State-of-the-art sustainable energy efficiency technologies roadmap for waterborne transport towards the fit-for-55 guidance compliance

Project 101192661— FLEETfor55

Deliverable D1.3 – Initial Data Management Plan

Co-funded by the European Union

Disclaimer

Co-funded by the European Union
Project 101192661 — FLEETfor55 — HORIZON-CL5-2024-D5-01

Co-funded by the European Union (Horizon Europe, FLEETfor55, GA no. 101192661). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union (EU) or the European Climate, Infrastructure and Environment Executive Agency (CINEA). Neither the European Union nor the granting authority can be held responsible for them.
The information presented in this document are confidential.

Document Info

Document	
Title	State-of-the-art sustainable energy efficiency technologies roadmap for waterborne transport towards the fit-for-55 guidance compliance
Acronym	FLEETfor55
Call	HORIZON-CL5-2024-D5-01
Type of Action	Innovation Action
Grant Number	101192661
Start date	01/01/2025
Duration	42 months
Document identifier	D1.3 – Initial Data Management Plan
Due Date of Delivery to EC	30/06/2025
Actual Date of Delivery to EC	30/06/2025
Dissemination level	PU – Public
Delivery Type	DMP – Data Management Plan
Work package	WP1
Related Tasks	T1.4
Lead Beneficiary	5 - UPAT

Contributor(s)	
Main Contributor(s)	5 - UPAT
Contributor(s)	5 - UPAT, ALL
Reviewers (s)	7 - NTNU, 10 - AES

History Sheet			
Version	**Date**	**Editor**	**Summary of Modifications**
v0.1	02.06.2025	Angelos Filippatos (UPAT), Nikolaos Dimoglis (UPAT), Dionysios Markatos (UPAT), George Kouvaras (UPAT)	First Draft
v0.2	24.06.2025	Andreas Roppelt (AES), Johans Jacobo (NTNU)	Review – AES & NTNU input
v1.0	26.06.2025	Angelos Filippatos (UPAT), Nikolaos Dimoglis (UPAT), Dionysios Markatos (UPAT), George Kouvaras (UPAT) Lydia Sfyraki (HYD) Astrinos Papadakis (HYD)	Comments and partners' input incorporated, Final Version

Acronyms and Abbreviations	Meaning
AAI	Authentication and Authorization Infrastructure
ABS	AMERICAN MPIRO OF SIPING HELLENIC MONOPROSOPI ETAIREIA PERIORISMENIS EVTHINIS
AES	ATLANTEC ENTERPRISE SOLUTIONS GMBH
CC0	Creative Commons Zero
CO	Project Coordinator
CSM	COLUMBIA SHIPMANAGEMENT LTD
CSV	Comma Separated Values
DMP	Data Management Plan
DOI	Digital Object Identifier
DST	ENTWICKLUNGSZENTRUM FUR SCHIFFSTECHNIK UND TRANSPORTSYSTEME EV
EET	Energy Efficiency Technology
EIF	European Interoperability Framework
EOSC	European Open Science Cloud
EPS	EPSILON INTERNATIONAL LTD
EU	European Union
FAIR	Findability Accessibility Interoperability Reusability
FCSI	FINCANTIERI SI SPA
GA	Grant Agreement
GDPR	General Data Protection Regulation
HYD	HYDRUS ANOTATI SYNEKTIKI MICHANIKI ETAIREIA SYMVOULON ANONYMI ETAIREIA
HTTP	HyperText Transfer Protocol
IP	Intellectual Property
JPEG	Joint Photographic Experts Group
JSON	JavaScript Object Notation
MP4	MPEG-4 Part 14
LoI	Letter of Intent
NetCDF	Network Common Data Form
NTUA	ETHNICON METSOVION POLYTECHNION
PDF	Portable Document Format
PID	Persistent Identifier
PNG	Portable Network Graphics
RDA	Research Data Alliance
RDF	Resource Description Framework

Acronyms and Abbreviations	Meaning
RINA	RINA SERVICES SPA
SEKAVIN	SEKAVIN AE
SPSS	Statistical Package or the Social Sciences
TIN	Technology Innovation Network
UoS	UNIVERSITY OF STRATHCLYDE
UPAT	PANEPISTIMIO PATRON
VPF	FUNDACION DE LA COMUNIDAD VALENCIANA PARA LA INVESTIGACION
WML	GOUOTERMELON SYMVOULEUTIKI I.K.E.
WP	Work Package
XML	eXtensive Markup Language

Table of Contents

Document Info **4**

Table of Contents **8**

List of Figures **10**

List of Tables **11**

Executive Summary **12**

1 Data Management Policies **13**

1.1 Open-Science Practices 13

1.2 FAIR Principles 13

1.3 FAIR Model Indicators & “FAIRification” 16

2 Data Collection, Handling and Documentation **18**

2.1 Collaborative Structure in FLEETfor55 18

2.2 Data Collection and Summary 20

2.3 FAIR Data Policy Alignment 25

2.3.1 Findability 28

2.3.2 Accessibility 28

2.3.3 Interoperability 30

2.3.4 Re-usability 30

2.4 Other Research Outputs 31

2.5 Data Security 33

2.6 Ethical Aspects 36

2.7 Other Aspects 38

3 Data Storage and Sharing **40**

3.1 Infrastructure 40

3.2 Backup-Protocol 41

Conclusions **41**

4 ANNEX..... 43

4.1 Questionnaire 43

5 References 51

List of Figures

Figure 1: Summary of types of data generated within the project 22
Figure 2: Formats of data generated within the project 23
Figure 3: The number of data origin sources of the partners' data 25
Figure 4: Selection of Persistent Identifier for data and metadata 28
Figure 5: Dissemination Level of the generated datasets 30
Figure 6: Ways to increase data Interoperability, data exchange and reuse by providing metadata 30
Figure 7: Expected purposes for data re-use 31
Figure 8: Measures that are applied on each organization to ensure data security 35
Figure 9: Ethical or legal issues that may emerge and impact data sharing 38
Figure 10: Other national / funder / sectorial / departmental procedures be used for data management 40
Figure 11: Structure of FLEETfor55 Teams folders 41
Figure 12: Questionnaire - First sheet – Instructions 43
Figure 13: Questionnaire - Second sheet – Data Summary [questions 1, 2] 44
Figure 14: Questionnaire - Second sheet – Data Summary [questions 3, 4, 5, 6] 45
Figure 15: Questionnaire - Second sheet – Data Summary [questions 7, 8] 46
Figure 16: Questionnaire - Third sheet – FAIR Data [Findability, Accessibility] 47
Figure 17: Questionnaire - Third sheet – FAIR Data [Interoperability, Reusability] 48
Figure 18: Questionnaire - Fourth sheet – Other Research outputs 49
Figure 19: Questionnaire - Fifth Sheet – Data Security 49
Figure 20: Questionnaire - Sixth Sheet - Ethics 49
Figure 21: Questionnaire - Seventh Sheet – Other Issues 50

List of Tables

Table 1: Connection of Interoperability Strategies to the corresponding categories [14] 15

Table 2: FAIR Data Maturity Model indicators 16

Table 3: Foundational data attributes of FLEETfor55 Project 20

Table 4: Detailed data attributes of FLEETfor55 Project 23

Table 5: Actions to ensure alignment with FAIR Data Policy 25

Table 6: FAIR data summary of partners' feedback 27

Table 7: Other Research Outputs – Summary of Partner selections 32

Table 8: Data Security – Summary of Partner selections 33

Table 9: Protection measures and consent requirements in terms of data management. 36

Table 10: Other Aspects – Summary of Partner selections 38

Executive Summary

FLEETfor55 project is an innovative project that focuses on the assessment, integration and exploitation of emission reduction and efficiency improvement technologies, also known as Energy Efficiency Technologies (EETs) within the maritime sector. The Consortium consists of 23 partners from 9 different countries, performing extensive collaborative work that will generate plenty of research data that will contribute toward a range of research outputs data namely publications, executive summaries, commercial exploitation etc. Data management presents a significant challenge, impacting both the internal communication of project partners and the potential utilization of post project data. Research data in any project forms the basis of scientific and engineering knowledge, sets the foundation for future research and must be properly managed to ensure successful project completion.

In this framework, the management of the research data based on subject-specific standards, the creation of explanatory metadata, the secure storage of data, and the long-term preservation of data after the completion of FLEETfor55 project — along with other standard data management practices — are essential for both the quality assurance of the project and facilitation of the reusability of research outcomes. The current report, performs a preliminary analysis of the FLEETfor55 project data as defined by Consortium partners and finally develops the FLEETfor55 Initial Data Management Plan. Given the current early stages of the project, fourteen out of twenty-three (14/23) partners provided feedback. Thus, the guidelines and rules are subject to change, as updated requirements emerge from all the partners.

1 Data Management Policies

This section presents the most commonly adopted data management policies. These policies are guided by the rules and regulations of the European Union and emphasize the compliance with Open-Science Practices [1] as well as the FAIR Principles (Findable, Accessible, Interoperable, and Reusable) [2].

1.1 Open-Science Practices

FLEETfor55 project as part of the call HORIZON-CL5-2024-D5-01 is obliged to follow the Open-Science practices as mentioned in the project's Grant Agreement (GA). Open Science refers to an approach to research that focuses on prompt and widespread distribution of research results, information and tools [3]. The benefits of Open-Science principles are various and contribute to making scientific process transparent. First and foremost, the adoption of such practices enhances collaborations and sharing of knowledge, resulting in advancement both with regards to scientific progress as well as societal benefit [4]. In addition, since everyone can access and reuse the knowledge in a uniform and structured format the linguistic gap in scientific information is being bridged [4]. Finally, the implementation of Open-Science practices widens the creation, evaluation and communication of scientific knowledge beyond the traditional scientific community [4].

In addition to the benefits of Open-Science Practices in improving accessibility of the research outputs, the protection of Intellectual Property (IP) [5] rights and sensitive data remains a top priority. In that framework, the '*as open as possible, as closed as necessary*' principle is at the forefront of the Open-Science Practices. This principle reflects on the idea that research data should be openly accessible unless doing so would compromise the interests of the beneficiaries, in which case restrictions are justified [3].

1.2 FAIR Principles

Many challenges arise throughout the execution of the Data Management Plan (DMP). One of the highest-ranking objectives is to facilitate knowledge and data discovery, access, and re-use when a search is conducted either from a human or automated methods. To implement that objective, the term FAIR was launched in 2014 and the FAIR guiding principles in 2016 [6]. FAIR summarizes that all research objects should be Findable, Accessible, Interoperable and Reusable. The FAIR framework consists of fifteen (15) guiding principles, with the primary goal of incorporating the most relevant and applicable ones into the Data Management Plan (DMP) for the FLEETfor55 Project.

Findability

The first term of FAIR principles, Findability, emphasizes that digital resources should be easy to find for both humans and computers. To ensure compliance with this term, both data and metadata should be assigned a globally unique and Persistent Identifier (PID) - usually Digital Object Identifier (DOI) [7] - and be archived in a trusted repository.

