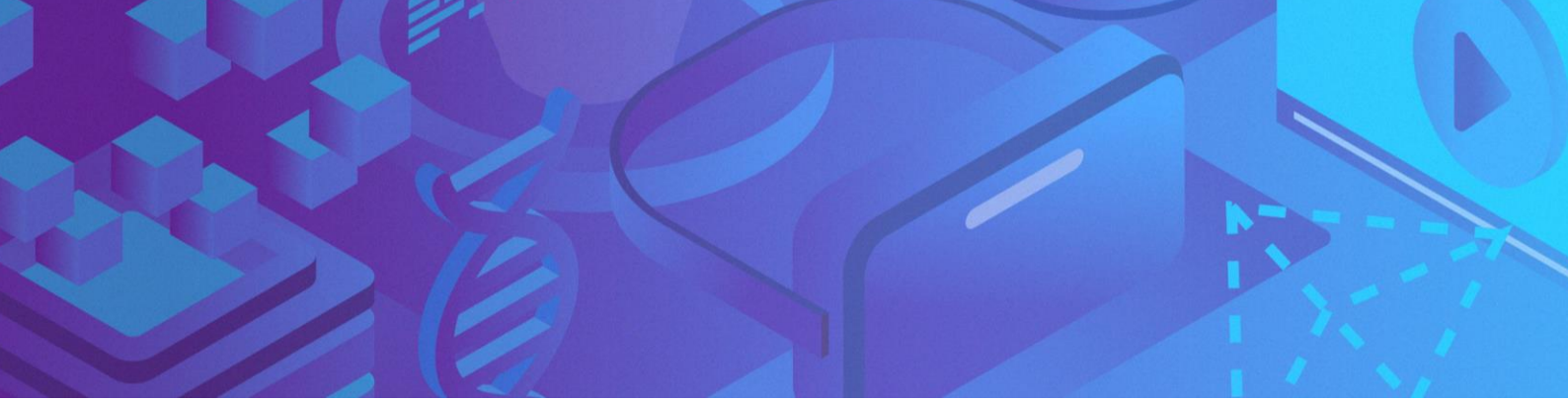

D1.2 DATA MANAGEMENT PLAN

Revision: v.1.0

Work package	WP 1
Task	Task 1.2
Due date	31/03/2023
Submission date	02/10/2023
Deliverable lead	Deutsche Telekom
Version	1.0
Authors	Vivien Helmut (DTAG)
Reviewers	Maria Chiara Campodonico (D4P)
Abstract	The SPIRIT DMP will describe the data that will be collected, processed and/or generated as part of the project, the methodologies and standards that will be applied to make research data FAIR, the data that will be shared/made open, and how it will be curated and preserved during and after the lifetime of the project.
Keywords	Data Management Plan.

Grant Agreement No.: 101070672
Call: HORIZON-CL4-2021-HUMAN-01

Topic: HORIZON-CL4-2021-HUMAN-01-25
Type of action: HORIZON-RIA

Document Revision History

Version	Date	Description of change	List of contributor(s)
V0.1	20/02/2023	ToC	Vivien Helmut *(DTAG)*
V0.2	08/03/2023	Additional Content Open Call Input	Vivien Helmut *(DTAG)* Maria Chiara Campodonico *(D4P)*
V0.3	22/05/2023	Additional Content	Vivien Helmut *(DTAG)*
V0.4	12/09/2023	Additional Content/Editing	Vivien Helmut *(DTAG)*
V1.0	28.09.2023	Additional Content/Review	Hermann Hellwanger (UniKlU), Maria Chiara Campodonico *(D4P)*

DISCLAIMER

COPYRIGHT NOTICE

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.

Funded by the Horizon Europe Framework Programme of the European Union

DMP: Data management plan

ETHICS: Deliverables related to ethics issues.

SECURITY: Deliverables related to security issues

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

Funded by the Horizon Europe Framework Programme of the European Union

EXECUTIVE SUMMARY

A Data Management Plan (DMP) is a written, formal document that describes how data will be handled until project completion and thereafter. The Guidelines on FAIR Data Management in Horizon 2020 [5] provide a set of principles and criteria to be followed.

The SPIRIT DMP will describe the data that will be collected, processed and/or generated as part of the project, the methodologies and standards that will be applied to make research data FAIR, the data that will be shared/made open, and how it will be curated and preserved during and after the lifetime of the project.

