP
- Dissemination level
- Date of issue
- Document status

To promote consistency, the following dedicated metadata template has been developed for use across all project documentation. This template will be regularly reviewed and updated to address evolving project needs and emerging documentation standards:

#	Title	Description
1	Title	Name given to resource
2	Creator	Person/entity primarily responsible for making the resource
3	Subject	The topic of the resource
4	Description	E.g., abstract, table of contents, graphics

5	Publisher	Only for published resources
6	Contributor	Entities contributing to the making of the resource
7	Date	The termination of the data collection period
8	Type	E.g., dataset, article, questionnaire
9	Format	The file format of the resource
10	Identifier	e.g., ISSN if item has been published
11	Source	Which tools were used to collect the data
12	Language	Language of the resource
13	Relation	A related resource
14	Rights	Information about the rights held in and over the resource

Table 5. Metadata Template

In the case of datasets, data providers are also required to attach supporting materials to enhance understanding and reuse. These may include:

- A brief description of the study of data collection context
- Methodology used for data generation or analysis
- Any questionnaires or tools applied
- User manual or data documentation
- Any other information that might be of interest to a data user.

These practices ensure compliance with the FAIR principles, facilitate proper data governance, and strengthen the long-term usability and value of SystR's research outputs. The following matrix presents relevant metadata information:

Settings	Value
Editor(s)	<Name> <Surname>
Lead Beneficiary	<Partner>
Status	{Draft, Final}
Version	##
Due Date	DD/MM/202#
Delivery Date	##/##/202#

Dissemination Level	{SEN,PU}
Project	SystR
Work Package	WP#:<WP Name>
Deliverable	D#.#: <Deliverable Name>
Editor(s)	<Partner>:< Name><Surname>
Contributor(s)	<Partner>:< Name><Surname>
Reviewer(s)	<Partner>:< Name><Surname>

*Table 6. Project Documentation Related Metadata as Part of the Deliverables Template*

The project will adopt general metadata standards (e.g., Dublin Core, DataCite Metadata Schema) and domain-specific standards relevant to climate and environmental data.

For climate-related datasets, the consortium will follow internationally recognized ISO standards to ensure consistency and interoperability, including:

- ISO 14090:2019- principles, requirements, and guidelines for adaption to climate change.
- ISO 14091:2021- guidelines for assessing the risks related to the potential impacts of climate change.
- ISO/TS 14092:2020- adaption planning for local governments and communities in vulnerability impacts, and risks assessments.
- ISO 14093:2022- financing mechanisms for local climate adaption.

All metadata will be openly published in Zenodo, ensuring that even where data access is restricted, metadata remains accessible and searchable. Each metadata record will include DOI to ensure long-term discoverability.

## 4.2 Making Data Accessible

For datasets that are eligible for public release, the SystR project will utilize a dedicated file repository, hosted on a secure collaborative platform (SharePoint), maintained by the project coordinator NCSR. Prior to any data publication or external dissemination, written notification must be submitted to the coordinator and all relevant partners.

All dissemination of results—whether individually or jointly owned—must comply with Article 17.4 of the GA and Annex 5: Dissemination Rules, as detailed in the GA. A final draft of any dissemination item (e.g., journal articles, datasets, presentations) must be circulated among consortium partners for review:

- **Long-form publications** (e.g., journal articles >1,000 words): must be shared at least 45 calendar days prior to submission.
- **Short-form dissemination** (e.g., abstracts, posters, presentations): must be shared at least 15 calendar days in advance.

Should any party raise an objection, they must notify both the coordinator and the proposing party within 30 calendar days of receiving the draft. If no objection is raised within this period, the dissemination will be considered approved.

SystR will adopt Green Open Access strategies for its scientific publications and outputs. Specific publication policies will be formalized as the project progresses, in line with the EC Guidelines on Open Access to Scientific Publications and Research Data and the obligations of Article 17 of the GA<sup>12</sup>. These policies ensure compliance with Horizon Europe requirements, maximize visibility, and facilitate broad access to scientific results.

Public research outputs will be stored in trusted repositories such as Zenodo, institutional repositories maintained by partners, and the SystR project website. Key updates will also be shared on scientific networking platforms and policy-focused communication channels to maximize visibility and impact.

#### **4.2.1 Methods or Software Needed to access the Data**

Access to SystR datasets is not expected to require any proprietary or specialized software. Data will be made available in widely accepted, open-standard formats to ensure usability, accessibility, and compatibility across research, policy, and community-based platforms. Formats will include:

- CSV, XLSX, and plain text files
- Relational and non-relational databases (e.g., SQLite, JSON)
- Standardized geospatial formats (e.g., GeoTIFF, shapefiles) where applicable
- Cloud-accessible files through secured URLs.

This strategy enables seamless use by consortium partners and the wider research and policy community.

#### **4.2.2 Deposit of Data, Associated Metadata, Documentation and Code**

All data, metadata, supporting documentation, and relevant code produced within the project will be deposited in trusted repositories or secure private storage environments, depending on the sensitivity and nature of each dataset. It is anticipated that most consortium partners will utilize their own institutional or private storage infrastructures for managing and storing the datasets they contribute, along with the corresponding metadata, documentation, and software tools.