The main dataset should be described with rich metadata, updated concurrently with the data, as a digital resource which is not well described cannot be located. The format of metadata is usually generated based on certain standardizations and it should follow the guide of minimal information, as any additional information would be a waste of time and resources. Moreover, each metadata must contain the Persistent Identifier (PID) [8] of the described resource.

Accessibility

As stated in the Grant Agreement (GA) and outlined in Section 1.1, FLEETfo55 project must align with the Open-Science scheme, which ensures open access to as many datasets as possible. However, certain datasets may contain confidential or personal information. To address this potential conflict, personal data must be processed lawfully, and appropriate measures should be implemented to ensure data security.

Accessibility, as defined by FAIR principles, refers not only to making data available but also ensuring that users can reliably retrieve it under well-defined conditions [9]. Data and metadata must comply with a standardized communications protocol, which is open, free and uniformly applicable. Where it is necessary, the protocol must support secure authentication and authorization procedures, allowing access to sensitive data only to those with appropriate rights [2].

Interoperability

Interoperability is defined by the European Interoperability Framework (EIF) as the "*ability of organizations to interact towards mutually beneficial goals, involving the sharing of information and knowledge between these organizations, through the business process they support, by means of the exchange data*" [10]. Interoperability is categorized into four (4) pillars:

- Technical: Regards for the ability of different systems, devices and applications to connect, communicate and exchange data effectively [11],
- Semantic: Ensures that the meaning of data is preserved and well understood consistently across systems [12],

- Organizational: Aligns with project's processes, policies and responsibilities to support collaborative data use [13], and
- Legal: Ensures that data exchange and reuse comply with existing policies, laws, licensing requirements [13].

Table 1 contains recommendations and strategies for each of the four interoperability categories.

Table 1: Connection of Interoperability Strategies to the corresponding categories [14]

Categories	Strategies
Technical	• Open Science scheme • Common security and privacy framework (Authorization & Authentication) • Easy to understand Service -level Agreements • Easy access to data sources available in different formats • Consistent PID selection policy
Semantic	• Accurately and publicly accessible definitions for all terms • Open licenses preferred • Specific rules and guidelines, protocols • Minimum required metadata model
Organizational	• Standardized data formats with their corresponding metadata • Management of permanent organization names and functions
Legal	• Knowledge and support on copyrights and licenses • CC0 permissive license preferred (allows re-use, modification, distribution of datasets) • Identification of different parts of a dataset and their corresponding licenses • Specification of license evolution for datasets • Follow GDRP for personal data • Alignment with EU legislation

Re-usability

The last term of FAIR principles to be considered is the Re-usability of research outputs. To ensure reusability, the tools used (e.g., software) should, if possible, be open source, and each dataset should be accompanied by findable metadata. Metadata should include sufficient instructions for access or reuse and contain significant and meaningful information. To facilitate reuse, any applicable license should be easily discoverable. Additionally, the provenance of the data must be clearly documented – including information about how and by whom the data was generated, what is the data origin, and the resources involved, as well as ownership information.

1.3 FAIR Model Indicators & "FAIRification"

Apart from implementing the FAIR Principles it is also essential to assess them, to ensure that research data can be shared, discovered and reused across scientific disciplines. To effectively assess the FAIR Principles, a structured measuring approach should be adopted translating the principles to measurable metrics or indicators. The Research Data Alliance (RDA) group has defined forty-one (41) FAIR data maturity model indicators [15], categorized in three (3) levels based on importance: essential, important and useful (see Table 2). These metrics have been transferred on an online tool, generated from the EU project FairSFair, F-UJI [16].

Table 2 illustrates the FAIR Data Maturity Model indicators, as defined by RDA, which serves as a framework for assessing compliance with FAIR principles. The "Prioritization column contains three (3) available options: (i) Essential which is a must have, (ii) Important which is a should and (iii) Useful could have. The indicators of the FAIR principles are presented in the Table 2 as recommendations and guidelines, to assist partners align with the FAIR principles. It is not an essential part of the DMP.

Table 2: FAIR Data Maturity Model indicators

FAIR	Indicator	Priority
F1	Metadata is identified by a Persistent Identifier	Essential
F1	Data is identified by a Persistent Identifier	Essential
F1	Metadata is identified by a globally unique identifier	Essential
F1	Data is identified by a globally unique identifier	Essential
F2	Rich metadata is provided to allow discovery	Essential
F3	Metadata includes the identifier for the data	Essential
F4	Metadata is offered in such a way that it can be harvested and indexed	Essential
A1	Metadata contains information to enable the user to get access to the data	Important
A1	Metadata can be accessed manually (i.e. with human intervention)	Essential
A1	Data can be accessed manually (i.e. with human intervention)	Essential
A1	Metadata identifier resolves to a metadata record	Essential
A1	Data identifier resolves a digital object	Essential

FAIR	Indicator	Priority
A1	Metadata is accessed through standardized protocol	Essential
A1	Data is accessible through standardized protocol	Essential
A1	Data can be accessed automatically (i.e. by a computer program)	Important
A1.1	Metadata is accessible through a free access protocol	Essential
A1.1	Data is accessible through a free access protocol	Important
A1.2	Data is accessible through an access protocol that supports authentication and authorization	Useful
A2	Metadata is guaranteed to remain available after data is no longer available	Essential
I1	Metadata uses knowledge representation expressed in standardized format	Important
I1	Data uses knowledge representation expressed in standardized format	Important
I1	Metadata uses machine-understandable knowledge representation	Important
I1	Data uses machine-understandable knowledge representation	Important
I2	Metadata uses FAIR-compliant vocabularies	Useful
I2	Data uses FAIR-compliant vocabularies	Useful
I3	Metadata includes references to other metadata	Important
I3	Data includes references to other data	Useful
I3	Metadata includes references to other data	Useful
I3	Data includes qualified references to other data	Useful
I3	Metadata includes qualified references to other metadata	Important
I3	Metadata include qualified references to other data	Useful
R1	Plurality of accurate and relevant attributes are provided to allow reuse	Essential
R1.1	Metadata includes information about the license under which the data can be reused	Essential
R1.1	Metadata refers to a standard reuse license	Important
R1.1	Metadata refers to a machine-understandable reuse license	Important

FAIR	Indicator	Priority
R1.2	Metadata includes provenance information according to community-specific standards	Important
R1.2	Metadata includes provenance information according to a cross-community language	Useful
R1.3	Metadata complies with a community standard	Essential
R1.3	Data complies with a community standard	Essential
R1.3	Metadata is expressed in compliance with a machine-understandable community standard	Essential
R1.3	Data is expressed in compliance with a machine-understandable community standard	Important

Most of the requirements regarding the findability and accessibility section of FAIR Principles can be achieved at the metadata level, whereas the interoperability and reusability sections require additional actions at the data level. The 'FAIRification' process (outlined by GO FAIR) suggests seven (7) steps, which defines the necessary actions in order to coordinate a dataset with FAIR principles [17]. It begins with the retrieval and analysis of the non-FAIR data, followed by the definition of the semantic & metadata model. Next, the data are made linkable, a suitable license is assigned, corresponding metadata is defined and finally the "FAIRified" dataset is published along with its metadata.

2 Data Collection, Handling and Documentation

Building on the foundational principles of FAIR and Open-Science, this section begins by analysing the collaborative structure of the FLEETfor55 project. Then, it identifies the types of data involved in the project, based on the partners feedback, and proposes recommendations for the development of the project's Data Management Plan (DMP).

2.1 Collaborative Structure in FLEETfor55

In addition to involving multiple partners from various regions across the EU, the FLEETfor55 project is structured into numerous Work Packages (WPs) and Tasks, each assigned to different partners, along with the Technology Innovation Network (TIN) (described below). This structure makes the coordination and collaboration of all partners a challenging process. This report aims to simplify this process by first understanding the types of collaborations found within the FLEETfor55 project. The identified data collaboration types can be summarized as follows:

- Exchange of Knowledge,
- Exclusive Data Network,
- Research and Data Pool,
- Connection to Industry

The **"Exchange of Knowledge"** is a fundamental aspect of collaboration that cannot be easily documented. It involves the sharing of experiences, insights and scientific hypotheses between the institutions. This process is characterized by ongoing dialogue and informal sharing – not purely technical – but essential for the completion of the project. It ensures that the strategies adopted are based on scientifically validated foundations.

In the case of the **"Exclusive Data Network"**, the sharing of data and knowledge is more formal, as it is expected to follow a standardized file sharing solution. This type of collaboration is most commonly found within each WP, where the flow of information tends to be linear. The institutions that work together in this context may share data exclusively among themselves.

With regard to **"Research and Data Pool"**, as the project progresses and individual Tasks and WPs conclude, the data generated within each WP should be fully and unrestrictedly accessible to all participating institutions. This type of access ensures that the evolving project requirements of each individual WP can be met effectively. In more practical terms, this model of collaboration involves storing scientific / research data in a secure central server, that enables partners to both share and access all possible types of data.

Finally, one of the key contributions, introduced by the FLEETfor55 project, is the establishment of the **Technology Innovation Network (TIN)**. This external board is initially formed by sixteen (16) Energy Efficiency Technologies (EETs) providers, who have formally confirmed their participation by signing Letters of Intent (LoIs), and it is expected to expand to at least thirty-five (35) members by the end of Month 6 (M06). The TIN serves as a bridge between the Consortium and the industry and can be characterized as the **"Connection to Industry"** collaboration that enables a two-way exchange of insights, data, and practical requirements. By engaging directly with EET providers, the project ensures that the research is based on real-world information and data, enhancing its relevance, applicability, and impact. This type of collaboration is more complex than internal knowledge-sharing models and requires clear communication, formal data-sharing arrangement as well as templates to facilitate efficient and secure information exchange.

2.2 Data Collection and Summary

FLEETfor55 project incorporates data from multiple sources – some derive from experiments, others from models or analytical solutions – and as a result there is a significant variation in terms of data type, format, size and origin of data. In addition to challenges related to data themselves, several issues arise – namely the dissemination level of data (whether the data can be publicly accessible), the potential for data re-use and the specific Tasks and WPs responsible to generate data. To address these issues, the Data Management Team developed a comprehensive questionnaire that aims to collect as much relevant information as possible to establish the complete picture of the data. At this initial stage of the project, data has been collected from approximately more than half of the Consortium partners i.e. 14/23. For the remaining partners, relevant data is either not yet available, currently under internal validation, or scheduled for collection in later project stages. The DMP will be updated as additional data contributions are received, ensuring full coverage over the course of the project. For the contributing partners that completed this questionnaire in detail, the results are summarized in Table 3 & Table 4. The scope of the questionnaire extended further to the issues that were described previously and accounted for specific institutional data policies of each partner, the potential ethical consideration that might arise regarding the data management and various other issues that will be explained within the next sections. Table 3 presents the foundation attributes for the data that are expected to be generated within the FLEETfor55 Project.