One essential part of the SPIRIT project is providing a platform for experimentation by third party experimenters (Open Call). Each experiment that generates open research data will need its own DMP. The project can only provide some guidance regarding the creation of experiment specific DMPs.

This document is divided into two sections. The first part is the Data Management Plan for the handling of data within the project. The second part describes the initial procedure and first recommendations for the Data Management generated by the Open Call experiments.

Funded by the Horizon Europe Framework Programme of the European Union

TABLE OF CONTENTS

Funded by the Horizon Europe Framework Programme of the European Union

LIST OF FIGURES

Funded by the Horizon Europe Framework Programme of the European Union

LIST OF TABLES

Funded by the Horizon Europe Framework Programme of the European Union

ABBREVIATIONS

DOI	Digital Object Identifiers
DMP	Data Management Plan
EC	European Commission
FAIR	Findable, Accessible, Interoperable, and Reusable
GDPR	General Data Protection Regulation
IP	Internet Protocol
IPR	Intellectual Property Rights
LL-DASH	Low Latency Dynamic Adaptive Streaming over HTTP
QoE	Quality of Experience
SPIRIT	Scalable Platform for Innovations on Real-time Immersive Telepresence
TCP	Transmission Control Protocol
WebRTC	Web Real-Time-Communication

….

Funded by the Horizon Europe Framework Programme of the European Union

1 INTRODUCTION

A Data Management Plan (DMP) is a written, formal document that describes how data will be handled until project completion and thereafter. The Guidelines on FAIR Data Management in Horizon 2020 [5] provide a set of principles and criteria to be followed.

The **Horizon Europe Model Grant Agreement** requires that a data management plan is established and regularly updated. A first version of the DMP – this document – was planned at M6 and updated versions of the DMP will be provided with the periodic project reports as relevant.

The SPIRIT DMP will describe the data that will be collected, processed and/or generated as part of the project, the methodologies and standards that will be applied to make research data FAIR, the data that will be shared/made open, and how it will be curated and preserved during and after the lifetime of the project.

One essential part of the SPIRIT project is providing a platform for experimentation by third party experimenters (Open Call). Each experiment that generates open research data will need its own DMP. The project can only provide some guidance regarding the creation of experiment specific DMPs.

This document is divided into two sections. The first part is the Data Management Plan for the handling of data within the project. The second part describes the first recommendations for the Data Management for the Open Call experiments.

During the course of the project the data management plan will evolve according to the needs and challenges of the project.

Funded by the Horizon Europe Framework Programme of the European Union

2 DATA MANAGEMENT PLAN FOR PROJECT DATA AND OUTPUT

The project will collect and generate a variety and considerable amount of data and outputs to implement the project use cases as well as the experimental platforms for the open call. In this section the management of data generated by the project partners is described.

In the SPIRIT project three essential aspects must be considered when dealing with data: The Open Access of publications, Open Data, and the IPR restrictions included in the Grant Agreement and the Consortium Agreement.

In general, partners need to consider that their project results have to be disseminated as soon as feasible, in a publicly available format, subject to any restrictions due to the protection of intellectual property, security rules or legitimate interests[1]. This means that beneficiaries have the right to protect the results if the institution plans to protect or exploit the results.

2.1 DATA SUMMARY

During the lifetime of SPIRIT project several documents and data sets will be generated.

2.1.1 Project-specific Documents

Project-specific documents to be generated and managed are reports on requirements analysis and architecture definition; use case descriptions; documentation of technologies and APIs.

These documents, collectively, offer clear documentation, guidelines, and insights for project partners, ensuring a shared understanding of the project's requirements, architecture, use cases, and technology components. They facilitate effective collaboration, streamline the development process, and enable project partners to work cohesively toward the project's objectives.

Additionally, the final versions of these documents are also project deliverables and will be shared with the public.

2.1.2 Publications

Besides the afore mentioned documents there will be additional documents, like

- Scientific and commercially oriented publications
- Documents for standardisation efforts
- Material for and result of the open calls and experimentation
- Communication and Dissemination material

2.1.3 Data sets

[1] Grant Agreement Article 17 supplement

Funded by the Horizon Europe Framework Programme of the European Union

The datasets generated by the project play a crucial role in various aspects of technology development, integration, testing, and evaluation of the proposed technologies and methodologies. They provide the foundation for research and development activities, to improve the SPIRIT framework. The data will provide the necessary input for fine-tuning algorithms and validating system performance. These datasets are used internally for framework improvements, as base for scientific publications, and be included in materials for the Open Calls. Table 1 : Data output from various project tasks, contains an overview of the planned project tasks, which generate this kind of data.

