D5.5 DATA MANAGEMENT PLAN

Revision: v.1.0

Work package	WP 5
Task	Task 5.4
Due date	30/06/2024
Submission date	28/06/2024
Deliverable lead	CEL
Version	1.0
Authors	Tetiana Vasylieva (CEL), Margot Bezzi (CEL)
Reviewers	Philippos Philippou (eBOS), Eva Hajdok (MAR)
Abstract	This document constitutes the Data Management Plan (DMP) of the 6G4Society project. Its major aim is to describe how all project data is going to be managed, from data collection to processing and storage, following efficient, ethical, secure and trusted practices of data management.

www.6g4society.eu

Co-funded by the European Union

Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

Keywords Data, FAIR, data management, personal data, GDPR

Document Revision History

Version	Date	Description of change	List of contributor(s)
V0.1	06/04/2024	Creation of the document with the ToC and sent for internal review and QA	Tetiana Vasylieva (CEL), Luigi Briguglio (CEL)
V0.2	24/05/2024	Updates ToC according to gathered comments from internal reviewer: Eva Hajdok (MAR), and Giota Lilli (eBOS) as QA and internal reviewer	Tetiana Vasylieva (CEL), Luigi Briguglio (CEL)
V0.3	31/05/2024	1st draft was sent to internal reviewers, QA and Risk leader, and Ethics Board members	Tetiana Vasylieva (CEL), Luigi Briguglio (CEL)
V0.4	10/06/2024	Integration of comments from internal reviewer Eva Hajdok (MAR), and Giota Lilli (eBOS) as QA and internal reviewer, and comments from members of the Ethics Board: Katrina Petersen (PSCE), Anna Aseeva (D4P), Argyro Michalopoulou (NOVA). Completion with further sections	Tetiana Vasylieva (CEL), Luigi Briguglio (CEL)
V0.5	12/06/2024	100% complete draft sent for QA and internal review	Tetiana Vasylieva (CEL), Luigi Briguglio (CEL)
V0.6	18/06/2024	Integration of comments from Eva Hajdok (MAR) as internal reviewer, and Giota Lilli (eBOS) as internal reviewer and QA and Risk leader. The document was sent to Peer Reviewers and QA and Risk leader	Tetiana Vasylieva (CEL), Luigi Briguglio (CEL)
V0.7	20/06/2024	Integration of comments from Peer Reviewers: Eva Hajdok (MAR) and Philippos Philippou (eBOS), and comments from Giota Lilli (eBOS) as QA and Risk leader. The document was sent to the Project Coordinator for feedback	Tetiana Vasylieva (CEL), Luigi Briguglio (CEL)
V1.0	28/06/2024	Document approved by the Project Coordinator and final release for EC	Tetiana Vasylieva (CEL), Margot Bezzi (CEL)

DISCLAIMER

Co-funded by the European Union

6GSNS

Project funded by

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

6G4SOCIETY project has received funding from the Smart Networks and Services Joint Undertaking (SNS JU) under the European Union's Horizon Europe research and innovation programme under Grant Agreement No 101139070. This work has received funding from the Swiss State Secretariat for Education, Research and Innovation (SERI).

Project co-funded by the European Commission in the Horizon Europe Programme		
Nature of the deliverable:	**DMP**	
Dissemination Level		
PU	*Public, fully open, e.g. web (Deliverables flagged as public will be automatically published in CORDIS project's page)*	✓
SEN	*Sensitive, limited under the conditions of the Grant Agreement*	
Classified R-UE/ EU-R	*EU RESTRICTED under the Commission Decision No2015/ 444*	
Classified C-UE/ EU-C	*EU CONFIDENTIAL under the Commission Decision No2015/ 444*	
Classified S-UE/ EU-S	*EU SECRET under the Commission Decision No2015/ 444*	

* R: Document, report (excluding the periodic and final reports)

DEM: Demonstrator, pilot, prototype, plan designs

DEC: Websites, patents filing, press & media actions, videos, etc.

DATA: Data sets, microdata, etc.

DMP: Data management plan

ETHICS: Deliverables related to ethics issues.

SECURITY: Deliverables related to security issues

OTHER: Software, technical diagram, algorithms, models, etc.

EXECUTIVE SUMMARY

This document constitutes the Data Management Plan (DMP) of the 6G4Society project. Its major aim is to describe how all project data is going to be managed, from data collection to processing and storage, following efficient, ethical, secure and trusted practices of data management.

This report delivers an initial analysis of the data that is anticipated to be managed by each of the project partners. It describes a questionnaire and input from consortium partners exploring the data that each partner expects to collect, store and make available internally (for further processing by project partners) and externally (disseminated) in full respect with the FAIR principles.

Throughout the project, the 6G4Society partners will adhere to the DMP in their work to properly manage data and protect the privacy and confidentiality of handled data. It will be periodically revised to reflect changes in the data that may be made available by the project and to provide additional information on the datasets.