Table 3: Foundational data attributes of FLEETfor55 Project

Partner	WPs / Tasks	Data Type	Data Format	Data Size
ABS	T4.6	Textual	PDF	Small
AES	T6.1, T6.3	Textual, Simulated	CSV, Excel, JSON, XML, TXT, JPEG, PNG, MP4, PDF	Medium
CSM	T8.5, T8.6	Quantitative, Qualitative, Geospatial, Textual, Sensor	CSV, Excel, JSON, XML, TXT, JPEG, PNG, MP4, PDF	Very Large
DST	WP2, WP3, WP4	Quantitative, Multimedia, Textual, Simulated	CSV, Excel, SPSS, JPEG, PNG, MP4, PDF	Large
EPS	T5.2, T5.5, T6.4	Quantitative, Qualitative, Textual	Excel, TXT, PDF	N/A
FCSI	T4.5	Qualitative	PDF	Small

Partner	WPs / Tasks	Data Type	Data Format	Data Size
HYD	WP2, WP3, WP9	Quantitative, Qualitative, Multimedia, Textual, Simulated	CSV, Excel, XML, TXT, JPEG, PNG, MP4, PDF	Large
NTUA	WP2, WP3, WP4, WP8	Quantitative, Qualitative, Multimedia, Textual, Simulated	CSV, Excel, XML, TXT, MATLAB, JPEG, PNG, PDF	N/A
RINA	T3.1, T3.2	Qualitative, Textual	Excel, TXT, PDF	Large
SEKAVIN	N/A	Quantitative, Qualitative, Textual	CSV, Excel, TXT	N/A
UoS	T5.1, T5.3, T5.4	Quantitative, Qualitative, Multimedia, Textual, Simulated	CSV, Excel, TXT, JPEG, MP4, PDF	Medium
UPAT	WP1, WP2, WP5, WP6, WP7, WP8	Quantitative, Qualitative, Textual, Simulated	CSV, Excel, TXT, MATLAB, PDF	Very Large
VPF	T8.1, T8.3, T8.5, WP9	Quantitative, Qualitative, Textual	EXCEL, TXT, JPEG, PNG, PDF	Large
WML	T2.3, T8.2, T9.4	Quantitative, Qualitative, Textual, Simulated	CSV, Excel, PDF	N/A

To better capture the nature of the Partners' data, the specific sub-types for each category were also obtained. For example, for the "Multimedia Data" category distinctions were made between the videos, audio recording or images. The questionnaire provided predefined options for selection, but partners were also encouraged to provide additional options based on their experience. The results for the specific sub-types based on partners' input are illustrated in Figure 1. In addition, regarding the expected data format, the majority of the partners indicated that most data will be generated in PDF format, followed closely by Excel spreadsheets, with CSV (.csv) [18] and TXT (.txt) files also close, as illustrated from Figure 2. Finally, in terms of expected data size, the majority of the dataset are expected to range from Large (10 GB to 100 GB) to Very Large (100 GB to 1 TB).

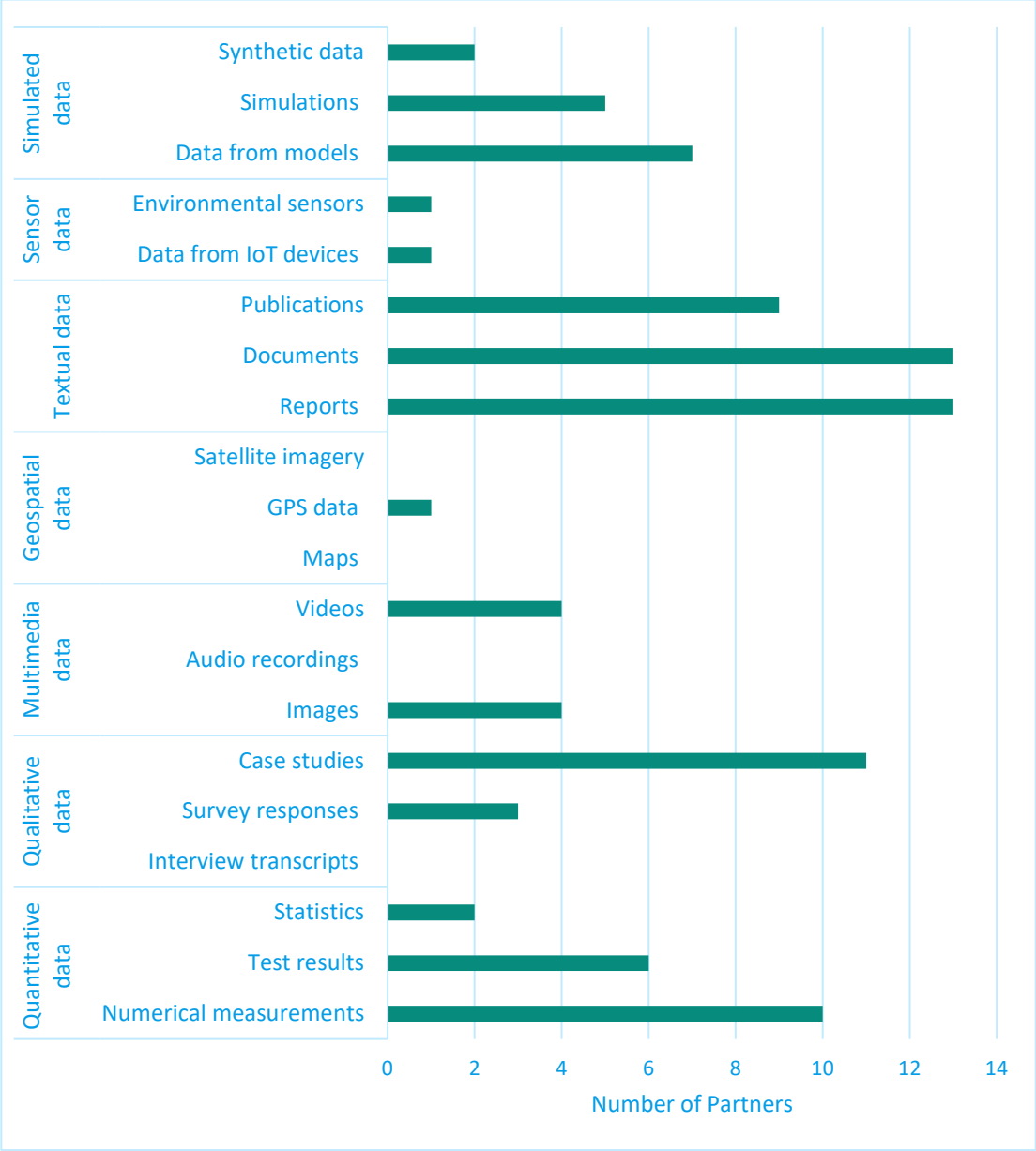

Figure 1: Summary of types of data generated within the project

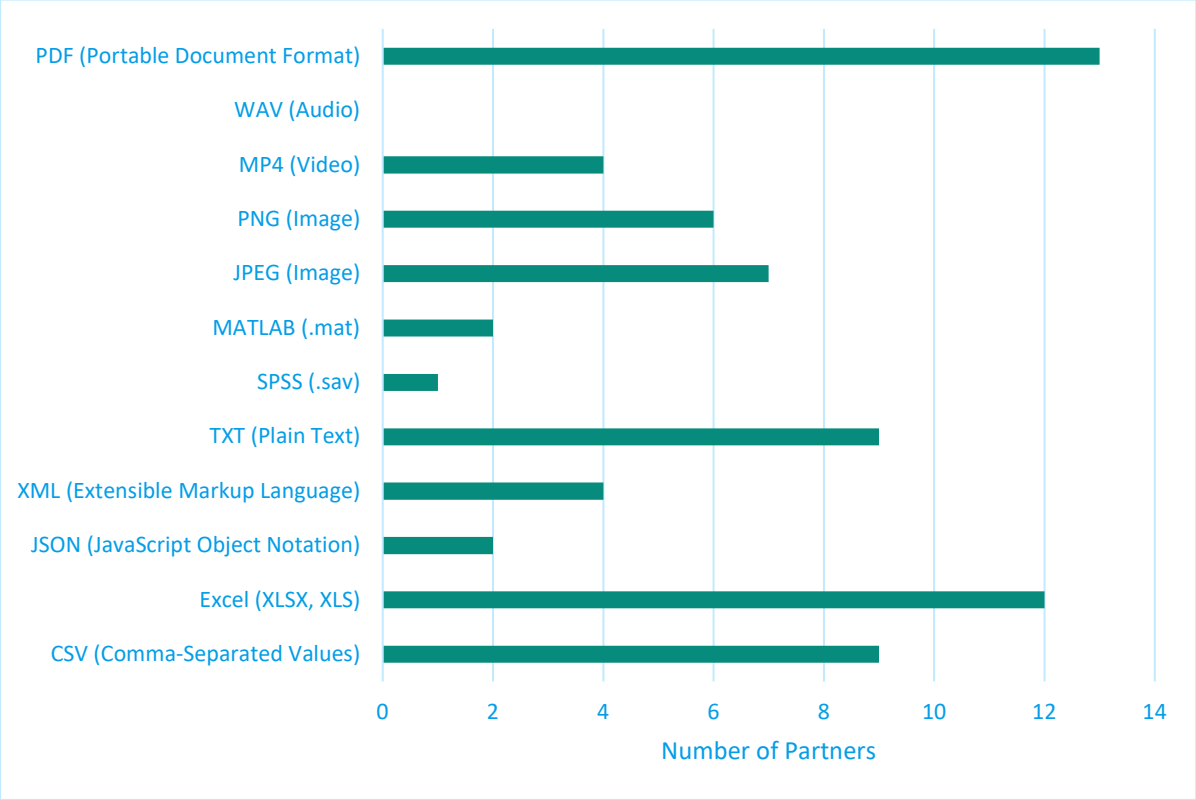

Figure 2: Formats of data generated within the project

Apart from the foundational data attributes of the generated data presented in Table 3, a more detailed overview of the generated data -including their origin, potential for re-use and anticipated dissemination level - is provided in Table 4. Regarding the Dissemination Level, multiple types of dissemination are indicated for each partner, which may initially appear conflicting – such as simultaneous selection of open access and confidential. However, this can be justified by the nature and variety of data being generated, as different datasets may require different dissemination strategies.

Table 4: Detailed data attributes of FLEETfor55 Project

Partners	Data Origin	Reusage of Data	Dissemination Level
ABS	Collaboration, Proprietary	Yes	Open access, Confidential
AES	Collaboration, Proprietary, Self-generated, External Resources	Yes	Open access, Restricted access, Internal Use only
CSM	Proprietary, Self-generated, External Resources	Yes	Open access, Restricted access, Internal Use only, Confidential

Partners	Data Origin	Reusage of Data	Dissemination Level
DST	Previously collected data from prior projects, Proprietary, Self-generated, External Resources	Yes	Open access, Restricted access, Internal Use only, Confidential
EPS	Public repositories, Collaboration, Previously collected data from prior projects, External Resources	Yes	
FCSI	Previously collected data from prior projects, Self-generated, External Resources	Yes	
HYD	Collaboration, Previously collected data from prior projects, Self-generated, External Resources	Yes	
NTUA	Public repositories, Collaboration, Previously collected data from prior projects, Commercial datasets, Self-generated, External Resources	Yes	
RINA	Public repositories, Collaboration, Previously collected data from prior projects, Proprietary data, Self-generated, External Resources	Yes	
SEKAVIN	Previously collected data from prior projects, Proprietary data	Yes	Open access
UoS	Public repositories, Collaboration, Previously collected data from prior projects, Self-generated, External Resources	Yes	Open access, Restricted access, Internal Use only, Confidential
UPAT	Public repositories, Collaboration, Previously collected data from prior projects, Self-generated, External Resources	Yes	
VPF	Public repositories, Collaboration, Previously collected data from prior projects, Self-generated, External Resources	Yes	
WML	Public repositories, Collaboration, Previously collected data from prior projects, Commercial datasets, Proprietary data, Self-generated, External Resources	Yes	

Figure 3 illustrates the total values for the origin of data within the FLEETfor55 Project, as part of the answers of the Questionnaire.