Some data will be manually collected. For example, in Quality of Experience (QoE) surveys. Manually collected datasets for quality of experience (QoE) and usability evaluations aim to assess the user's perception, satisfaction, and overall experience with a particular technology, application, or system. They provide valuable insights into the user's perspective.

TABLE 1 : DATA OUTPUT FROM VARIOUS PROJECT TASKS

Project Task	Data output	Occurence
3.1 Network layer innovation	Performance monitoring of network and application metrics to steer transmission of immersive media and adaptive streaming mechanisms.	Each session
3.3 Application layer innovation	Identification and test of (1) content types and (2) use cases where LL-DASH/WebRTC	Limited time period
3.4 Content innovation	real-time captured humans	Each session
4.2 Technical integration and validation	detailed tests will be performed	Limited time period
4.3 Use case development and integration	Validation of the proposed scenarios, performance evaluation and user experience testing following Task 4.4 metrics.	Each session
4.4 User experience evaluation and usability validation	Perform limited subjective tests	Limited time period
4.4 User experience evaluation and usability validation	Develop and provide “QoE tools”, including APIs for objective QoE estimation and procedures for subjective tests, to be used in the Open Call experiments.	Each session
5.2 Open call experimentation	Data from participant’s experiments	Session/ Limited time period

Funded by the Horizon Europe Framework Programme of the European Union

2.1.4 Data Management Process

In this section the process for handling data collected during the project is depicted. Figure 1: Data Management process provides an overview followed by a detailed description.

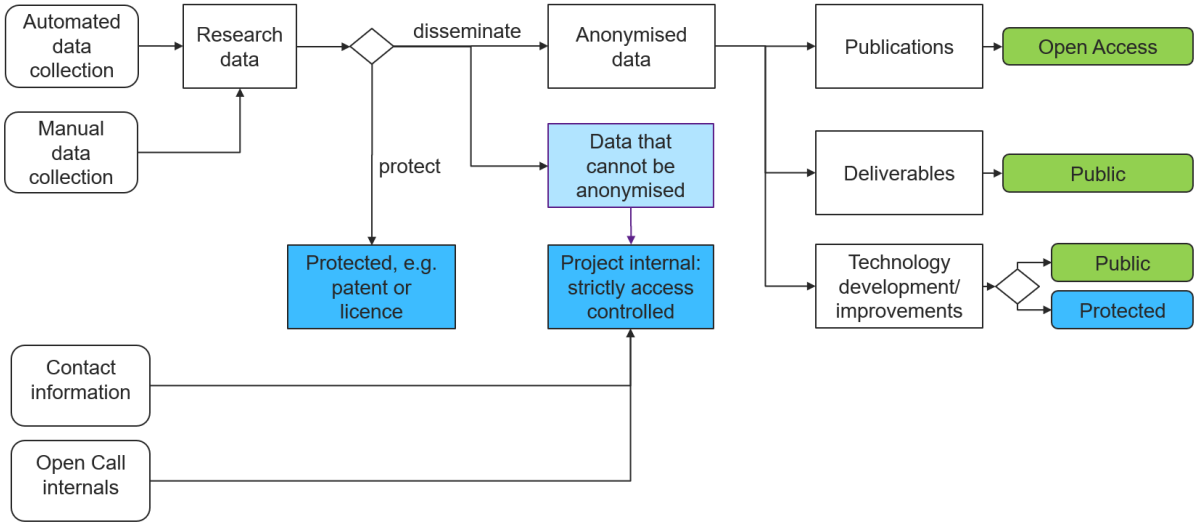

FIGURE 1: DATA MANAGEMENT PROCESS

The Data Management Process starts with data collection, which takes place in a secure environment. This environment ensures that appropriate security measures are in place to protect the data from unauthorized access, breaches, or leaks. This may involve using secure servers, encryption techniques, access controls, and monitoring systems to safeguard the data during the collection phase.

Following the data collection, the next step involves extracting or identifying the relevant research data. This step aims to filter out unnecessary or irrelevant information and focus on the data that is most pertinent to the research objectives or questions. During this phase, it's important to maintain data integrity and security.