### **4.3 Making Data Interoperable**

Achieving interoperability within the project depends on the consistent use of terminology across all project documents and datasets, as well as the adoption of machine-readable formats for both data and metadata. Key enablers of interoperability include the use of a standardized naming convention for all SystR-generated content and adherence to recognized data formats.

It is the responsibility of all partners to comply with these standards by following the guidelines outlined in this DMP. Any deviations from these practices must be formally communicated to the Project Coordinator, and any decisions or adjustments must be incorporated into an updated version of the DMP to ensure alignment across the consortium.

#### **4.3.1 Interoperability of Data Assessment**

Each partner is responsible for ensuring that data they contribute is structured according to project standards and adapted where needed to meet external user requirements. Data interoperability will be reviewed periodically to support ongoing alignment with stakeholder needs and technological developments.

These reviews will help ensure that SystR outputs remain compatible across domains such as environmental policy, socio-economic analysis, climate risk modeling, and public administration.

---

<sup>12</sup> Horizon Europe Model Grant Agreement, Article 17: Open Access to Scientific Publications [https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/agr-contr/unit-mga\\_he\\_v1.1\\_en.pdf](https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/agr-contr/unit-mga_he_v1.1_en.pdf)

### 4.3.2 Vocabulary Use

SystR adopts terminology commonly used within its primary domains: climate resilience, environmental governance, systemic risk management, territorial planning, and community-based adaptation. This ensures interoperability and avoids introducing inconsistencies across datasets.

To facilitate broader integration and exchange, SystR aligns with recognized metadata and vocabulary standards, including:

- Metadata and Sematic Vocabularies
- Dublin Core
- DataCite metadata schema
- ISO/IEC 11179
- ISO/TC 211 (for spatial data)
- Technical Standards and Persistent Identifiers
- JSON and JSON-LD
- PURL (Persistent Uniform Organizational System)

These standards support structured data sharing across systems and stakeholders throughout the lifecycle of the project.

## 4.4 Making Data Reusable

The reusability of SystR data is central to its contribution to open science and policy innovation. All datasets intended for public release will:

- Include comprehensive metadata describing origin, structure, and usage terms
- Be linked to their origin
- Be published under clear, standardized usage licenses, based on the nature of the data and its intended re-use.

These practices ensure that data will remain valuable beyond the project's duration, supporting long-term impact in research, decision-making, and resilience planning.

### 4.4.1 Increasing Data Reusability with Clear Licensing Guidelines

To maximize the reuse of project outputs, SystR will apply appropriate licensing models to each dataset and deliverable, in line with the GA and Consortium Agreement (CA). Where necessary, restrictions may be applied to sensitive data, which will be made available only for research purposes and under non-commercial use licenses.

All datasets must include citation instructions and acknowledgement requirements, ensuring that future users attribute the data correctly.

### 4.4.2 Timeframe for Data Accessibility and Reuse

SystR aims to ensure the long-term availability and reusability of data beyond the formal end of the project. At minimum, all public datasets will remain accessible for one year after project completion, with options for extension based on repository guidelines and mutual agreement within the consortium.

To support sustainability, data will be maintained in trusted repositories with persistent identifiers and appropriate metadata, ensuring retrievability and usability for future research, policy design, and societal impact.

## 5 Resource for Data Collection and Management

### 5.1 Data Management Responsibilities

In the SystR project, data will be stored in a collaborative file repository (SharePoint) designated by the Project Coordinator, NCSR, as the project's official internal repository. Data will be retained for at least one year following the project's completion, with the possibility of one-year extension subject to formal agreement among consortium partners.

The DMP will be developed, maintained, and periodically updated by the Project Coordinator, and the respective WP Leaders. These roles will share joint responsibility for:

- Maintaining and updating the DMP to reflect ongoing project needs and evolving standards.
- Ensuring secure storage, controlled access, and appropriate sharing mechanisms.
- Developing sustainable strategies for data preservation, quality control, and reusability.

WP Leaders will oversee local compliance with project data standards before submitting datasets to the central repository or an approved alternative storage system.

To guarantee the integrity and quality of SystR datasets, a multi-layered validation system will be employed:

- **Automated verification:** Real-time detection of inconsistencies, missing values, or format errors during data entry and processing.
- **Systematic error detection:** Algorithmic monitoring for anomalies requiring investigation.
- **Manual verification:** Expert reviews of datasets against established quality benchmarks.

Each consortium partner is accountable for the quality and integrity of the data they contribute, while the Project Coordinator and jointly supervises overall compliance with integrity standards. This dual automated/manual approach guarantees reliable research outputs throughout the project lifecycle.

SystR-specific adaptations include:

- Defined roles aligned with SystR's organizational structure.
- A transparent escalation path for addressing data quality issues. Emphasis on both technical and experts human validation processes.

The text maintains all original substantive requirements while being completely original in expression and tailored to SystR's context.

### 5.2 Cost allocation

The costs associated with making SystR's FAIR data will be primarily covered by project funds. These costs include personnel, data publishing, updates, maintenance, hosting, backup, sharing, and security.

While long-term preservation costs (beyond the project's lifecycle) cannot be accurately estimated at this stage, SystR commits to a one-year minimum retention period, with the possibility for extension if justified and supported by partner consensus.