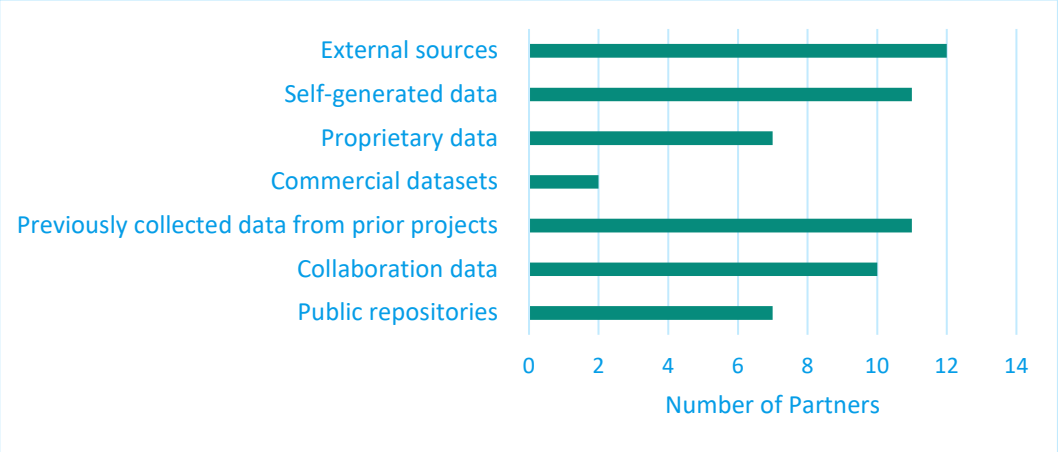

Figure 3: The number of data origin sources of the partners' data

2.3 FAIR Data Policy Alignment

An important aspect of the Data Management Plan (DMP) - also addressed in the questionnaires completed by the Consortium Partners - includes the application of FAIR data principles. The insights collected for the questionnaire are summarized in Table 5 and include information on whether a Persistent Identifier (PID) will be used and the type of PID selected. More information regarding PID is presented in Section 2.3.1. Additionally, the partners provided input on whether keywords will be included within the generated data to enhance findability, as well as the type of repository intended for data storage.

Table 5: Actions to ensure alignment with FAIR Data Policy

Partner	Usage of PIDs	Keywords to Enhance Findability	Selected Repository
ABS	N/A	N/A	Internal & External Repositories
AES	Follow the recommendations from DMP	NO	Internal & External Repositories, Repository to be selected later
CSM	Comply with DMP, use of DOI	YES	Internal & External Repositories
DST	Comply with DMP, use of DOI	YES	Repository to be selected later
EPS	Comply with DMP, use of DOI	YES	Repository to be selected later

Partner	Usage of PIDs	Keywords to Enhance Findability	Selected Repository
FCSI	Comply with DMP, use of DOI	YES	Institutional
HYD	Follow the recommendations from DMP	YES	External trusted repository, Repository to be selected later
NTUA	Comply with DMP, use of DOI	YES	Institutional
RINA	N/A	NO	Institutional
SEKAVIN	Comply with DMP, use of DOI	N/A	Institutional
UoS	Comply with DMP, use of DOI	YES	Institutional
UPAT	Comply with DMP, use of DOI	YES	Institutional
VPF	Comply with DMP, use of DOI	YES	Institutional
WML	Comply with DMP, use of DOI	YES	Repository to be selected later

In response to the question about additional secure storage repositories beyond those indicated in the DMP, partners mentioned that their institutional repositories would be the most commonly used alternatives.

Table 6 contains information regarding the intention of partners to use free standardized protocols for the management of their data (in addition to the actions required from the DMP), the planned actions to ensure data interoperability, and finally, whether any embargoes or restrictions will be posed regarding the re-usage of the data. The contents of Table 5 are in line with the Accessibility part of FAIR Principles and are explained in detailed in Section 2.3.2.

Table 6: FAIR data summary of partners' feedback.

Partner	Usage of protocol	Actions to make data Interoperable	Embargos / Restrictions on Re-use
ABS	N/A	Descriptive metadata	NO
AES	DEPENDS	Descriptive metadata, Technical metadata	NOT EXPECTED
CSM	YES	Descriptive metadata, Structural metadata, Technical metadata	YES
DST	N/A	N/A	N/A
EPS	N/A	Descriptive metadata, Structural metadata, Technical metadata	NO
FCSI	YES	Descriptive metadata, Structural metadata, Technical metadata	YES
HYD	NO	Descriptive metadata, Technical metadata	YES
NTUA	YES	Descriptive metadata, Structural metadata, Technical metadata	YES
RINA	YES	N/A	N/A
SEKAVIN	YES	Descriptive metadata, Structural metadata, Technical metadata	NO
UoS	YES	Descriptive metadata, Structural metadata, Technical metadata	YES
UPAT	YES	Descriptive metadata, Structural metadata, Technical metadata	YES
VPF	N/A	N/A	N/A
WML	NO	Descriptive metadata, Structural metadata, Technical metadata	N/A

2.3.1 Findability

The main goal of the Findability principle is to assign a "global" unique and Persistent Identifier (PID). Almost every Partner - as Figure 4 indicates - proposed DOI as the PID that the Consortium will align to.

A decision must be made on whether the data and the corresponding metadata should be assigned with the same DOI, or separate DOIs [19]. Assigning the same DOI saves time and resources. On the other hand, assigning them with different DOIs aligns datasets with FAIR principles, because even on restricted datasets there is the capability of an open access metadata preview. This allows partners to be aware of what every data set contains and then apply a request if needed.

Also, the metadata that will be implemented (author, type, format etc.) should be selected. The metadata should follow a certain standardization – protocol. Dublin core [20] is the easiest and covers a wide range of elements.

One of the most used repositories which follows EU principles - as it is CERN's trusted repository – and assign automatic the metadata is Zenodo [21].

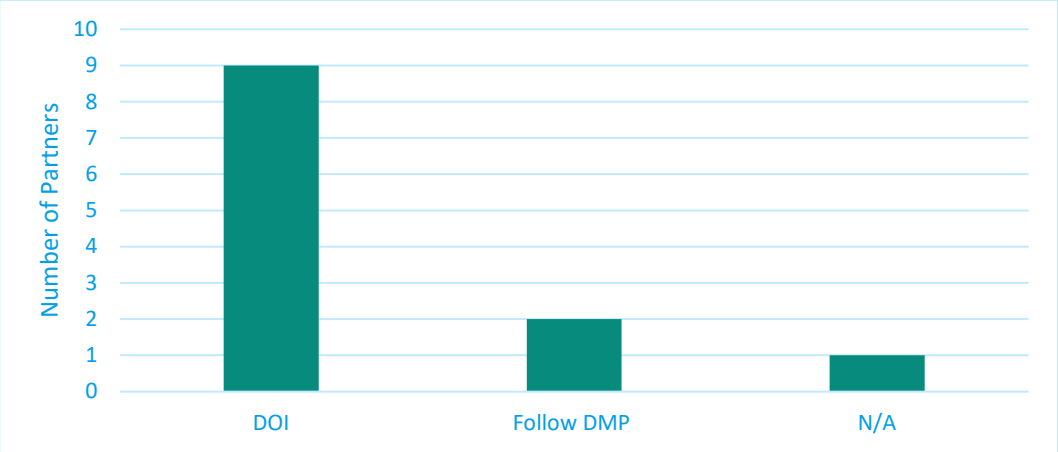

Figure 4: Selection of Persistent Identifier for data and metadata

2.3.2 Accessibility

The main goal of accessibility is to ensure that data can be retrieved using an open & standardized protocol – such as HTTP. The most commonly used platforms that can support these types of protocols are:

- Zenodo,
- GitHub,

- OpenAIRE,
- EOSC portal repositories with access control, and
- Institutional repositories under the management and responsibility of every partner.

In the case of restricted/confidential data, the Institutional repository for each corresponding partner appears to be the safest option. Access to such datasets can be granted upon request, with every partner being responsible for authorizing access. Importantly, metadata should always be openly available, even if the dataset that it describes is restricted. This ensures transparency, communication and alignment with the FAIR data principles.

The main repositories throughout the project have already been selected to be the Microsoft Teams [22] in conjunction with each partner's institutional repository. For long-term preservation and open access datasets that can be shared with the community another repository must be unanimously selected later in the project and will be part of the updated version of the Data Management Plan (DMP).

The dissemination level of the data generated, as illustrated in Table 4, is part of the accessibility aspect of FAIR Principles. Figure 5 presents the dissemination level of partners, indicating that no Partner has decided that Embargoed datasets will be generated. All Partners who gave information through the questionnaires indicated that Open Access datasets will be generated. Furthermore, any restricted access datasets must follow a clear 2-way authorization – authentication that follows the AAI (Authentication and Authorization Infrastructure) [23]. Finally, it is important to define the dissemination level of each dataset clearly on its corresponding metadata.

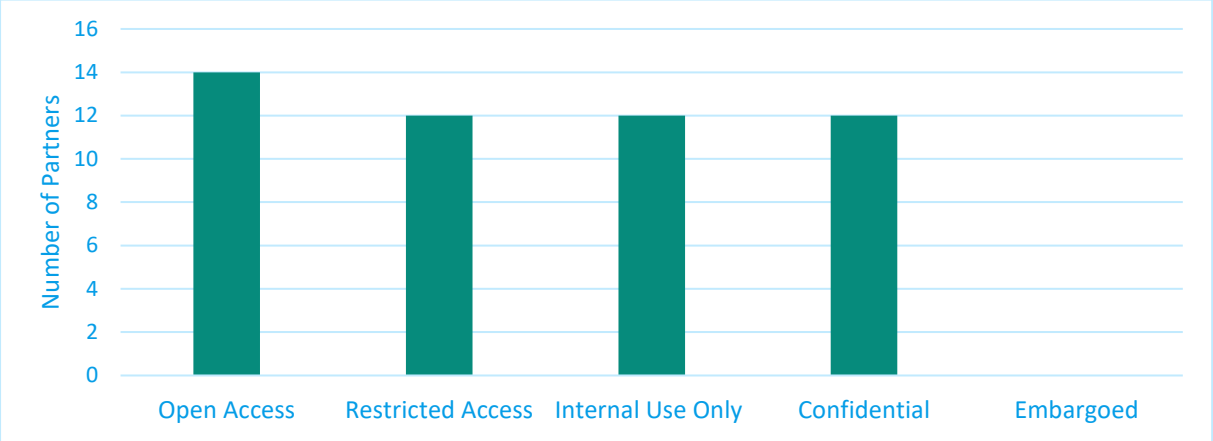

Figure 5: Dissemination Level of the generated datasets

2.3.3 Interoperability

Datasets should be as compatible as possible with other datasets and tools. All the partners should share languages, formats, standards, templates etc. To ensure long term interoperability and accessibility, open file formats should be used, in line with FAIR principles, such as CSV [18], JSON [24], NetCDF [25], RDF [26], XML [27]. Every dataset should be accompanied by a detailed README text file whenever possible. A template has been already developed based on the Dublin Core elements [20]; this template will be enhanced in the updated version of the DMP. Based on the information provided in Table 6, Figure 6 illustrates the types of metadata that the Partners will use to ensure data interoperability.