In cases where the research data is intended for dissemination purposes, it is crucial to protect the privacy and confidentiality of individuals involved. Anonymization techniques are employed to remove or modify any personally identifiable information from the data, ensuring that the identities of the individuals cannot be discerned.

After the data has been anonymized, it serves as the foundation for publications or deliverables. Researchers analyse and interpret the data to draw conclusions, make discoveries, or derive insights. These findings are then shared through various means such as research papers, articles, reports, or other forms of dissemination, depending on the intended audience and purpose.

When utilizing the anonymized data for publications or deliverables, privacy considerations remain a priority. Researchers should ensure that the disseminated findings do not compromise the privacy or confidentiality of individuals. Careful attention is given to avoid any unintended re-identification or disclosure of sensitive information.

In cases where intellectual property potential can be identified within the data. The identified intellectual property is protected through various means, e.g., filing patents. Once the intellectual property is adequately protected and developed, partners can reconsider the dissemination option.

Funded by the Horizon Europe Framework Programme of the European Union

In cases where it is not possible to anonymize the collected data while maintaining its integrity, the raw data remains confidential and is not shared. However, the research findings and insights derived from the data analysis are carefully extracted and shared in publications, reports, or other appropriate means.

2.2 FAIR DATA

A key enabler for the successful dissemination, exploitation and potential innovations of the results is openness. SPIRIT commits to bring research results closer to the public and adhere to the Open Access guidelines set by the Horizon Europe Work Programme. The acronym FAIR stands for **Findable, Accessible, Interoperable**, and **Reusable**, and these principles were developed to address the challenges researchers face in managing and sharing their data effectively. In line with these guidelines, all the scientific publications supported by the project will be available as Open Access through an OpenAire-compliant repository such as Zenodo and the Open Research Europe publishing platform, to select open access repository and/or deposit publications for its research results storage, allowing also for easy linking with the EU-funded project.

The partners will prioritize Journals that are indexed and Conferences, Workshops, and scientific events ensuring recognized impact. Partners will be required to perform a plagiarism check prior to any submission and verify the findings of the paper.

- Any consortium member should consider the Consortium Agreement stipulations prior to the submission of a scientific article for publication.
- Open Access (OA) journals that do not require transfer of IPR will be prioritized.

Beyond research publications, project summaries, presentations, general information, and public reports and deliverables will be made available through the project website also to effectively communicate and coordinate, if possible, with parties outside the consortium, such as other related projects or the EC.

The following subsections describe in more detailed the measures to make data generated within in the SPIRIT project FAIR.

2.2.1 Making data findable, including provisions for metadata

The data and outputs resulting from the project will be stored in secure and trusted repositories that comply with OpenAire standards. Specifically, repositories such as Zenodo[7] and Open Research Europe publishing platforms will be utilized as the default choices.

To ensure the accessibility and discoverability of these outputs, each item will be assigned persistent and unique identifiers, such as digital object identifiers (DOIs). These identifiers serve as permanent links to the outputs, enabling their long-term availability and traceability.

Additionally, comprehensive metadata will be associated with each output. This metadata includes various details such as identifiers, keywords, data type, authorship information, and licenses. By providing detailed metadata, the outputs can be easily found and identified through search engines and other relevant discovery platforms.

The combination of persistent identifiers and rich metadata enhances the findability and identification of the project's outputs, facilitating broader access to the research findings. This approach ensures that the outputs are properly catalogued, enabling researchers and interested individuals to locate, cite, and build upon the work effectively.

Funded by the Horizon Europe Framework Programme of the European Union

2.2.2 Making data accessible

The use of the repositories mentioned in section 2.2.1 will make it possible to keep the data available after the project finished, adhering to OpenAire guidelines in Horizon Europe (https://www.openaire.eu/horizon-europe), and thus to the EC's Open access & Data management guidelines, following the principle "as open as possible, as closed as necessary". The repositories used will be included in registries of scientific repositories to increase the accessibility of the obtained results.

Even though the project will work toward open access, when possible, specific project results could also be protected and exploited, and therefore IPR handling rules will be provided. IPR management will be detailed in the Consortium Agreement (CA), indicating what structures and processes will apply during the project lifetime, IPR considerations and timeline for open access (if specific outputs will not be shared as open access), as well as provisions for access to restricted data for verification purposes.