To optimize resources, SystR will use cost-effective solutions, such as:

- Open-access repositories, e.g., Zenodo (offering up to 50 GB free per dataset).
- The consortium's private SharePoint for internally managed data.



Each partner will be responsible for the costs related to their own data generation and processing, including:

- Data storage and backup.
- Anonymization or pseudonymization (if applicable).
- Secure data manipulation and internal sharing mechanisms.

The long-term value of SystR’s datasets—in supporting climate resilience strategies, policy innovation, and cross-regional adaptation practices—underscores the importance of their preservation as a public and scientific asset (EC, 2023; Wilkinson et al., 2016).

## 6 Data Security

The SystR consortium adheres to the highest standards of data confidentiality, integrity, and availability, implementing robust technical and organizational safeguards in line with GDPR and other relevant legal frameworks.

### 6.1 Secure Data Storage Infrastructure

The project’s primary data repository is a dedicated, password-protected cloud environment featuring:

- TLS/SSL encryption for all data transfers
- Optional end-to-end encryption for sensitive content.
- Role-based access controls to regulate viewing, editing, and administrative rights.
- Full compliance with GDPR and applicable data sovereignty regulations.

Moreover, partners may maintain local institutional copies of their datasets, provided equivalent data protection standards (e.g., access logging, secure classification, and encryption) are applied.

### 6.2 Multi-Layered Security Protocol

To mitigate risks such as unauthorized access, breaches, or accidental loss, SystR applies a multi-layered security approach, including:

- Two-Factor Authentication (2FA) for repository access
- Activity logging and access tracking for accountability
- Brute-force protection and login monitoring tools
- Automated version control and rollback functionality
- Regular encrypted backups to prevent permanent data loss.

Each partner must secure local systems with updated antivirus software, firewalls, device-level encryption, and regular audits

### 6.3 Data Transfer

All transfers of personal or sensitive data between project partners will occur through secure, encrypted channels. To comply with GDPR<sup>13</sup> and safeguard individual privacy, data will be anonymized or

---

<sup>13</sup> GDPR Regulation (EU) 2016/679

pseudonymized before any transmission. Data sharing will be limited to the minimum necessary, and robust safeguards will be implemented to ensure data integrity and confidentiality during the exchange.

## 6.4 Backup and Recovery

Regular backups of the SharePoint environment ensure data resilience. These backups include version history, enabling the restoration of previous file states when needed. Deleted files are kept for a configurable period to allow for short-term recovery. Partners who maintain local data copies must adopt similar backup strategies to guarantee data availability in case of hardware failure, accidental deletion, or other disruptions.

All consortium members must maintain and enforce their organization's established data security protocols, ensuring alignment with applicable regulations and industry standards. Each partner bears full responsibility for implementing these protective measures to secure project data.

In case of any suspected or confirmed security incident, partners must:

1. Immediately contain and isolate compromised systems.
2. Conduct thorough forensic analysis to determine:
  - a. Breach scope and severity;
  - b. Root causes;
  - c. Potential impacts.
3. Notify relevant regulatory bodies as legally required.
4. Execute corrective actions and preventive safeguards.

Partners must promptly alert the Project Coordinator of any security incidents to enable coordinated protective measures and maintain compliance across the consortium.

At the coordination level, the project adopts a proactive and comprehensive approach to data security, combining the robust capabilities of SharePoint with strict organizational controls to ensure the confidentiality, integrity. By implementing secure storage, access restrictions, encryption, regular backups, and a clearly defined breach response plan, the project fully aligns with legal requirements and best practices in data protection, including GDPR. These measures ensure that sensitive information is handled responsibly throughout the project lifecycle and beyond.

## 7 Ethical and Legal Aspects

Several SystR partners will explore the use of AI models for systemic analysis, data clustering, and decision-support systems. All AI-related activities will comply fully with the **EU AI Act** (2021) and relevant ethical guidelines, including principles of transparency, accountability, and human oversight.

AI development in SystR will:

- Be explainable and transparent in methodology and outcomes.
- Include impact assessments on bias, privacy, and fairness. AI models will undergo systematic evaluation to identify potential biases, mitigate privacy risks, and ensure equitable outcomes.
- Undergo internal ethical review when used in stakeholder or community contexts.
- SystR's approach aligns with the Ethics Guidelines for Trustworthy AI (EC, 2019) and the FAIR principles for data management when AI is applied to research datasets.



## 8 Summary

This DMP provides a comprehensive framework for managing data throughout the SystR project's lifecycle—from initial collection and processing to secure storage, sharing, and long-term preservation. The DMP is a living document that will evolve alongside the project's implementation.

As SystR progresses and additional data is generated, the DMP will be updated to reflect emerging needs, regulatory developments, and consortium insights. A revised and expanded version of the DMP will be submitted in later months, incorporating lessons learned from early-stage research and stakeholder engagement.

## About SystR

SystR is an EU-funded project introducing a novel approach to systemic resilience by linking science and policy through cross-sector, place-based solutions.

Coordinated by Demokritos and funded with €9 million from the European Union, the project addresses systemic risks (those that threaten society's essential systems) by breaking down silos, aligning multi-level governance, and tailoring responses to local strengths through Smart Specialisation Strategies.

Through its six demonstrations, SystR will prove how integrated, locally tailored approaches can build systemic resilience across Europe.