Co-funded by the European Union

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Co-funded by the European Union

ABBREVIATIONS

BSCW	Basic Support for Cooperative Work
CA	Consortium Agreement
CEN	European Committee for Standardization
D	Deliverable
DCE	Dissemination and Exploitation
DMP	Data Management Plan
DoA	Description of Action
DPO	Data Protection Officer
EEA	European Economic Area
EC	European Commission
EN	European Standard
ENGAG	Engagement
EU	European Union
ETSI	European Telecommunications Standards Institute
FAIR	Findable, Accessible, Interoperable and Reused
GA	Grant Agreement
GDPR	General Data Protection Regulation
GR	Group Report
GS	Group Specification
ICT	Information and communications technology
IT	Information technology
ITU	International Telecommunication Union
KPI	Key Performance Indicator
KVI	Key Value Indicator
MNGT	Management
RSCH	Research

SNS JU	Smart Networks and Services Joint Undertaking
SR	Special Report
T	Task
TS	Technical Specification
TR	Technical Report
VPN	Virtual Private Network
WP	Work Package
5G	5th Generation
6G	6th Generation
6G-IA	6G Industrial Association

1 INTRODUCTION

This document delivers the DMP that has been identified in the Description of Action (DoA) as 6G4Society deliverable (D) 5.5 and a result of activities performed in Task (T) 5.4 “Data Management”.

The primary aim of the DMP is to define datasets the project will generate and/or collect, and how the research data will be managed from data collection to processing and storage following Fair Data management principles, as well as secure and trusted practices of data management.

Written in the early stages of the project, the DMP provides an initial analysis of the data anticipated to be managed by each project partner. It is based on inputs from consortium partners obtained through the initial Data Management Plan Questionnaire (hereafter the DMP questionnaire or the questionnaire), which was distributed to all partners at the beginning of the project. This questionnaire explores the data that each partner expects to collect, store and make available internally (for further processing by project partners) and externally with full respect to the FAIR principles.

The DMP is intended to be a living document. It will be periodically revised to reflect changes in the data that may be made available by the project. If updates are needed, these will be reported in the D5.2 - First Progress Report (M12) and D5.3 - Final Progress Report (M24).

1.1 RELATION TO PROJECT WORK

The general indications for the project deployment have been defined in the Smart Networks and Services Joint Undertaking (under the powers delegated by the European Commission) Grant Agreement (GA), the Description of Action (DoA), the Consortium Agreement (CA), the Project Handbook (D5.1), and the “Ethics and Legal Guidelines” (D5.4).

For the sake of clarity, D5.4 was released at the same time as this present document, however, it provides relevant information regarding data protection in compliance with the EU regulatory framework (e.g., GDPR).

As a result, the present deliverable does not replace any of these established agreements or deliverables, and partners should abide by the following order of precedence:

- Grant Agreement (GA)
- Commission Rules
- Consortium Agreement (CA)
- D5.1: Project Handbook
- D5.4: Ethics and Legal Guidelines

1.2 STRUCTURE OF THE DOCUMENT

The document is divided into 6 sections.

TABLE 1: STRUCTURE OF D5.5. DATA MANAGEMENT PLAN

	Section title	Summary
Section 1	Introduction	A brief explanation of the objectives of the deliverable, its relation to other project documents and the structure of the present deliverable.
Section 2	Methodology	The section highlights the methodology pursued to initially screen the research data flow, that is, a tailored DMP questionnaire submitted to all the partners of the consortium.
Section 3	Data Summary, Usage and Management	It provides a summary of the data collected and/or generated within the whole 6G4Society lifecycle, how this data is processed, as well as how data are securely stored and managed.
Section 4	Fair Data Management	This section describes the management of research data in line with the FAIR principles.
Section 5	6G4SOCIETY Compliance with the GDPR	It provides the GDPR principles that 6G4Society will follow in day-to-day activities, as well as a list of scenarios pursuant to which partners may process the personal data of individuals belonging to the consortium.
Section 6	Conclusions	Provide general conclusions of the work done.

2 METHODOLOGY

To define the DMP, the **DMP questionnaire** was initially elaborated, basing its questions on the Horizon Europe Data Management Plan Template [1]. These questions, provided in the questionnaire, aim to better understand how data is used by the 6G4Society consortium and its partners to succeed in the research activities, and the procedures enacted to manage and protect data. Subsequently, in February 2024, it was submitted to all partners of the 6G4Society project.

In the second phase, each project partner responded to the questionnaire, filling it with as much detail as possible at this stage of the project. Completed questionnaires were stored for **analysis** and traceability by CEL in its IT infrastructure.

In a third phase, the **DMP was created as a synthesis** of the questionnaire results, attempting to take advantage of commonalities between responses to provide a concise view of data management procedures within the consortium.

FIGURE 1: DMP METHODOLOGY

2.1 DATA MANAGEMENT PLAN QUESTIONNAIRE OVERVIEW

The DMP questionnaire has been defined 4 sections in order to:

- Section 1 **"Introduction":** Provide the 6G4Society partners with details on the objective of the questionnaire and the DMP activity;
- Section 2 **"Data Summary":** Get answers from the 6G4Society partners on Data Summary, i.e. summary of data to be used for the project activities;
- Section 3 **"Fair Data":** Get answers from the 6G4Society partners on Fair Data, i.e. findable (i.e., based on metadata), accessible (e.g., based on API), interoperable (i.e., based on standard formats/protocols) and re-usable;
- Section 4 **"Data Security":** Get answers from the 6G4Society partners on Data security, i.e. description of procedures and practices to ensure the security of stored and managed data.