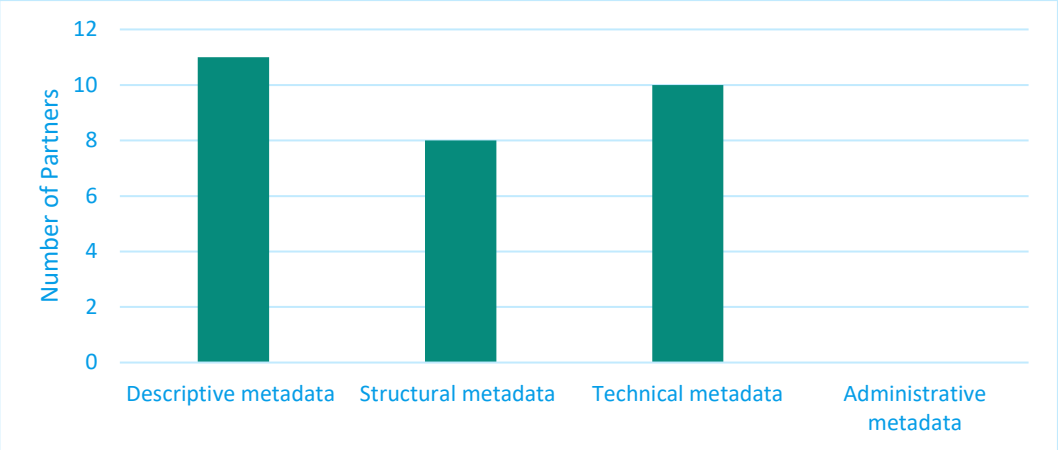

Figure 6: Ways to increase data Interoperability, data exchange and reuse by providing metadata

2.3.4 Re-usability

Data should be well described and licensed, so that it can be reused in the future by others (e.g. researchers, stakeholders, companies etc.). To enhance reusability of the generated

datasets -provided the author gives consent- the data should be documented thoroughly in a "metadata description file" (e.g. "README file"). This file may include details such as: author and contributors, data collection method and research methodology, abstract – dataset description, instruments/software used, versions and date, contextual notes from the data providers, other information that facilitates understanding and reuse.

Every open access dataset is recommended to be accompanied by a CC0 license [28], to ensure that the datasets set clear rules and copyrights of the dataset. Under current copyright laws, when no license exists, it considers as "all rights reserved" [29].

All partners indicated that data will be Re-used after the completion of the project (Table 4). This is aligned with the Grant Agreement (GA) and more specifically with the Communication and Dissemination Strategy, which fosters the exploitation of the generated knowledge and the peer-based distribution of results. The questionnaire provided by the DMP Team also accounts for what is the anticipated purpose of re-use as presented in Figure 7.

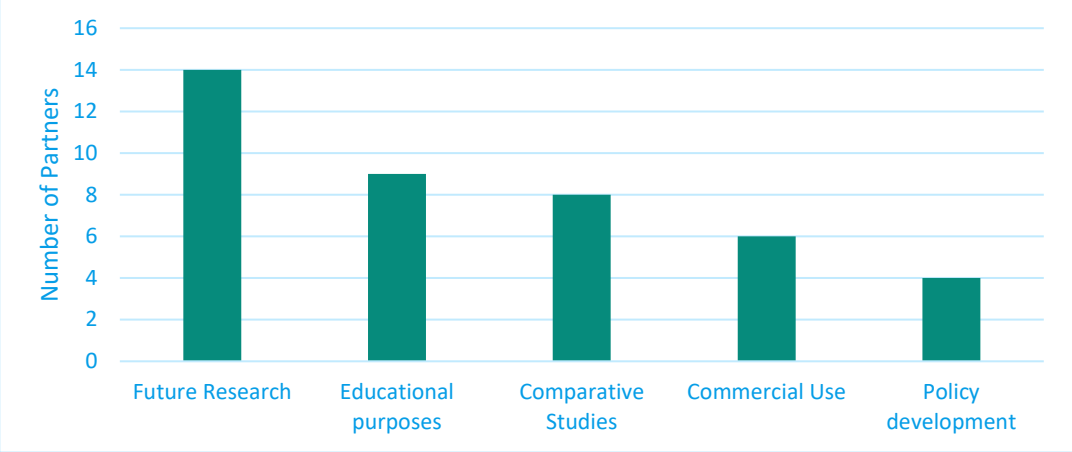

Figure 7: Expected purposes for data re-use

2.4 Other Research Outputs

This chapter is dedicated to the management of other research outputs that will be generated through the FLEETfor55 project such as digital or physical outputs. The provided questionnaire aimed to identify which partner is going to generate other research output for the available pool of categories:

- Software and Tools,
- Protocols and Methodologies,
- Models and Simulations,

- Training Materials

In the questionnaire the plan for storage of the other research outputs is accounted for and the results for this can be summarized in Table 7.

Table 7: Other Research Outputs – Summary of Partner selections

Partner	Management of other research outputs
ABS	N/A
AES	Software and Tools: Stored in GitHub, Models and Simulations: Stored in repositories, Storage: Cloud platforms
CSM	Software and Tools: Stored in GitHub
DST	N/A
EPS	Software and Tools: Stored in GitHub Storage: Cloud platforms
FCSI	Software and Tools: Stored in GitHub, Models and Simulations: Stored in repositories
HYD	Models and Simulations: Stored in repositories, Storage: Cloud platforms
NTUA	Models and Simulations: Stored in repositories, Training Materials: Available through YouTube, GitHub, or institutional websites, Storage: Cloud platforms
RINA	N/A
SEKAVIN	Storage: Cloud platforms
UoS	Models and Simulations: Stored in repositories, Training Materials: Available through YouTube, GitHub, or institutional websites, Storage: Cloud platforms
UPAT	Software and Tools: Stored in GitHub, Models and Simulations: Stored in repositories, Storage: Cloud platforms
VPF	Storage: Cloud platforms

Partner	Management of other research outputs
WML	Models and Simulations: Stored in repositories, Storage: Cloud platforms

As for the other research outputs that might occur during the project the majority of partners expect this other research outputs to be models and simulations which will be stored in cloud platforms with regular backups.

2.5 Data Security

Data security within FLEETfor55 Project is handled with a clear and robust approach. Unshared data are stored locally within each partner's institutional drives or secure cloud platforms like GitLab and GitHub. Third party platforms are utilized to facilitate data storage, version control and accessibility across the Consortium. To mitigate possible risks associated with the use of these platforms, all partners are expected to perform regular backups, in accordance with the DMP Backup Protocol, and to ensure strict adherence to the dissemination level of the datasets they access and utilize. Shared data, on the other hand, are stored centrally in Microsoft Teams, which is integrated with SharePoint. This integration ensures that all shared data are automatically synced and have a level of security that is ensured by Microsoft. Each partner is responsible for ensuring compliance with the General Data Protection Regulation (GDPR) and has to clearly define the dissemination level of every dataset generated within the project.

Microsoft Teams provides a high level of security since it has a two-factor authentication and encryption of data both in transit and at rest. Files stored on SharePoint have the SharePoint encryption.

Access to the Microsoft Teams is managed by Hydrus and is restricted to authorized project partners only. Only invited users with personal accounts and credentials are granted access, resulting in the data sharing remaining both secure and controlled. Table 8 provides an overview of the data security measure expected from each partner, with the primary selected options being the regular data backups and the usage of secure servers with restricted access.

Table 8: Data Security – Summary of Partner selections

Partner	Measures to ensure Data Security
ABS	Secure servers with restricted access, Encrypted data transfer, Regular data backups, Access control policies,

Partner	Measures to ensure Data Security
	Compliance with regulations
AES	Secure servers with restricted access, Encrypted data transfer, Regular data backups
CSM	Secure servers with restricted access, Encrypted data transfer, Regular data backups, Access control policies, Compliance with regulations
DST	Secure servers with restricted access, Encrypted data transfer, Regular data backups, Access control policies
EPS	Secure servers with restricted access, Encrypted data transfer, Regular data backups, Compliance with regulations, Institutional cloud services with certified security standards
FCSI	Secure servers with restricted access, Encrypted data transfer, Regular data backups, Access Control Policies, Compliance with regulations, Institutional cloud services with certified security standards
HYD	Secure servers with restricted access, Encrypted data transfer, Regular data backups, Compliance with regulations, Institutional cloud services with certified security standards
NTUA	Secure servers with restricted access, Encrypted data transfer, Regular data backups, Access Control Policies, Compliance with regulations, Institutional cloud services with certified security standards, Data anonymization / pseudonymization
RINA	Secure servers with restricted access, Encrypted data transfer, Regular data backups, Access Control Policies, Compliance with regulations, Institutional cloud services with certified security standards, Data anonymization / pseudonymization
SEKAVIN	Secure servers with restricted access, Encrypted data transfer, Regular data backups, Access Control Policies, Compliance with regulations, Institutional cloud services with certified security standards,

Partner	Measures to ensure Data Security
	Data anonymization / pseudonymization
UoS	Secure servers with restricted access, Encrypted data transfer, Regular data backups, Access Control Policies, Compliance with regulations, Institutional cloud services with certified security standards
UPAT	Secure servers with restricted access, Encrypted data transfer, Regular data backups, Access Control Policies, Compliance with regulations, Institutional cloud services with certified security standards
VPF	Secure servers with restricted access, Regular data backups, Access Control Policies, Compliance with regulations
WML	Secure servers with restricted access, Regular data backups, Compliance with regulations, Institutional cloud services with certified security standards

Table 8 is illustrated in Figure 8, which shows that partners unanimously agreed that datasets will be stored in secure repositories and that regular backups will be performed.