## Partners



Funded by  
the European Union



# Annex 1- Data Management Plan Questionnaire

## Instructions

Following the structure of the template released by the HORIZON EUROPE, the questionnaire consists of the following main sections:

- **“Data Summary”** focuses on questions related to any existing data to be reused, types and formats of data generated, the purpose and relation to project objectives, expected data size, origin, and potential utility for external parties.
- **“Fair Data”** includes questions aiming to address making data findable, accessible, interoperable, and reusable by discussing persistent identifiers, metadata provisions, repository arrangements, data accessibility and restrictions, interoperability standards, and measures to increase data re-use, while considering resource allocation, data security, and ethical aspects.
- The section titled **“Other research outputs”**, emphasizes questions related to managing and planning for both digital and physical research outputs generated or reused throughout the project, and application of FAIR data principles to these.
- **“Allocation of Resources”** delves into the costs associated with making data and research outputs FAIR, covering direct and indirect expenses, funding sources, the assignment of data management responsibilities, and the resources required for long-term preservation and data retention decisions.
- **“Data Security”** enlists questions that address the measures implemented for data security, including data recovery, secure storage, archiving, and transfer of sensitive data, along with the assurance of safe storage in trusted repositories for long-term preservation and curation.
- The section about **“Ethics”** aims to explore potential ethical and legal issues impacting data sharing, discussing informed consent for data sharing and long-term preservation in relation to personal data and referencing relevant ethics deliverables and chapters.
- The section on **“Personal Data”** enlists questions related to the Use and Management of personal data.
- The section titled **“Artificial Intelligence”** dives into the possible use of AI technologies for data management.

## Partner Information

Partner Information	
Partner Name	Partner Acronym
Corresponding Person (email)	example@email.com
Name of the Dataset	Please specify the name of the dataset
Name of the Use Case	Please specify the use case that this dataset will be used (if applicable)

## Data Summary

Data Summary
Will you be re-using any existing data in this project?
<input type="checkbox"/> Yes <input type="checkbox"/> No

If you answered "Yes" to the previous question, what will you re-use the existing data for? (Select all that apply)

- To test hypotheses
- To support conclusions
- To compare with newly generated data
- To provide background information or context
- n/a
- Other (Please specify) *Click or tap here to type your answer.*

What is the source of the existing data that you intend to re-use? (Select all that apply)

- Publicly available dataset or repository
- Privately owned dataset or repository
- Previously generated by the project team
- From previous research conducted by others
- Other (Please specify): *Click or tap here to type your answer.*

What criteria did you use to determine the suitability of the existing data for re-use? (Select all that apply)

- Data quality
- Data format and compatibility
- Data relevance to the project's objectives
- Availability of metadata
- Compliance with legal and ethical requirements
- Other (Please specify): *Click or tap here to type your answer.*

Have you obtained permission or authorization from the original data owners to re-use their data?

- Yes  No  Other (Please specify): *Click or tap here to type your answer.*

Are there any limitations or restrictions to the use of the existing data, such as copyright or confidentiality agreements?

- Yes  No

What types of data will be collected/ generated or re-used in the project? (Select all that apply)

- Text
- Images
- Audio
- Video
- Numeric data (e.g., measurements, statistics)
- Geospatial data (e.g., maps, GPS coordinates)
- Genetic data
- Survey or questionnaire data
- Social media data
- Other (please specify): *Click or tap here to type your answer.*

In what formats will the data be collected/ generated or re-used? (Select all that apply)

- Plain text
- PDF
- CSV
- JSON
- XML
- RDF
- Image formats (JPEG, PNG, etc.)
- Audio formats (MP3, WAV, etc.)
- Video formats (MP4, AVI, etc.)
- Other (please specify): [Click or tap here to type your answer.](#)

Will the data be structured or unstructured?

- Structured (data that has a defined schema or format)
- Unstructured (data that does not have a defined schema or format)
- Both structured and unstructured
- Not sure at this stage

If the data is structured, what will be its structure? (Select all that apply)

- Spreadsheet (e.g., Excel, Google Sheets)
- Hierarchical structure (e.g., XML, JSON)
- Graph structure (e.g., RDF, OWL)
- Other (Please specify): [Click or tap here to type your answer.](#)

In what types of storage formats will the data be stored? (Select all that apply)

- Relational database (e.g., SQL)
- NoSQL database (e.g., MongoDB)
- Spreadsheet (e.g., Excel, Google Sheets)
- Text file (e.g., CSV, TSV)
- Binary file (e.g., image, audio, video)
- Cloud storage (e.g., AWS S3, Google Cloud Storage)
- Other (please specify): [Click or tap here to type your answer.](#)

What is the purpose of the data collection/ generation or re-use and its relation to the objectives of the project?

What specific research questions will the data help to answer?

[Click or tap here to enter text.](#)

Can you estimate the expected volume of data that will be collected/ generated or re-used in the project?

[Click or tap here to enter text.](#)

Will the data be collected/ generated over a period of time, and if so, what is the expected rate of data collection/ generation?