2.1.1 Section 1 "Introduction"

This section of the questionnaire requires the provisioning of email and affiliation. This allows the users to receive by email the resume of the answers, as evidence of their participation. Moreover, this has given opportunity to discuss the answers and revise them in case of misunderstanding.

TABLE 2: DMP QUESTIONNAIRE, INTRODUCTION SECTION

DATA MANAGEMENT PLAN QUESTIONNAIRE

Dear 6G4Society partners,

as CEL, we are responsible for drafting the Data Management Plan (D5.5 - June 2024).

Data Management Plan (DMP) is 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 the 6G4Society project.

To prepare and then release this relevant project document, we need your collaboration. The Questionnaire will last you less than 15 minutes, answering to 15 questions (for most of them, you have to select options).

Therefore, we kindly ask you to provide a summary of the data you expect to work with as a partner in the overall context of the 6G4Society project.

Where it is not yet clear exactly what kind of data you will be working with, please indicate your current expectations, and at what stage in the project this information will become clearer. If you need to distinguish between different categories of data, please provide an extensive answer indicating the different categories.

Please note also that the structure and the content of the questions provided here below are consistent with the Horizon FAIR Data Management guidelines.

Deadline to complete the questionnaire: March 22 2024

Email address (to later contact you in case of doubts) *

Company *

2.1.2 Section 2 “Data Summary”

For this section, the 6G4Society partners have been requested to answer 10 questions.

TABLE 3: DMP QUESTIONNAIRE, SUMMARY QUESTIONS

QN№	Questions
1	What kind of data will you manage during the project lifecycle?
2	What types and formats of data will you generate/collect? (e.g. docx, test results, etc.)?

3	What is the expected size of the data?
4	Will you re-use any existing data (e.g., from other projects) and how?
5	Are you going to share data with other partners/actors? If yes, please provide details
6	Do you expect to process data classified as personal data during the project lifecycle? If yes, please provide details.
7	Do you expect to process data classified as “sensitive data” (e.g., data concerning health, political opinions) during the project lifecycle? If yes, please provide details.
8	If you process personal/sensitive data, is this processing performed in compliance with the relevant data protection laws? If yes, please provide details.
9	How long will data be stored?
10	Are there any ethics or legal (e.g., processing data without consent, sharing personal data with non-EEA countries) issues that can have an impact on data sharing? If so, please provide details.

2.1.3 Section 3 “Fair Data”

For this section, the 6G4Society partners have been requested to answer 4 questions.

TABLE 4: DMP QUESTIONNAIRE, FAIR DATA QUESTIONS

QN№	Questions
1	Are the data produced and/or used in the project discoverable with metadata? Are they identifiable and locatable by means of a standard identification mechanism? If so, which one?
2	What data are you working with that can be made “Open” (we have obligations to EC to support open data from the project)?
3	Are the data produced in the 6G4Society project interoperable? (if yes, how?)
4	If is there any data that may need to be closed or restricted in distribution, and if so, why?

2.1.4 Section 4 “Security”

For this section, the 6G4Society partners have been requested to answer 1 question.

TABLE 5: DMP QUETIONNAIRE, SECURITY QUESTION

QN№	Questions
1	How do you ensure the security of the data that you store and manage? Security and access processes?

3 DATA SUMMARY, USAGE AND MANAGEMENT

This section provides the reader with the collection of data summary, how data is used by the 6G4Society consortium and its partners to succeed in the research activities, and the procedures enacted to manage and protect data.

The present section is based on the analysis performed on the results from the DMP questionnaire submitted to the 6G4Society consortium at the beginning of the project. The questionnaire is presented in the previous section.

3.1 DATA FOR ACTIVITY TYPE

The analysis of the answers provided by the partners identifies a summary of the data types (data classification) that will be used during specific activities of the project, as well as the expected size.

TABLE 6: DATA TYPES IN 6G4SOCIETY

Data for Activity Type / WP	Description	Used by % of partners
ENGAG (ALL WPs)	The Engagement Data type includes all the data processed for the engagement campaign (e.g., contact details, interviews, workshops, questionnaires, survey responses, ideas and suggestions from participants, quotes, photos, and videos of activities).	83,3%
DCE (WP4)	Dissemination and Exploitation Data type includes all the data processed for the purpose of the dissemination/exploitation activities (e.g., publications, blogs, contact details, data related to the refinement of key exploitable results, market and research assessments, exploitation strategies, intellectual property rights management, standardisation and certification roadmaps, and funding sources).	66,7%
RSCH (WP1, WP2, WP3)	Research Data type (e.g., documents, analysis and insight from engagement and collaboration events).	66,7%
MNGT (WP5)	Management Data type includes all the data processed for the purpose of the project management (e.g., progress reports and financial statements, contact details), and quality and risk management (e.g., risk identification, analysis, mitigation strategies, and contingency planning. This may include quality assurance records, risk registers, risk assessment reports, mitigation plans, and contingency plans).	83,3%

The above Table 6 allows to remark how the most relevant research data are generated, collected and processed among the Engagement (83%) and the Management (83%) activities of the 6G4Society project. The result is not surprising, due to the specific objectives of the 6G4Society project, being considered the first project in the 6G-IA context which will engage a wider audience from the whole society with workshops and interviews.