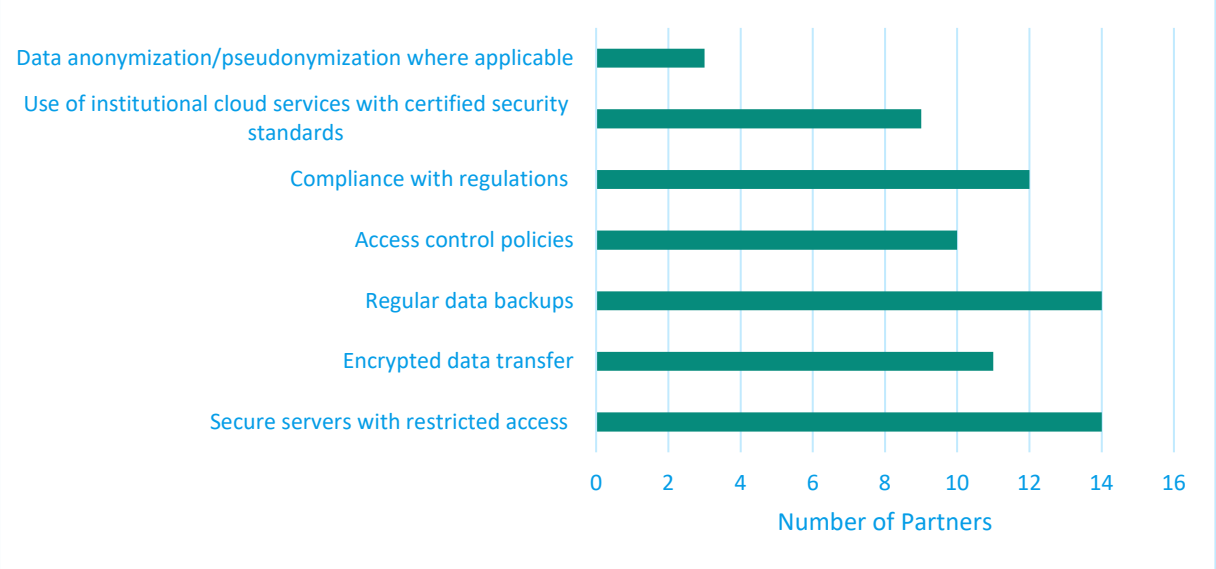

Figure 8: Measures that are applied on each organization to ensure data security

2.6 Ethical Aspects

Within the framework of ethical consideration, the FLEETfor55 Consortium strictly adheres to ethical practices set by the EU, both during the project's implementation as well as after its completion. Particular attention should be given to preventing misuse of personal data. Under no circumstances will the FLEETfor55 project process or distribute personal data, including during dissemination activities, where the data will be stored and presented in anonymous form.

As the Grant Agreement (GA) defines, on chapter 4.1, the project will be strictly limited to mechanical engineering concepts and does not include aspects involving clinical trials or processing of personal data. The design activities have no potentially harmful impacts on local communities and the environment. Also, per the chapter 4.2, the Consortium will follow a specific ethically focused approach during the development, deployment, use of AI-based solutions. The project partners have to comply with requirements in the following categories: Human agency and oversight, Privacy and data governance, Transparency, Fairness, diversity and non-discrimination, Societal and environmental well-being and Accountability.

Table 9 provides information on potential ethical and legal considerations related to data management. Given the involvement of multiple datasets from various sources, the responses provided by the partners account for a range of ethical protections measures and consent requirements.

Table 9: Protection measures and consent requirements in terms of data management.

Partner	Ethics – Legal Issues
ABS	Data includes third party or proprietary content
AES	GDPR [30] – data protection laws, Data use agreements – licenses restrict sharing, Data includes third party or proprietary content
CSM	Requires informed consent
DST	Requires informed consent, Subject to ethics
EPS	Requires informed consent, GDPR – data protection laws

Partner	Ethics – Legal Issues
FCSI	Requires informed consent
HYD	Requires informed consent, GDPR – data protection laws, Data use agreements – licenses restrict sharing
NTUA	Requires informed consent, GDPR – data protection laws, Data includes third party or proprietary content
RINA	Requires informed consent, GDPR – data protection laws, Data includes third party or proprietary content, Data use agreements – licenses restrict sharing
SEKAVIN	Openly accessible data – no legal/ethical restrictions
UoS	Requires informed consent, Data includes third party or proprietary content
UPAT	Requires informed consent
VPF	Requires informed consent, GDPR – data protection laws
WML	Requires informed consent, GDPR – data protection laws, Data use agreements – licenses restrict sharing, Anonymous – non sensitive data

Based on the partners' input in the questionnaire, the most commonly selected options was the acknowledgement of potential legal or ethical issues. To mitigate these issues, the majority of the partners indicated that getting informed consent for the reusage or sharing of the data, from the relevant partners' is crucial (Figure 9).

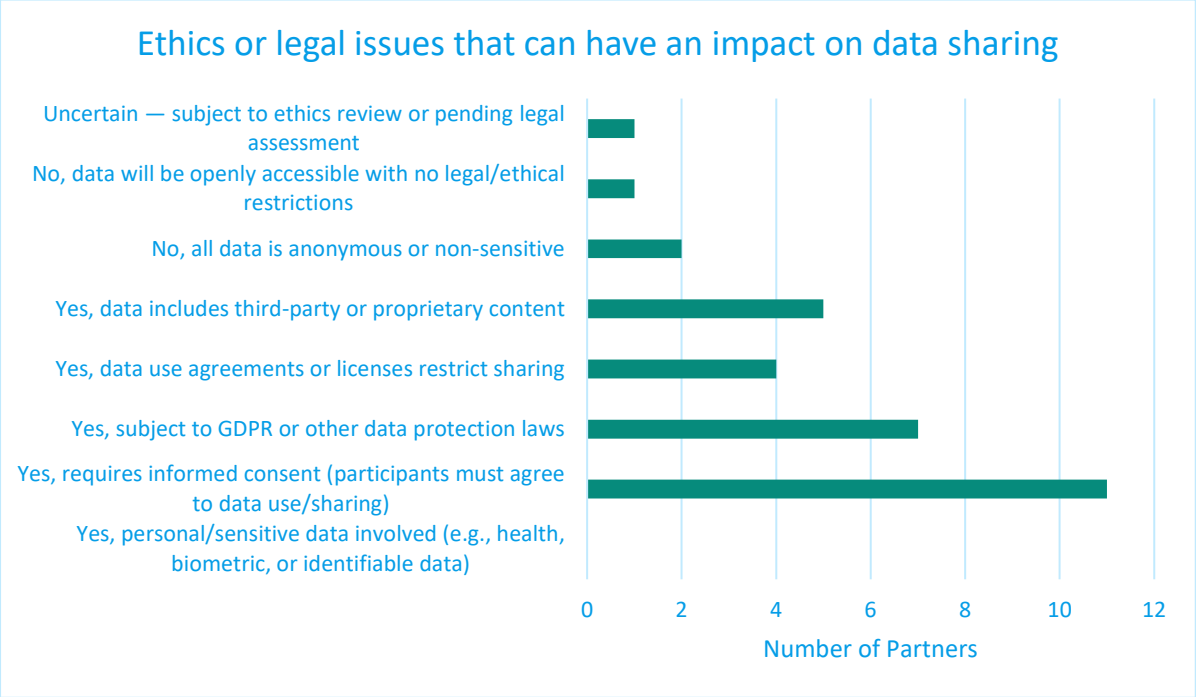

Figure 9: Ethical or legal issues that may emerge and impact data sharing

2.7 Other Aspects

In this chapter, any other national / funder / sectorial / departmental procedures and policies that may apply are analyzed per Partner and presented in Table 10. Any potential issues, conflicts and/or questions that may arise will be addressed during the regular meetings of the Consortium.

Table 10: Other Aspects – Summary of Partner selections

Partner	Other procedures used for data management
ABS	Institutional / departmental data policies
AES	Consortium defined data procedures will be used, To be determined
CSM	Funder requirements
DST	N/A

Partner	Other procedures used for data management
EPS	Funder requirements, Institutional / departmental data policies
FCSI	Funder requirements, Institutional / departmental data policies
HYD	Funder requirements, Discipline-specific protocols
NTUA	Consortium defined data procedures will be used
RINA	National data management regulations, Funder requirements, Institutional / departmental data policies
SEKAVIN	Consortium defined data procedures will be used
UoS	Funder requirements, Institutional / departmental data policies
UPAT	Funder requirements, Institutional / departmental data policies
VPF	Funder requirements, Institutional / departmental data policies
WML	Funder requirements, To be determined

In response to the question of whether additional national, sectoral, or departmental procedures might be used, the majority of partners mentioned that funder requirements will primarily indicate the rules and guidelines for Data Management processes (see Figure 10).

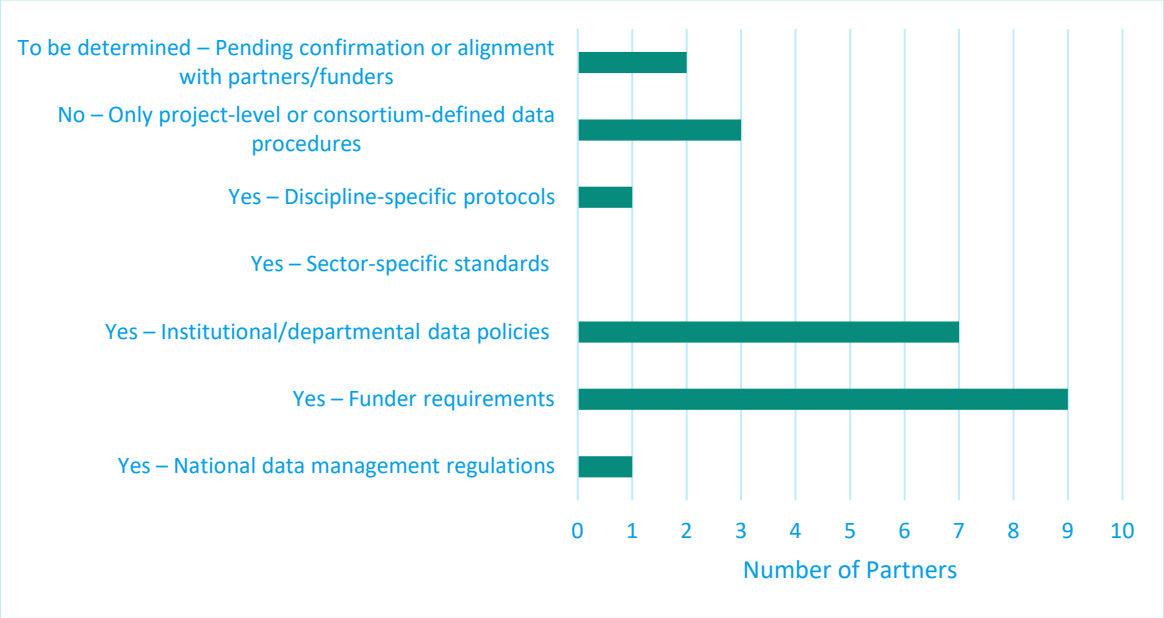

Figure 10: Other national / funder / sectorial / departmental procedures be used for data management

3 Data Storage and Sharing

3.1 Infrastructure

The main repository throughout the project, Microsoft Teams, have been already selected. It is accessible to all Partners that have authorized profiles and have been added from the Project Coordinator (CO), Hydrus. Moreover, files are automatically and in sync updated throughout the repository. Only invited users with personal accounts and credentials are granted access, resulting in the data sharing remaining both secure and controlled. For long-term preservation and open access datasets to the community another repository must be unanimously selected later in the project. In the FLEETfor55 General Assembly, which took place in Trondheim 24-25 of June 2025, it was agreed that all public documents generated during the project will be uploaded and released for public access through the project's official website, www.fleetfor55.eu. Figure 11 presents the structure of the FLEETfor55 Microsoft Teams folders that account for administrative, communication and technical aspects of the project.