[Click or tap here to enter text.](#)

How will the data be managed and stored to ensure that it remains accessible and usable over time? (Select all that apply)

- Data will be stored in a trusted repository.
- Data will be stored in multiple locations to prevent loss.
- Data will be stored in an encrypted format.
- Data will be stored in a cloud-based storage service.
- Data will be regularly checked for errors and inconsistencies.

- Data will be regularly tested for security vulnerabilities.
- Data will be regularly audited for compliance with ethical and legal standards.
- Data will be backed up regularly.
- Data will be made available in open and standardized formats.
- Data will be assigned persistent identifiers to ensure findability.
- Access to the data will be controlled through a formal access policy.
- Data will be preserved for a minimum number of years.
- Data will be regularly refreshed or updated to maintain its usefulness.
- Data will be versioned to track changes over time.
- Data will be migrated to new formats if necessary.
- Data will be anonymized or de-identified if necessary.
- Other (please specify): *Click or tap here to enter text.*

Can you describe the origin/provenance of the data, either collected/ generated or re-used including how it was collected/ generated and any associated metadata?

Are there any quality issues with the data, such as missing values or errors, and if so, how will these be addressed?

*Click or tap here to enter text.*

Is the data representative of the topic or phenomenon of interest?

Yes  No

Who are the potential beneficiaries of the data that you will collect/ generate or re-use? (Select all that apply)

- Other researchers in the same field
- Researchers in other fields
- Industry partners or companies
- Government agencies or policymakers
- Non-governmental organizations or advocacy groups
- The general public
- Educators or students
- Other (please specify): *Click or tap here to type your answer.*

What is the potential impact of the data on the wider research community, industry, or society? (Select all that apply)

- Advancing scientific knowledge and discovery
- Driving innovation and economic growth
- Informing policy and decision-making
- Improving public health and well-being
- Enhancing education and training
- Enabling new technologies or applications
- Fostering international collaboration and partnerships
- Other (please specify): *Click or tap here to type your answer.*

How will you ensure that the data is discoverable and accessible to others who might be interested in using it? (Select all that apply)

- Depositing data in a trusted repository
- Providing metadata to enable discovery.
- Assigning persistent identifiers to the data
- Making data available through a standardized access protocol
- Enabling open access to the data
- Offering search keywords to optimize discovery.
- Providing documentation to validate data analysis and facilitate re-use.
- Other (please specify): [Click or tap here to type your answer.](#)

## FAIR Data

### FAIR Data- Making data findable, including provisions for metadata

#### 4.1 FAIR Data - Making data findable, including provisions for metadata

Will you assign a unique identifier to the data to ensure it can be consistently identified and cited?

Yes  No

Which identifier scheme(s) will you use for your data? (Select all that apply)

- DOI
- URN
- ARK
- PURL
- Other (Please specify) [Click or tap here to type your answer.](#)

Will rich metadata be provided to allow discovery?

Yes  No

What metadata will be created? (Select all that apply)

- Descriptive metadata (e.g., title, author, date, description)
- Administrative metadata (e.g., access restrictions, provenance, file format)
- Structural metadata (e.g., relationships between different data objects)
- Technical metadata (e.g., file size, resolution, software used)
- Other (Please specify): [Click or tap here to enter text.](#)

What disciplinary or general standards will be followed? (Select all that apply)

- Dublin Core
- Darwin Core
- DataCite Metadata Schema
- ISO/IEC 11179
- FGDC Metadata Standard
- EML (Ecological Metadata Language)
- Other (Please specify): [Click or tap here to enter text.](#)

Will the metadata be created manually or using automated tools?

- Manually
- Automated
- Both
- Not Applicable
- Other (Please specify): *Click or tap here to enter text.*

If metadata standards do not exist in your discipline, what type of metadata will be created and how will it be structured to enable discovery and interoperability?

Will search keywords or tags be provided in the metadata to optimize the possibility for discovery and then potential re-use?

- Yes  No

How will you select the keywords?

- Manually
- Using automated tools
- Combination of both.
- Other (Please specify): *Click or tap here to enter text.*

Will the keywords be standardized across the project or left to individual researchers to assign?

- Standardized across the project.
- Left to individual researchers to assign.
- Combination of both
- Other (Please specify): *Click or tap here to enter text.*

How will you ensure that the keywords accurately reflect the content of the data?

*Click or tap here to type your answer.*

Will the metadata be made available through a metadata repository or catalog that can be searched and indexed by search engines and other discovery services?

- Yes  No

Will the metadata be freely available or restricted to certain users or communities?

- Freely available
- Restricted to certain users.
- Restricted to certain communities.
- Other (Please specify): *Click or tap here to type your answer.*

## FAIR Data-Making data accessible

### FAIR Data - Making data Accessible Repository

Have you identified one or more trusted repositories to deposit the data and ensure its long-term preservation and accessibility?

*Click or tap here to type your answer.*

Have you confirmed that the identified repository meets the relevant standards and requirements for data management and preservation?

Yes  No

Will the repository assign a persistent identifier to the data, such as a DOI or URN, and ensure that the identifier resolves to the digital object?

Yes  No

## FAIR Data - Making data Accessible Data

Will all data generated by the project be made openly available, or will certain datasets be subject to restrictions?