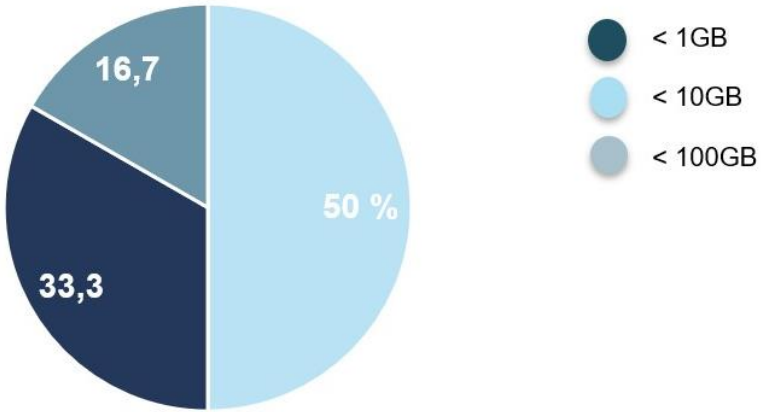

FIGURE 2: DATA SIZE IN 6G4SOCIETY

Another result from the questionnaire relates to the data size, illustrated in Figure 2. The majority of Project partners indicated they are going to handle data size of "less than 10 GB". Within this range, the most prevalent data types are generated through video and audio recordings of the engagement activities, as shown in the next section. The largest reported size falls within the "less than 100GB".

3.2 DATA FORMATS

From the analysis of the answers provided by the partners, the following table shows a summary of the data formats that will be used during the 6G4Society project, depending on the specific activity.

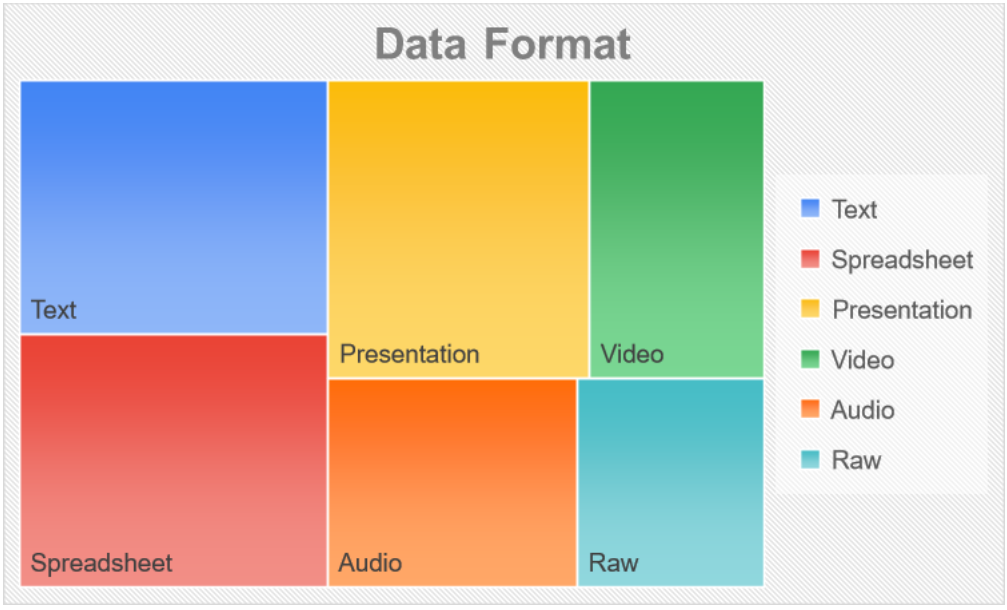

FIGURE 3: DATA FORMATS

It is important to note, that the D5.1 Project Handbook in section 6.4.2 provides the list of software formats and versions of production tools that shall be used by all partners in the project. According to this information, all the data formats managed by the partners are interoperable (as well as FAIR) ones, due to the fact that they are compliant with widely adopted (defacto) standards.

As expected, the most used data formats are Text, Spreadsheet and Presentation, that are used in almost all the activity types. While Audio, Video and Raw data are mostly used for recording and processing within the engagement activities, as well as for dissemination and communication activities.

3.3 DATA FLOW

The 6G4Society project adheres to the data lifecycle guidelines of Horizon Europe (i.e., from data creation, management, processing, to re-use). For a suitable definition of data management procedures, it is fundamental to characterise the data flow.

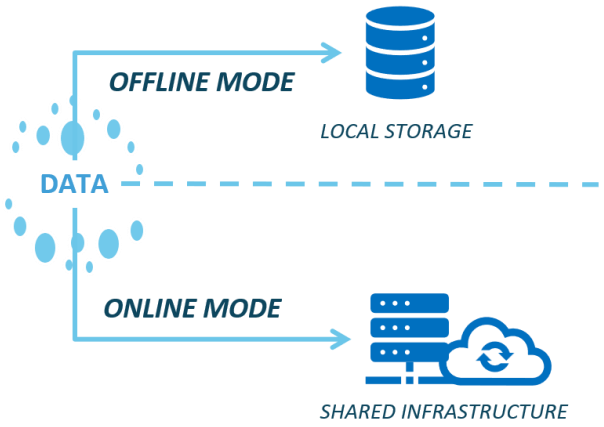

FIGURE 4: DATA PROCESS MODES

The project identifies two main treatment processes and flows, namely offline and online modes:

- **Offline mode** - data management is carried out exclusively by a specific partner, without sharing results within the consortium. This is the case when a partner is dealing with specific information and has to respect ethics and regulatory principles (e.g., personal data processing according to GDPR);
- **Online mode** – data management is carried out through the 6G4Society shared infrastructure, as well as other online services, and allows the research and innovation team to collaborate and perform activities, sharing data and results.