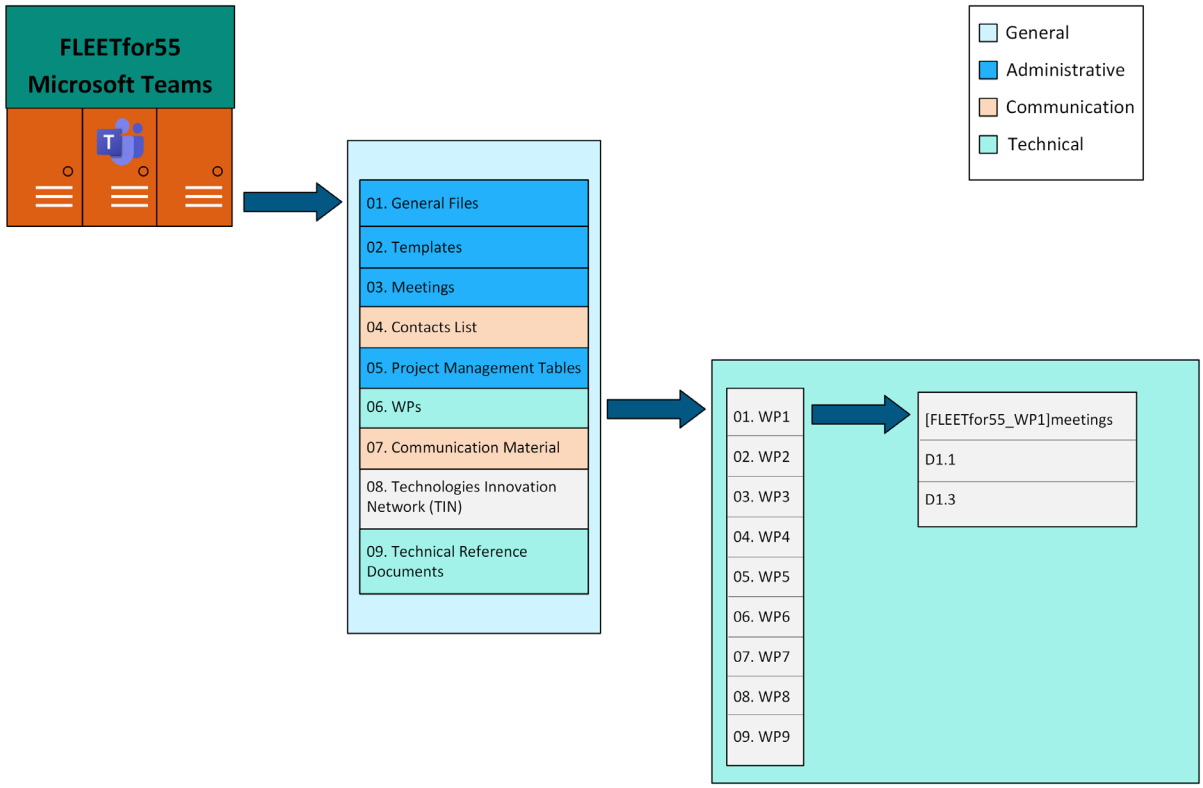

Figure 11: Structure of FLEETfor55 Teams folders

3.2 Backup-Protocol

As an additional safety measure, data is backed up monthly, with each individual partner being responsible for performing this action. In the event of failure, this strategy allows the data to be restored.

Conclusions

The goal of the Initial Management plan was to record the Partners' needs and their expectations of the data that will be generated (e.g. format, type, etc.). Also, to set down the requirements of the project, as far as the data storage and management are concerned. In this line, a Questionnaire was made and sent to all project Partners. Inputs from partners were collected and analysed, as mentioned in this report.

DMP is a living document that evolves in parallel with the project [31]. In Month 18 (June 2026) a second version will be developed, the third version will be delivered in Month 36 and in Month 42 the final version of DMP will be published.

The objective for the upcoming deliverable is to gather input from all partners, through the distribution of an updated version of the questionnaire. Additionally, identifying any potential gaps that there are in this report and including all possible perspectives, will increase the robustness of the DMP.

Contact Personnel

Contact person: **Prof. Angelos Filippatos**, Associate Professor at University of Patras

Email: angelos.filippatos@upatras.gr

Responsibilities

- Initial Data Management Plan and continuous update of DMP

Contact person: **Mr. Astrinos Papadakis**, Innovation Hub Manager – FLEETfor55 Project Coordinator, HYDRUS Engineering Ltd.

Email: a.papadakis@hydrus-eng.com

Responsibilities

- Hydrus is responsible for FLEETfor55 project administrative and technical coordination

4 ANNEX

4.1 Questionnaire

As part of the Initial DMP a questionnaire was sent to all partners in order to collect useful data. The questionnaire is constructed on Microsoft's Excel and is illustrated on Figures {12 - 21}.

Report of the consortium regarding the plans related to data management to be in line with the mandatory Open Science (OS) practices set by the EC.
Please complete as many fields of the questionnaire as possible.
Provide your answers in each of the Thematic Areas (I-VI).
Elaborate on your answers, whenever needed, in the comment area.
Beneficiary Name:

Questionnare Topics	
Thematic Area I	A summary of the data generated within the Fleetfor55 project, from the types to the origin of the data.
Thematic Area II	Presentation of the correlation of the data to the FAIR
Thematic Area III	Presentation of the planned research outputs for the data generated within the project.
Thematic Area IV	Presentation of the planned data security strategy.
Thematic Area V	Issues related to ethics with regards to data
Thematic Area VI	Other issues related to data management.

Sources
https://open-research-europe.ec.europa.eu/articles/1-42
https://www.go-fair.org/fair-principles/
https://www.ugent.be/en/research/openscience/datamanagement/before-research/datamanagementplan.htm

Figure 12: Questionnaire - First sheet – Instructions

I. Data summary		Answers related to the project data		Specify based on selection
1. Types of data generated within the project?	☐	Quantitative data	☐	Numerical measurements
			☐	Test results
			☐	Statistics
	☐	Qualitative data	☐	Interview transcripts
			☐	Survey responses
			☐	Case studies
	☐	Multimedia data	☐	Images
			☐	Audio recordings
			☐	Videos
	☐	Geospatial data	☐	Maps
			☐	GPS data
			☐	Satellite imagery
	☐	Textual data	☐	Reports
			☐	Documents
			☐	Publications
	☐	Sensor data	☐	Data from IoT devices
			☐	Environmental sensors
	☐	Simulated data	☐	Data from models
			☐	Simulations
			☐	Synthetic data
2. Formats of data generated within the project?	☐	CSV (Comma-Separated Values)		
	☐	Excel (XLSX, XLS)		
	☐	JSON (JavaScript Object Notation)		
	☐	XML (Extensible Markup Language)		
	☐	TXT (Plain Text)		
	☐	SPSS (.sav)		
	☐	MATLAB (.mat)		
	☐	JPEG (Image)		
	☐	PNG (Image)		
	☐	MP4 (Video)		
	☐	WAV (Audio)		
	☐	PDF (Portable Document Format)		

Figure 13: Questionnaire - Second sheet – Data Summary [questions 1, 2]

3. Data dissemination level?	☐	Open Access – Data will be publicly available without restrictions.		
	☐	Restricted Access – Data available upon request or under specific conditions (e.g., with data sharing		
	☐	Internal Use Only – Data will only be accessible to project partners or within the organization.		
	☐	Confidential – Data will not be shared due to sensitivity, legal, or contractual reasons.		
	☐	Embargoed – Data will be made available after a defined period (e.g., post-publication or project end).		
4. Will the generated data be re-used? What is a reason that might make you consider using the data.	☐	Yes	☐	Future Research
			☐	Educational purposes
			☐	Comparative Studies
			☐	Commercial Use
			☐	Policy development
	☐	No		
5. Which WP and Tasks will generate data?		Example: WP5.T5.2		
6. What is the expected size of the data that you intend to generate?		Select from the available options		

Figure 14: Questionnaire - Second sheet – Data Summary [questions 3, 4, 5, 6]

7. What is the origin of the previous data utilized?	☐	Public repositories (e.g., government databases, open-access research datasets)		
	☐	Collaboration data (e.g., data shared by research partners, collaborators)		
	☐	Previously collected data from prior projects (e.g., historical data collected before the current project)		
	☐	Commercial datasets (e.g., data purchased from commercial providers)		
	☐	Proprietary data (e.g., internal company or organization datasets)		
	☐	Self-generated data (e.g., data collected by your team or organization within the scope of this project)		
	☐	External sources (e.g., third-party providers, publicly available data from internet sources)		
8. Are data planned to be re-used after the completion of the project?	☐	Yes – Data will be preserved for reuse by others (e.g., researchers, public, industry)		
	☐	Yes – Data will support future research, replication, or follow-up studies		
	☐	Yes – Data will be made available in a repository for long-term access		
	☐	No – Data will not be reused (e.g., too sensitive, limited value, or restricted by consent)		
	☐	Undecided – Reuse depends on future legal/ethical assessment or project results		

Figure 15: Questionnaire - Second sheet – Data Summary [questions 7, 8]

IIa. Findable		Describe the methods to make data Findable
1. Data and metadata are going to be identified by a persistent identifier (PID). Which identifier do you plan to use?		*Example: DOI (Digital Object Identifier)*
2. What type of machine-readable metadata will accompany the generated datasets?		*Example: - Documentation will include a standardized folder structure, codebooks (metadata about the data), logbooks (metadata about data processing), analysis plans, input and output files from databases and statistical software* *- The following metadata will be provided (as Excel file) for each experiment: Experiment number, Condition, Date, Entity, Description, Format*
3. Will search keywords be provided in the metadata to enhance discovery and re-usage?		Select from the available options

IIb. Accessible		Describe the methods to make data Accessible
1. Will the data be safely stored in trusted repositories for long term preservation at your organization or extra repository is required?	☐	Yes, institutional repository available (e.g., university/archive system)
	☐	Yes, using a certified external repository (e.g., Zenodo, Figshare, Dryad)
	☐	No internal repository – external trusted repository will be used
	☐	Combination of internal and external repositories
	☐	Repository to be selected later based on data type and access needs
	☐	Metadata will be registered in a public catalog even if full data access is restricted
2. Does the repository ensure that the data is assigned an identifier?		Select from the available options
3. Will a free and standardized protocol be used to access the data?		Select from the available options
4. How will the sensitive data be provided, both during and after the end of the project?		
5. Will the collected/generated data require special software or hardware to be accessed or "read"? Please specify in the area.		*Example:* *Hardware: Sensors (e.g., temperature sensors, GPS devices, motion detectors), Wearables (e.g., smartwatches, fitness trackers, biosensors),Cameras (e.g., digital cameras, drones, video surveillance equipment),Microphones (e.g., recording devices for audio data collection),Computers (e.g., laptops, desktops, servers for data processing),IoT devices (e.g., smart devices, smart meters, connected environmental sensors), Laboratory equipment (e.g., microscopes, spectrometers, test instruments), Field equipment (e.g., survey instruments, soil probes, data loggers),Mobile devices (e.g., smartphones, tablets for data collection in the field)*
6. How long after the completion of the project will the data remain available and findable?		