- Openly available
- Certain datasets will be subject to restrictions.
- Other (Please specify): [Click or tap here to type your answer.](#)

If there are any restrictions on data access, what are the reasons for them, and how will they be enforced? (Select all that apply)

- Legal or ethical reasons
- contractual reasons
- There are no restrictions on data access.
- Other (Please specify): [Click or tap here to type your answer.](#)

How will these restrictions be enforced?

[Click or tap here to type your answer.](#)

Is an embargo period placed on any of the data? If so, what is the duration of the embargo and why is it needed?

[Click or tap here to type your answer.](#)

Will the data be accessible through a standardized access protocol, such as an API or web services?

Yes  No

If access to the data is restricted, how will access be granted to approved users, both during and after the end of the project? (Select all that apply)

- Password-protected access
- User authentication process
- Access to data is not restricted.
- Other (Please specify): [Click or tap here to type your answer.](#)

What measures will be put in place to verify the identity of users accessing the data?

- User registration process
- Two-factor authentication
- Other (Please specify): [Click or tap here to type your answer.](#)

How will you ensure that your data remains accessible and usable over time, including any necessary updates to metadata or other documentation?

- Regularly update metadata or documentation
- Use version control.
- Other (Please specify): [Click or tap here to type your answer.](#)

## FAIR Data - Making data Accessible

**Metadata: data used to describe other data. It summarizes basic information about data, which can make finding and working with instances of data easier.**

Will metadata describing the data be made openly available and licensed under a public domain dedication, such as CC0?

- Yes, metadata will be openly available and licensed under a public domain dedication.
- Metadata will be available, but not licensed under a public domain dedication.
- No, metadata will not be openly available.
- Other (Please specify): [Click or tap here to type your answer.](#)

Will the metadata be structured in accordance with relevant disciplinary or general standards to facilitate discovery and interoperability?

- Yes, disciplinary standards will be followed.
- Yes, general standards will be followed.
- Both disciplinary and general standards will be followed.
- No, standards will not be followed.
- Other (Please specify): [Click or tap here to type your answer.](#)

Will the metadata include sufficient information to enable users to access the data, such as links to the data or instructions for accessing it?

- Yes, links to the data will be provided.
- Yes, instructions for accessing the data will be provided.
- Yes, both links and instructions will be provided.
- No, neither links nor instructions will be provided.
- Other (Please specify): [Click or tap here to type your answer.](#)

How long will the metadata and data be available and findable, and how will they be maintained over time?

[Click or tap here to type your answer.](#)

If software is required to read or access the data, how will you ensure it?

- Documentation to the software will be included.
- References to the software will be included.
- Both documentation and references to the software will be included.
- Not applicable, software is not required to access or read the data.
- Other (Please specify): [Click or tap here to type your answer.](#)

Will the software be made available as open-source code?

- Yes, the software will be made available as open-source code.
- No, the software will not be made available as open-source code.
- Not applicable, software is not required to access or read the data

## FAIR Data- Making data interoperable

### FAIR Data - Making data interoperable

Have you identified relevant data and metadata standards and best practices for ensuring data interoperability within and across disciplines?

- Yes  No

Will you follow community-endorsed best practices for data interoperability, such as the FAIR principles?

Yes  No  Other (Please specify): [Click or tap here to type your answer.](#)

What data and metadata vocabularies, standards, formats, or methodologies will you follow to make your data interoperable to allow data exchange and re-use within and across disciplines? (Select all that apply)

- Dublin Core
- EML (Ecological Metadata Language)
- FGDC (Federal Geographic Data Committee) metadata standard
- ISO/TC 211 metadata standard
- Other (Please specify): [Click or tap here to type your answer.](#)

If you need to use project-specific or uncommon ontologies or vocabularies, how will you ensure that they are interoperable with more commonly used ones? (Select all that apply)

- Provide mappings to more commonly used ontologies.
- Work with experts in the field to ensure compatibility.
- Not applicable
- Other (Please specify): [Click or tap here to type your answer.](#)

Will you provide mappings or translations between your ontologies and more commonly used ones to facilitate interoperability?

Yes  No

Will you openly publish the ontologies or vocabularies you generate to enable others to reuse, refine, or extend them?

Yes  No

Will your data include qualified references to other data (e.g. other data from your project, or datasets from previous research) to enable users to contextualize, understand, and re-use your data?

- Yes, all relevant data will be referenced and properly cited.
- Yes, but only the most important or relevant data will be referenced.
- No, the data will not include any references to other data.

How will you ensure that the references are accurately recorded and that the linked data remain accessible over time? (Select all that apply)

- By using persistent identifiers such as DOIs or URNs
- By following relevant standards and best practices for data citation
- By providing detailed documentation on how to access the referenced data
- By ensuring the referenced data is deposited in trusted repositories with proper preservation and access policies
- Other (Please specify): [Click or tap here to type your answer.](#)

## FAIR Data- Increase data re-use

FAIR Data - Increase Data re-use

How will you provide documentation needed to validate data analysis and facilitate data re-use? (Select all that apply)

- Through readme files
- Through codebooks
- Through data dictionaries
- Other (Please specify): [Click or tap here to type your answer.](#)

Will the documentation include information on data cleaning, methodology, and variable definitions to help others understand and reproduce your analysis?