3.4 ACCESS TO EXISTING DATASETS

When working in offline mode the specific partner will use its own local storages and tools, while in online mode the partners collaborate in a next-to-real-time manner in data management. Definitely, the 6G4Society project builds on existing knowledge that is publicly available from scientific publications, as well as from SNS JU deliverables and standardisation bodies and fora most importantly ITU, ETSI and CEN. Table 7 summarises some of the different datasets that are input to the project.

TABLE 7: ACCESS TO EXISTING DATASETS IN 6G4SOCIETY

Dataset Name	Description of dataset	Owner/Source	Access Considerations
Scientific publications	Journals, books, conference proceedings, etc.	Publishers such as Springer [2] among other.	Available at a cost based on unit purchase or subscription basis.
Open Access Scientific Publications	Online open access scientific publications.	Respective copyright holders, such as publishers and authors, e.g.	Typically, available at no cost on the Internet.

		arXiv [3] and ERCIM [4].	
ETSI/ITU/CEN Standards	European Standard (EN), Guide (EG), Technical Specification (TS), Technical Report (TR), Special Report (SR), Group Report (GR), Group Specification (GS).	ETSI/ITU/CEN and authors of working drafts.	Available at no cost on the Internet. Working drafts available for members.
SNS JU BSCW **[5]**	Online restricted access SNS JU deliverables and publications.	Respective copyright projects and authors.	Available at no cost on the online repository. Documents available for members, according to SNS JU collaboration agreement.

3.5 DATASETS AND OUTPUTS TO BE PRODUCED

The project will create the following categories of outputs, inter alia:

- Deliverables
  - Public deliverables
  - Sensitive deliverables
- Scientific publications

3.5.1 Deliverables

In the course of the project, several deliverables will be drafted and then submitted to the EC. Deliverables will describe activities and outcomes of the project, including conceptual frameworks (e.g., technology acceptance models, taxonomy and ontology for the KPIs). It should be noted that for security reasons, already in the DoA deliverables have been classified into two different categories, depending on the level of security. In particular, deliverables are classified as (i) public deliverables, and (ii) sensitive deliverables (i.e. limited under the conditions of the Grant Agreement). A list of such deliverables is provided in the following paragraphs.

3.5.1.1 Public Deliverables

The following table provides the list of public deliverables as provided within the DoA.

TABLE 8: LIST OF PUBLIC DELIVERABLES

ID	Title	Responsible	Due Date
D1.1	Societal aspects in 6G Technology: concerns, acceptance models and sustainability indicators	CEL	M9
D1.2	Policy Brief. Towards a socially accepted and sustainable 6G	CEL	M24
D1.3	Operation Brief. Towards a socially accepted and sustainable 6G	CEL	M24
D2.1	Public Engagement Strategy and Plan	D4P	M6
D2.2	Exploring 6G technologies. Information package	D4P	M14
D2.3	Report on Public positions on 6G technology	D4P	M24
D2.4	Exploring 6G technologies - final	D4P	M24
D3.1	Report on Liaison activities	MAR	M14
D3.2	6G-IA Paper “Social Acceptance of 6G Technology”	CEL	M24
D3.3	6G-IA Paper “Key Sustainability Indicators for 6G Technology”	PSCE	M24
D3.4	Report on Liaison activities - final	MAR	M24
D4.1	Dissemination and Communication Strategy and Plan (including project website)	D4P	M4
D4.2	Dissemination and Communication Report	D4P	M24
D4.3	Exploitation Report v1	eBOS	M12
D4.4	Exploitation Report v2	eBOS	M24
D5.5	Data Management Plan	CEL	M6

3.5.1.2 Sensitive Deliverables

The following table provides the list of sensitive deliverables (i.e. limited under the conditions of the GA) as provided within the DoA.

TABLE 9: LIST OF SENSITIVE DELIVERABLES

ID	Title	Responsible	Due Date
D5.1	Project Handbook	MAR	M04
D5.2	First Progress Report	MAR	M12
D5.3	Final Progress Report	MAR	M24
D5.4	Ethics and legal guidelines	CEL	M6

3.5.2 Scientific Publications

The 6G4Society partners have set a target of publishing four scientific publications in journals and four scientific publications in conference papers to support the 6G4Society project approach. The table below provides the initial list of the relevant publications for submission, which will be further reviewed and completed in the upcoming months.

TABLE 10: PLANNED SCIENTIFIC PUBLICATIONS, STAND: JUNE 2024

Title/Topic	Conference or Journal
Towards a sustainable and socially accepted 6G for society	EuCNC 2024
Challenges of the industry: KPIs/KVIs, sustainability, Vision	SNS Journal

All scientific publications issued by the consortium will be made available through the project's website at the following link: https://www.6g4society.eu/scientific-publications/. Furthermore, these publications will be reported through the EC project management portal and will be disseminated and promoted across relevant channels such as, for example, Zenodo following open-access principles and the SNS JU BSCW Social Workspace Server, according to criteria and rules of the SNS JU collaboration agreement.