Figure 16: Questionnaire - Third sheet – FAIR Data [Findability, Accessibility]

IIc. Interoperable		Describe the methods to make data Interoperable
1. What actions will you follow to make your data interoperable to allow data exchange and re-use across disciplines?	☐	Descriptive metadata e.g author, title, abstract, date, location, time, data collection method (tools)
	☐	Structural metadata e.g links to related digital objects,such as the article written based on the linked research data
	☐	Technical metadata e.g data format, hardware/software used, calibration, version, authentication, encryption, metadata standard
	☐	Administrative metadata e.g license, possible reasons for an embargo, waivers, Search logs, user tracking
2. Will you provide mapping to commonly used ontologies for the specific ontologies generated within the project?		Select from the available options
3. Will your data include references to other data or metadata ?		*Example: Other data from your project, Datasets from previous research*

IId. Reusable		Describe the methods to make data Reusable
1. Will you provide documentation to validate data analysis and facilitate data re-use?		*Examples: readme files with information on methodology, codebooks, data cleaning, analyses, variable definitions, units of measurement, etc.*
2. Will you pose embargos or specific restrictions regarding the re-use of data?		
3. Describe all relevant data quality assurance processes your organization will follow in this		

Figure 17: Questionnaire - Third sheet – FAIR Data [Interoperability, Reusability]

III. Other Research Outputs		Describe the other research outputs that the project will generate
1. Plan for the management of other research outputs that may be generated throughout the project such as digital outputs (e.g. software, protocols, models, etc.).	☐	Software and Tools: Stored in GitHub, with version control and clear documentation (e.g., user manuals, license).
	☐	Protocols and Methodologies: Stored in Open Science Framework (OSF) with versioning and detailed documentation.
	☐	Models and Simulations: Stored in repositories (e.g., GitHub, Zenodo) with metadata and versioning.
	☐	Training Materials: Available through YouTube, GitHub, or institutional websites.
	☐	Storage: Cloud platforms (e.g., Google Drive, OneDrive) with regular backups.
2. In what way (in line with the FAIR principles) will these research outputs be managed and shared? If any of these not applicable, specify the reasons.	☐	Findable: Outputs will be stored in public repositories with DOIs and metadata for easy discovery.
	☐	Accessible: Open access with clear licensing (e.g., Creative Commons, MIT License).
	☐	Interoperable: Standard file formats (e.g., CSV, Python) with APIs or documentation for integration.
	☐	Reusable: Clear documentation and open licenses for adaptation and redistribution.

Figure 18: Questionnaire - Fourth sheet – Other Research outputs

IV. Data security		Answers related to data security
1. What measures are in place at your organization to ensure data security (including data recovery as well as secure storage/archiving and transfer of sensitive data)?	☐	Secure servers with restricted access (e.g., password-protected, firewalled)
	☐	Encrypted data transfer (e.g., via VPN, SFTP, HTTPS)
	☐	Regular data backups (daily, weekly) with off-site or cloud redundancy
	☐	Access control policies (user roles, audit trails, authentication protocols)
	☐	Compliance with regulations (e.g., GDPR, institutional IT security policies)
	☐	Use of institutional cloud services with certified security standards (e.g., ISO 27001)
	☐	Data anonymization/pseudonymization where applicable

Figure 19: Questionnaire - Fifth Sheet – Data Security

V. Ethics		Answers related to data ethics
1. Are there, or could there be, any ethics or legal issues that can have an impact on data sharing?	☐	Yes, personal/sensitive data involved (e.g., health, biometric, or identifiable data)
	☐	Yes, requires informed consent (participants must agree to data use/sharing)
	☐	Yes, subject to GDPR or other data protection laws
	☐	Yes, data use agreements or licenses restrict sharing
	☐	Yes, data includes third-party or proprietary content
	☐	No, all data is anonymous or non-sensitive
	☐	No, data will be openly accessible with no legal/ethical restrictions
	☐	Uncertain — subject to ethics review or pending legal assessment

Figure 20: Questionnaire - Sixth Sheet - Ethics

VI. Other issues		Answers related to the usage of different data management procedures
1. Will other national/funder/sectorial/departmental procedures be used for data management? If yes, which ones?	☐	Yes – National data management regulations apply (e.g., national open data policy, research data mandates)
	☐	Yes – Funder requirements (e.g., Horizon Europe DMP guidelines, NIH data sharing policy)
	☐	Yes – Institutional/departmental data policies (e.g., university data governance frameworks)
	☐	Yes – Sector-specific standards (e.g., clinical trial data standards, ISO data security standards)
	☐	Yes – Discipline-specific protocols (e.g., FAIR principles, OpenAIRE, discipline-specific repositories)
	☐	No – Only project-level or consortium-defined data procedures will be used
	☐	To be determined – Pending confirmation or alignment with partners/funders

Figure 21: Questionnaire - Seventh Sheet – Other Issues

5 References

[1] European Research Executive Agency, "Open Science - European Commission." Accessed: May 14, 2025. [Online]. Available: https://research-and-innovation.ec.europa.eu/strategy/strategy-research-and-innovation/our-digital-future/open-science_en

[2] European Commission, "FAIR Data - A Quick Guide for Researchers."

[3] European Research Executive Agency, "Open science in Horizon Europe." Accessed: May 14, 2025. [Online]. Available: https://rea.ec.europa.eu/open-science_en

[4] UNESCO, "UNESCO Recommendation on Open Science | UNESCO." Accessed: May 14, 2025. [Online]. Available: https://www.unesco.org/en/open-science/about

[5] P. Hanel, "Intellectual property rights business management practices: A survey of the literature," *Technovation*, vol. 26, no. 8, pp. 895–931, Aug. 2006, doi: 10.1016/J.TECHNOVATION.2005.12.001.

[6] M. D. Wilkinson *et al.*, "Comment: The FAIR Guiding Principles for scientific data management and stewardship," *Sci Data*, vol. 3, no. 1, pp. 1–9, Mar. 2016, doi: 10.1038/SDATA.2016.18;SUBJMETA=479,648,697,702,706;KWRD=PUBLICATION+CHARACTERISTICS,RESEARCH+DATA.

[7] N. Paskin, "Digital Object Identifier (DOI ®) System", doi: 10.1081/E-ELIS3-120044418.

[8] P. Golodoniuc, N. N. J. Car, and J. Klump, "Distributed Persistent Identifiers System Design," *Data Sci J*, vol. 16, pp. 34–34, Jun. 2017, doi: 10.5334/DSJ-2017-034.

[9] "FAIR Principles," https://www.go-fair.org/fair-principles/.

[10] "The evolution of the interoperability concept a european quest for simplicity and universality," https://www.slideshare.net/slideshow/the-evolution-of-the-interoperability-concept-a-european-quest-for-simplicity-and-universality1/249787436.

[11] "What is interoperability?," https://www.ibm.com/think/topics/interoperability.

[12] "FAIR Semantics, Interoperability, and Services," https://www.fairsfair.eu/fair-semantics-interoperability-and-services-0.

[13] "ISA 2 New European Interoperability Framework Promoting seamless services and data flows for European public administrations", doi: 10.2799/360327.

[14] P. O. of the E. Union, "EOSC interoperability framework : report from the EOSC Executive Board Working Groups FAIR and Architecture.," Feb. 2021, doi: 10.2777/620649.

[15] P. O. of the E. Union, "Recommendations on FAIR metrics for EOSC.," Jan. 2021, doi: 10.2777/70791.

[16] R. Huber, A. Devaraju, R. Huber, and A. Devaraju, "F-UJI : An Automated Tool for the Assessment and Improvement of the FAIRness of Research Data," *EGUGA*, pp. EGU21-15922, Mar. 2021, doi: 10.5194/EGUSPHERE-EGU21-15922.

[17] A. Jacobsen *et al.*, "A generic workflow for the data fairification process," *Data Intell*, vol. 2, no. 1–2, pp. 56–65, Jan. 2020, doi: 10.1162/dint_a_00028.

[18] J. Mitlohner, S. Neumaier, J. Umbrich, and A. Polleres, "Characteristics of open data CSV files," *Proceedings - 2016 2nd International Conference on Open and Big Data, OBD 2016*, pp. 72–79, Sep. 2016, doi: 10.1109/OBD.2016.18.

[19] A. Jacobsen *et al.*, "FAIR Principles: Interpretations and Implementation Considerations," *Data Intell*, vol. 2, no. 1–2, pp. 10–29, Jan. 2020, doi: 10.1162/DINT_R_00024.

[20] "Using Dublin Core™ - The Elements," https://www.dublincore.org/specifications/dublin-core/usageguide/elements/.

[21] V. P. Gurav and S. R. Nagarkar Librarian, "ZENODO: A PLATFORM FOR OPEN ACCESS AND SUSTAINABLE DIGITAL RESEARCH REPOSITORY".

[22] "Microsoft Teams," https://www.microsoft.com/en-us/microsoft-teams/group-chat-software.

[23] J. Lopez, R. Oppliger, and G. Pernul, "Authentication and authorization infrastructures (AAIs): a comparative survey," *Comput Secur*, vol. 23, no. 7, pp. 578–590, Oct. 2004, doi: 10.1016/J.COSE.2004.06.013.

[24] F. Pezoa, J. L. Reutter, F. Suarez, M. Ugarte, and D. Vrgoč, "Foundations of JSON schema," *25th International World Wide Web Conference, WWW 2016*, pp. 263–273, 2016, doi: 10.1145/2872427.2883029.

[25] R. Rew and G. Davis, "NetCDF: An Interface for Scientific Data Access," *IEEE Comput Graph Appl*, vol. 10, no. 4, pp. 76–82, 1990, doi: 10.1109/38.56302.

[26] B. Mcbride, "RDF Primer", Accessed: Jun. 02, 2025. [Online]. Available: http://www.w3.org/TR/2003/PR-rdf-primer-20031215/

[27] S. Decker *et al.*, "Semantic Web: The roles of XML and RDF," *IEEE Internet Comput*, vol. 4, no. 5, pp. 63–74, Sep. 2000, doi: 10.1109/4236.877487.

[28] "Open COnTenT-A prACTiCAl guiDe TO using CreATive COmmOns liCenCes WIKIMEDIA DEUTSCHLAND WIKIMEDIA DEUTSCHLAND", Accessed: Jun. 02, 2025. [Online]. Available: www.wikimedia.de

[29] I. Labastida and T. Margoni, "Licensing FAIR Data for Reuse under a Creative Commons Attribution 4.0 International (CC BY 4.0) license," *Data Intell*, vol. 2, pp. 199–207, 2020, doi: 10.1162/dint_a_00042.

[30] P. Voigt and A. von dem Bussche, "The EU General Data Protection Regulation (GDPR)," 2017, doi: 10.1007/978-3-319-57959-7.

[31] T. Miksa, S. Simms, D. Mietchen, and S. Jones, "Ten principles for machine-actionable data management plans," *PLoS Comput Biol*, vol. 15, no. 3, p. e1006750, Mar. 2019, doi: 10.1371/JOURNAL.PCBI.1006750.