- Yes  No

How will you ensure that the documentation is clear, concise, and easily understandable by others? (Select all that apply)

- By hiring a technical writer
- By conducting usability testing
- By having non-experts review the documentation
- Other (Please specify): [Click or tap here to type your answer.](#)

Will you make your data freely available for maximum reuse and impact, and ensure compliance with relevant grant agreement obligations and standard reuse licenses such as Creative Commons?

- Yes, the data will be made freely available and licensed under Creative Commons or similar standard licenses.
- Yes, the data will be made freely available, but no license will be used.
- No, the data will not be made freely available.
- Other (Please specify): [Click or tap here to type your answer.](#)

Will the data produced in the project be useable by third parties, in particular after the end of the project?

- Yes  No

How will you ensure that the data remains accessible and useable by third parties, including after the end of the project? (Select all that apply)

- By depositing the data in a trusted repository
- By providing permanent identifiers to the data
- By documenting the data and metadata according to standards
- Other (Please specify): [Click or tap here to type your answer.](#)

Will you provide sufficient documentation and metadata to enable others to understand and reuse the data?

- Yes  No

How will you document the provenance of the data, including information on how it was collected, processed, and analyzed?

- By using appropriate metadata standards and vocabularies
- By providing detailed documentation and version control information
- Other (Please specify): [Click or tap here to type your answer.](#)

What processes and measures will you use to ensure the quality, accuracy, completeness, consistency, and freedom from errors or bias of the data?

- Validation checks or error detection routines.
- Manual data review and verification
- Peer review or quality control procedures
- Statistical methods or software tools for data analysis and validation
- Other (Please specify): [Click or tap here to type your answer.](#)

Will you provide information on any limitations or assumptions associated with the data to help third parties interpret and use it appropriately?

Yes  No

## Other Research Outputs

### Other research outputs

Which research outputs other than data will be generated and/or re-used throughout the project? (Select all that apply)

- Software
- Workflows
- Protocols
- Models
- Physical materials
- Other (Please specify): [Click or tap here to type your answer.](#)

How will you manage and preserve these outputs to ensure their long-term accessibility and usability? (Select all that apply)

- Store them in a trusted repository.
- Use appropriate metadata standards and documentation to describe and facilitate re-use.
- Use appropriate license to ensure that they can be freely reused and repurposed by others.
- Other (Please specify): [Click or tap here to type your answer.](#)

How will you ensure that research outputs other than data are managed and shared in line with the FAIR principles? (Select all that apply)

- Use appropriate metadata standards and documentation to describe and facilitate re-use
- Publish them using an appropriate license to ensure that they can be freely reused and repurposed by others.
- Make them available through a trusted repository or other public platforms.
- Other (Please specify): [Click or tap here to type your answer.](#)

How will you manage and share physical materials or other non-digital outputs?

[Click or tap here to type your answer.](#)

How will you allocate resources to support the management and sharing of research outputs other than data?

*What resources, such as storage, curation, or dissemination, will be necessary to support the management and sharing of these outputs? How will you ensure that sufficient resources are allocated to support the long-term preservation and accessibility of these outputs?*

[Click or tap here to type your answer.](#)

## Allocation of Resources

### Allocation of resources

Have you identified the specific costs associated with making your data and other research outputs FAIR, including costs related to storage, curation, and dissemination?

**How will you allocate resources to support data management and sharing activities, such as storage, curation, and dissemination?**

- By hiring dedicated data management personnel**
- By allocating funds to purchase necessary hardware and software**
- By using cloud-based storage and curation services**
- Other (Please specify):** *Click or tap here to type your answer.*

**How will these costs be covered, and what funding sources will be used to support data management activities?**

*Will these costs be covered by the HORIZON EUROPE grant or other funding sources, and what are the conditions and limitations of these funding sources? How will you ensure that sufficient resources are allocated to support the necessary data management activities throughout the project lifecycle?*

*Click or tap here to type your answer.*

**Who will be responsible for data management in your project, and what are their specific roles and responsibilities?**

*Have you identified a specific individual or team who will be responsible for data management activities, such as data curation, documentation, and dissemination? What are their specific roles and responsibilities, and how will they work with other project staff to ensure that data management activities are integrated into project workflows?*

*Click or tap here to type your answer.*

**How will long-term preservation of data be ensured, and what resources will be necessary to accomplish this, including costs and potential value, who decides and how, what data will be kept, and for how long?**

*Have you identified a specific plan for the long-term preservation and accessibility of your data, including the necessary resources and infrastructure? Who will be responsible for deciding which data to keep and for how long, and what factors will be considered in these decisions? How will you ensure that the data is preserved and made accessible in a sustainable and responsible way, taking into account ethical and legal considerations?*

*Click or tap here to type your answer.*

## Data Security

### Data Security

**Have you identified the potential risks and threats to data security, such as unauthorized access or data loss, and developed a plan to mitigate these risks?**

- Yes, potential risks and threats to data security have been identified, and a plan to mitigate these risks has been developed.**
- No, potential risks and threats to data security have not been identified yet.**
- Other (Please specify):** *Click or tap here to type your answer.*

**What are these potential risks and threats identified? (Select all that apply)**

- Unauthorized access by hackers or cybercriminals
- Accidental data loss or corruption
- Data breaches resulting from inadequate security measures.
- Insider threats, such as employees mishandling data or deliberately leaking it
- Natural disasters or other environmental risks
- Cyber-attacks from foreign governments or state-sponsored actors
- Other (Please specify): *Click or tap here to type your answer.*

What is the plan to mitigate those risks?