3.5.3 Handling and Storage of Research Data

Research data will be stored in different repositories, both privately and publicly accessible, to ensure long-term preservation and access. The 6G4Society project identifies this first list of storage repositories, as summarised in the Table below.

TABLE 11: STORAGE REPOSITORIES

Repository	Description	Private / Public	URL/Link (if public)
Zenodo	Zenodo (CERN/OpenAIRE) archives research data & publications (any format, free, open access). Get a DOI for easy citation & share openly or restrict access.	Public	https://zenodo.org/
6G4Society project repository	6G4Society project shared repository. Here the project shares and stores its own data, for the day-by-day project activities.	Private	---
Partners' repositories	Each 6G4Society partner uses its own internal repository for the day-by-day project activities.	Private	---
SNS JU BSCW	The SNS JU BSCW Social Workspace Server established for sharing data within the SNS JU projects, according to the collaboration agreement.	Public	https://bscw.sns-ju.eu/

3.6 ROLES AND RESPONSIBILITIES REGARDING THE DATA MANAGEMENT PLAN

Each partner is responsible for the data generated, collected, processed and in any case analysed, and disclosed.

Moreover, T5.4 is responsible for the data management lifecycle monitoring for all datasets to be collected, processed or generated by the project. To ensure alignment with data management decisions as they relate to the DMP, the following measures apply in 6G4Society:

- WP leaders are considered responsible for adhering to the specifications above in their respective work packages.
- While each partner might appoint a dedicated Data Protection Officer (DPO) or a suitably qualified expert for 6G4Society, the project manager within each organisation is considered responsible for the DMP actions. They should be accessible to the partner team in the event of any issues related to the DMP. Furthermore, it is the responsibility of the project manager and main contact from each partner to ensure that all personnel involved in the project have read the data management plan and apply/exercise all the principles outlined in the DMP.
- Partners responsible for the collection, generation and management of the data (so-called "data owners") have the ultimate responsibility of complying with the specifics of the 6G4Society DMP.

3.7 SECURITY

Based on the responses provided by the partners in the DMP Questionnaire, as well as, the Ethics and Data Protection Questionnaire, it results clear that each partner is committed to ensuring the security of the data collected and analysed, regardless of whether the data are personal or non-personal.

To safeguard data during communication and collaboration, the project will utilise existing security features provided by ICT tools, such as Google Meet and Microsoft Teams. Additionally, 6G4Society has established a shared space to facilitate seamless information exchange and file sharing among project partners. Google Drive, chosen for its compliance with all the security and GDPR requirements, serves as the Consortium's online collaboration tool.

Furthermore, partners will utilise secure repositories with restricted access rights within their organisations to securely store data. The data will be stored on password-protected devices and encrypted cloud-based services, encrypted cloud-based services that have appropriate cybersecurity measures (e.g. anti-virus software, firewalls, VPNs). Regular data backups and recovery procedures are also in place to mitigate the risk of data loss.

Partners will process personal data only where necessary and for the specific purpose for which it was gathered. These data will be anonymised or pseudonymised, as appropriate. They will adhere to their internal policies, ethics codes of conduct, and the project's Ethics and Legal guidelines (D5.4) to ensure personal data protection. Additionally, partners will provide comprehensive training to employees on data protection best practices, including how to handle sensitive information securely and use cloud-based storage safely.

As a final remark, while data will be accessible between the partners through this common space of the project, personal data will be kept confidential (due to privacy and data protection according to GDPR). In case of need-to-know, the personal data will either be anonymised/aggregated before being accessible. Alternatively, partners should sign an agreement (details are provided in section 5.5 of D5.4 - Ethics and Legal guidelines).

4 FAIR DATA MANAGEMENT

FAIR data management relates to the European Commission guidelines on the data being **F**indable, **A**ccessible, **I**nteroperable and **R**eused. Conforming to the EU guidelines, 6G4Society provides information for every used dataset in a disciplined manner, following a well-structured method for defining, creating and managing data sets. Specifically, the 6G4Society compliance to FAIR implies that the following detailed FAIR principles hold:

- FINDABLE:
  - F1. (meta) data are assigned a globally unique and eternally persistent identifier.
  - F2. data are described with rich metadata.
  - F3. (meta)data are registered or indexed in a searchable resource.
  - F4. Metadata specify the data identifier.
- ACCESSIBLE:
  - A1. (meta)data are retrievable by their identifier using a standardised communications protocol.
    - A1.1. The protocol is open, free, and universally implementable.
    - A1.2. The protocol allows for an authentication and authorisation procedure, where necessary.
  - A2. metadata are accessible, even when the data are no longer available
- INTEROPERABLE:
  - I1. (meta)data use a formal, accessible, shared, and broadly applicable language for knowledge representation.
  - I2. (meta)data use vocabularies that follow FAIR principles.
  - I3. (meta)data include qualified references to other (meta)data.
- RE-USABLE:
  - R1. meta(data) have a plurality of accurate and relevant attributes.
    - R1.1. (meta)data are released with a clear and accessible data usage license.
    - R1.2. (meta)data are associated with their provenance.
    - R1.3. (meta)data meet domain-relevant community standards.

The project partners have all provided an analysis of the data they expect to work with within the project and this will be updated during the project as the potential for new data types emerge.