*Click or tap here to type your answer.*

What provisions are or will be in place for data security, including measures for data recovery, secure storage and archiving, and transfer of data?

*Click or tap here to type your answer.*

Will the data be safely stored in trusted repositories for long-term preservation and curation?

Yes  No

Have you identified the relevant ethical and legal frameworks for data security and privacy, such as GDPR or other data protection regulations?

- GDPR (General Data Protection Regulation)
- NIS II Directive
- Data Governance Act (DGA)
- Other (Please specify): *Click or tap here to type your answer.*

What measures will be in place to ensure compliance with these frameworks?

- Obtaining informed consent from participants.
- Anonymizing or de-identifying sensitive data.
- Implementing access controls to limit data access to authorized personnel only.
- Other (Please specify): *Click or tap here to type your answer.*

How will you ensure that data security and privacy considerations are integrated into project workflows and activities throughout the project lifecycle?

- Including data security and privacy considerations in project planning and design
- Providing regular reminders or training on data security and privacy to staff
- Periodically reviewing and updating data security and privacy measures
- Other (Please specify): *Click or tap here to type your answer.*

Does your organization have a Data Protection Officer?

- Yes
- No
- Other (Please specify): *Click or tap here to type your answer.*

What measures will you put in place to ensure that data security and ethical considerations are addressed throughout the project lifecycle?

- By implementing appropriate access controls and encryption.
- By conducting privacy impact assessments.
- By complying with relevant ethical and legal requirements.
- Other (Please specify): *Click or tap here to type your answer.*

## Ethics

### Ethics

Have you identified any potential ethical or legal issues related to data sharing, such as privacy concerns or issues related to intellectual property rights? If so, how will these issues be addressed, and what measures will be in place to ensure compliance with relevant ethical and legal frameworks.

*Click or tap here to type your answer.*

Have you sought an evaluation/approval from an Ethics Committee? If yes, please explain why.

*Click or tap here to type your answer.*

## Personal Data

### Personal Data Handling

Will you collect/process any personal data?

Yes  No

If yes, what personal data will you collect/process

*Click or tap here to type your answer.*

How will you collect the personal data?

*Click or tap here to type your answer.*

What is the purpose of the personal data processing and its relation to the objectives of the project? (Please specify, by showing that the data you will collect are proportional and limited to the objectives of the project following the data minimization principle).

Will you process any “special categories of personal data” (racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, sex life or sexual orientation), and if so, for what purpose?

*Click or tap here to type your answer.*

Will informed consent be obtained from individuals providing personal data, and how will this consent be documented and stored?

- Yes, consent will be obtained and documented using a consent form.
- Yes, consent will be obtained and documented using other methods (please specify): *Click or tap here to type your answer.*
- No, consent will not be obtained.
- Not applicable to my research.

**Will informed consent be obtained from data subjects for data sharing and long-term preservation?**

- Yes
- No
- Not applicable

**If not, under which legal basis will you process personal data?**

*Click or tap here to type your answer.*

**Are you going to transfer /share personal data? If yes, where and how will you transfer them**

*Click or tap here to type your answer.*

**Are there any ethical or legal issues that can have an impact on data sharing?**

*Click or tap here to type your answer.*

**Will you safely store data in certified repositories for long time preservation and curation?**

*Click or tap here to type your answer.*

**Will you process any previously collected personal data (including use of pre-existing data sets or sources, merging existing data sets etc.)? If yes, under which legal basis?**

*Click or tap here to type your answer.*

**Have you identified the potential risks and threats to personal data security, such as unauthorized access or data loss, and developed a plan to mitigate these risks?**

- Yes, potential risks and threats to personal data security have been identified, and a plan to mitigate these risks has been developed.
- No, potential risks and threats to personal data security have not been identified yet.
- Other (Please specify): *Click or tap here to type your answer.*

**What provisions are or will be in place for data security, including measures for data recovery, secure storage and archiving, and transfer of personal data?**

*Click or tap here to type your answer.*

**Does your organization have a Personal Data Management Plan in place (please explain)?**

*Click or tap here to type your answer.*

Did you put in place any of the following meters to comply with the GDPR or equivalent legislation?

- Data protection Impact Assessment (DPIA)
- Designate a Data Protection Officer (DPO)
- Oversight mechanisms for data processing (limited access by qualified members, mechanisms for logging data access and modifications)
- Measures to enhance privacy by design and default (e.g. anonymization, encryption, pseudonymization)

Did you consult your institution's DPO concerning the legitimacy of these processing activities?

*Click or tap here to type your answer.*

## Artificial Intelligence

### Artificial Intelligence

Will you be using AI tools or systems?

- Yes  No

If yes, state what are these tools or describe the AI systems.

*Click or tap here to type your answer.*

Will the data holder be informed of the use of AI tools and systems prior?

- Yes  
 No  
 Not Applicable

Will there be continuous human supervision?

- Yes  
 No  
 Not Applicable

Could the use of the AI tools or AI systems raise ethical concerns related to human rights and values and detail how this will be addressed?

*Click or tap here to type your answer.*