4.1 NAMING CONVENTIONS AND DATA/DOCUMENT VERSIONING

In order to guarantee consistency and quality of the documents/reports, and more in general of the data that the project is going to generate, within D5.1 – Project Handbook, in section 6.4.3 “Filename Convention”, the project has provided therein the naming convention, as well the quality revision procedure.

In accordance with the abovementioned deliverable, all partners of the project should use the following file naming convention for the final version of the documents uploaded in the shared repository:

TABLE 12: FILE NAMING CONVECTION (THE TABLE IS TAKEN FROM D5.1)

6G4Society _<document name>_<version>_<date>_<company/person>.extension Where: **<date>:** dd.mm.yyyy, e.g. 30.11.2023 **<document name>** short (3-4 words) document name, e.g. D5.1 Project Management Manual **<version>:** increasing number with decimals between public releases **<company/person>:** consortium partner short name e.g. Martel or sender initials e.g. EH for Eva Hajdok e.g. **“6G4Society_D5.1_Project Manual_V01_30.03.2024.docx”**

Additionally, as a general rule, each document (either an official deliverable or internal report) is governed by the following rules:

- The document is owned by the person who initiates it. For the official documents this is the beneficiary representative listed in the DoA;
- Only the document owner should create a new (either major or minor) version of the document;
- In case a partner makes comments or changes to a document, he/she should append his/her **“_<company/person>”** field just **before the extension.**

This goes on until the document owner creates and releases the new version.

In the D5.1 is highlighted, that “the filename conventions apply to other electronic objects, besides documents, that are used to exchange project information, e.g. prototype code. If such an object is composed of multiple files organised within a directory structure (e.g., source code that has not been zipped into one file), the filename convention requirement applies only to the top directory name”.

4.2 DATA IDENTIFICATION AND SEARCHING CAPABILITIES

During the lifetime of the project, each partner will use Google Drive as a tool to upload, share and download documents, reports and more in general to get access to project data. Moreover, this 6G4SOCIETY Google Drive repository will provide users with a wide range of tools and

features essential for effective team coordination, including email, online forums, dynamic news boards, and more.

These features, combined with proper data and file-naming conventions, will facilitate efficient data searching capabilities for 6G4Society, directing to data itself, data owners, report owners/authors as well as data contributors.

Additionally, to enhance searchability, each deliverable/report owner will include some metadata (as keywords) directly into the document, facilitating easier search within documents, reports, deliverables etc.

4.3 METADATA PROVISIONS AND DATA INTEROPERABILITY

As outlined in the previous section regarding data identification and searching capability, the 6G4Society document and data repository build the actual data model that supports several identification mechanisms (based on keywords, tags, unique identifiers etc.). This ensures that respective metadata information is easily kept, extracted and referenced for all purposes of data handling and utilisation within 6G4Society.

6G4Society considering the primary importance of metadata provisioning and searching capabilities, will be used as the channels to enable data interoperability. Well-agreed and proper data/file naming conventions, in combination with file tagging and advanced search capabilities, will enable and maximise data interoperability inside 6G4Society.

5 6G4SOCIETY COMPLIANCE WITH GDPR

The protection of individual's personal data and privacy rights is one of the priorities of all the partners during the entire duration of the 6G4Society.

Indeed, as it results from the DoA, as well as according to the answers provided by the partners to the Data Management Plan questionnaire and Ethics and Data Protection questionnaire submitted in February and March 2024, for the purposes of the project, some of the 6G4Society activities might entail personal data processing. In this respect, within the D5.4 – Ethics and Legal guidelines it has been provided with those guidelines and procedures that partners should follow to comply with data protection rules and ethics principles regarding data processing of third-party individuals.

The present section instead, without prejudice to the above, will provide a non-exhaustive list of scenarios pursuant to which partners may process the personal data of individuals belonging to the consortium.

5.1 GENERAL PRINCIPLES APPLICABLE IN CASE OF PERSONAL DATA PROCESSING

As a general rule, when it comes to process personal data of individuals (regardless to their affiliation or their nature as individuals external to the consortium) each 6G4Society partner commits to respect the GDPR Regulation, as well as any other applicable laws and regulations concerning data protection and privacy rights.

To this extent, it is valuable to briefly outline the fundamental principles of data processing (a more detailed description of all principles is provided in section 5.2 of D5.4 (Ethics and Legal Guidelines).

First of all, personal data shall be processed **lawfully, fairly and in a transparent manner** in relation to the data subject. To this extent, each partner commits to process personal data in a way that ensures compliance with the principle of **purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality,** and **accountability.**

In light of the above, in any case of processing of personal data, the interested 6G4Society partner will remain accountable and responsible for the data collected during the project and will be required to ask for consent before those data is collected (provided that any other lawful basis is not applicable). In addition, all partners processing personal data are aware by means of the current guidelines of their obligations as potential data processors (where appropriate) as well as issues beyond data and information protection and privacy here described.

Personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Technical or organisational measures shall permit the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. At the end of the project, all processed personal data shall be destroyed in accordance with the specific law requirements.

5.2 DAY-TO-DAY DATA USAGE AND PROCESSES RELATED TO PROJECT MANAGEMENT

In light of the above, the present paragraph is dedicated to identifying those sets of activities entailing personal data processing of individuals belonging to the 6GSociety consortium.

TABLE 13 : DAY-BY-DAY DATA PROCESSING SCENARIO

Scenario	Solution
6G4Society mailing list	To achieve 6G4Society results, and also to manage the workflow among all the partners involved in the project, it has been created a mailing list. Its scope is to keep updated the relevant partners on tasks, events, and the progress of the project in general. Moreover, the same mailing lists created are restricted only to 6G4Society partners, and the end of the project will be erased. The management of this mailing list, i.e. the additions and/or removals, are responsibility of MAR (i.e. the Coordinator). In any case, it will be the responsibility of each partner to be sure to get the consent of the relevant person before including his/her contact in the mailing; moreover, each person included in a mailing has the right to opt-out by contacting the Coordinator.
Meetings and related material	During 6G4Society meetings, whether virtual or in person, various documents may be created and used, such for example, agendas, presentations, and minutes. These documents will be created and managed only inside the consortium and its partners and will solely serve the purposes of the relevant meeting. Furthermore, each partner may access the documents, which will be stored in the project's internal shared repository (Google Drive). The retention of these documents will be restricted to 2 years following the conclusion of the project. In accordance with applicable law, individuals whose personal data is included therein shall have the right to request at any time to the Coordinator to opt-out.
Workshops/Conferences, training and dissemination sessions	Events such as workshops, conferences and plenary meetings might be attended by one or more individuals belonging to the consortium. Personal data such as names, surnames, company affiliations, emails, and images/videos might be gathered during these events. This data might be collected and utilised not only for event organisation but also for dissemination purposes. In cases of dissemination, before the publication, relevant individuals might request to opt-out from publication by contacting the Coordinator via email.

	The data will be stored in the 6G4Society shared repository and retained for 2 years after the project's conclusion.
Reporting	Reports providing for updates on the Project progress, as well as on financial data, might contain personal data. These reports might be shared either within and outside the Consortium for compliance purposes with national financial law, and in particular with the EC.
Deliverables, internal documents and other 6G4Society reports	Throughout the 6G4Society project lifecycle, many documents and reports will be generated, relating to the project deliverables and/or internal documents. These files will be used to meet contractual obligations and will be shared with 6G4Society partners, the Granting Authority, the EC, and, where applicable, external parties (as this might be the case for those deliverables that are classified as public and might be published on 6G4Society website). These documents may contain the names or email addresses of the authors. Internally within 6G4Society and EC distributed documents are related, they will be utilised only for reporting purposes and stored in the 6G4Society cloud server under the deliverables section. Publicly shared reports (public deliverables) will only reference the partner's name and exclude any other personal data. All reports will be retained for more than 2 years following the conclusion of the project.
6G4Society website - cookies	In the cases that in any 6G4Society application (web) the usage of cookies is needed, a related pop-up window informing the user must be present, prompting the user to accept (or not) the conditions under which her/his personal information is stored. 6G4Society will maximise efforts to reduce the usage of cookies in its web developments.
Other scenarios not included above	As a general principle, whenever personal data is needed to be included in any document for the purposes of the project, the controller (i.e., the document creator) shall have to notify the data subject. This notification should specify that his/her personal data will be included in the related document, along with details regarding the purposes, retention period, storage requirements, etc.

6 CONCLUSIONS

Deliverable D5.5 "Data Management Plan" reports the results of the first six months of activities in the context of the 6G4Society project and specifically in Task T5.4 “Data Management”. In particular, to develop this important document for the project's entire duration, the DMP questionnaire was initially elaborated and circulated among the partners at the project beginning (M2). Consequently, the DMP was created as a synthesis of the questionnaire results.

DMP provides an overview of the data that will be created, processed, and utilised within 6G4Society, detailing the types, formats, and sizes of the data managed by the 6G4Society partners. In addition, the deliverable includes a presentation of the details that allow the research data to be findable, accessible, interoperable, and reusable (FAIR), with special attention to the handling of research data during and after the end of the project, what data will be collected, processed and/or generated, which methodology and standards will be applied, and how data will be shared and preserved (including after the end of the project). It also provides details on how partners will ensure the security of the data collected and analysed, regardless of whether the data is personal or non-personal.

A separate section of the report is dedicated to the protection of personal data, detailing data protection principles and offering a non-exhaustive list of scenarios under which partners may process the personal data of individuals belonging to the consortium.

The DMP is a living document, subject to periodic revisions to reflect changes in project data. If updates are needed, these will be reported in the D5.2 - First Progress Report (M12) and D5.3 - Final Progress Report (M24).

Co-funded by the European Union

REFERENCES

[1] European Commission, “EU Grants: Data management plan (HE): V1.1,” 2022. [Online]. Available: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/temp-form/report/data-management-plan_he_en.docx. [Accessed May 2024].

[2] Springer, “Springer Open,” [Online]. Available: https://www.springeropen.com/. [Accessed May 2024].

[3] Arxiv, “Arxiv,” [Online]. Available: https://arxiv.org/. [Accessed May 2024].

[4] ERCIM EEIG, “Ercim News,” [Online]. Available: https://ercim-news.ercim.eu/. [Accessed May 2024].

[5] Fraunhofer FIT and OrbiTeam, “BSCW Social Workspace Server,” [Online]. Available: https://bscw.sns-ju.eu/. [Accessed May 2024].

[6] IEEE Communications Society, “Publications,” [Online]. Available: https://www.comsoc.org/publications/journals. [Accessed May 2024].