2.2.3 Making data interoperable

To promote interoperability, re-usability, and facilitate searching, filtering, and analysis activities, the project will adopt existing standards and formats for specifying, describing, and classifying datasets and data types, along with their associated metadata.

By utilizing established standards and formats, the project ensures compatibility and seamless integration with existing data infrastructures and systems. Furthermore, the project emphasizes the openness of the metadata. Open metadata implies that the metadata associated with the datasets and data types will be publicly accessible, enabling transparency and facilitating the discovery and understanding of the data. This openness enhances the potential for wider adoption and reuse of the project's datasets.

By adopting existing standards and formats and ensuring open metadata, the project aims to promote seamless interoperability, encourage re-usability of the datasets and data types, and facilitate effective searching, filtering, and analysis activities.

During the project, further details regarding the specific standards and formats to specify, describe, and classify the datasets and data types, along with their associated metadata, will be provided. These details will be determined through careful evaluation and consideration of relevant industry practices and community guidelines. The project team is committed to selecting standards and formats that promote interoperability, re-usability, and facilitate searching, filtering, and analysis activities. Updates and specific recommendations on the formats will be shared as the project progresses, ensuring the adoption of appropriate and widely accepted approaches that align with best practices in the field.

2.2.4 Increase data re-use

Open Access Sharing in trusted and OpenAire-compliant repositories, with a strong focus on assignment of licenses toward data sharing and re-usability (e.g. Creative Commons, Open Data Commons), together with the usage of data and metadata standards, will ease and promote the re-usability of data outputs. This will in turn ease the adoption of existing tools / software / models for data generation and validation / interpretation / re-use, as well as the development and sharing of new ones to both analyse the obtained results.

2.2.4.1 Quality assurance process

At the start of the project, a procedure was defined by which all deliverables and project-related documents would first undergo an internal quality-check prior to publishing the document to

Funded by the Horizon Europe Framework Programme of the European Union

the outside world. Through this approach we expect to ensure high data quality within the project, promoting project data reuse and sharing.

2.3 OTHER RESEARCH OUTPUTS

An important resource in the Spirit project is software, both for partners and experimenters. Some of the software is made available to the public as open source. For this, public repositories and links to the repositories are shared, e.g., first on the SPIRIT website and later in OpenAire repositories.

2.4 DATA SECURITY

In this chapter, the security features of the research data infrastructure used to store and handle data in the SPIRIT project are described.

The components provided by partners to the SPIRIT testbeds, e.g., application frameworks and use case applications are developed and maintained in the partner's development environments. The partners are responsible for the security and privacy in their development environments, e.g., access restrictions and back-up. It is expected that the partners ensure in their own interest the security and privacy of these environments. Therefore, these environments are out of scope for the data management of the project.

2.4.1 Data Security imec's Teams Workspace

Imec's MS Teams Workspace is the online collaboration platform used by the SPIRIT project. A dedicated project workgroup has been established on this platform, accessible only by the partner representatives in the consortium. As part of the Teams Workspace, a Sharepoint instance is used for data collaboration and sharing.

The SPIRIT Teams Sharepoint has the following security settings:

- Access level: Restricted to persons (project members only).
- Encryption with SSL/TLS protects data transfer between partners and the SharePoint site.
- The version management documents content changes and prevents accidental loss of data.
- Microsoft Teams ensures regular backups of the stored data
- The data is available after the end of the project. If necessary, the contents of the team server will be archived and made available to the partners.

Documents and elements in the MS Teams Workspace are stored in Microsoft's cloud solution Azure. The Azure instance hosting MS Teams Workspace is located in Europe.

2.4.2 Data security as specified for Zenodo

Regarding Zenodo's security the website[2] states:

We take security very seriously and do our best to protect your data.

[2] https://about.zenodo.org/infrastructure/

Funded by the Horizon Europe Framework Programme of the European Union

- CERN Data Centre: Our data centres are located on CERN premises and all physical access is restricted to a limited number of staff with appropriate training and who have been granted access in line with their professional duties (e.g. Zendo staff do not have physical access to the CERN Data Centre).
- Servers: Our servers are managed according to the CERN Security Baseline for Servers, meaning e.g. remote access to our servers are restricted to Zenodo staff with appropriate training, and the operating system and installed applications are kept updated with latest security patches via our automatic configuration management system Puppet.
- Network: CERN Security Team runs both host and network-based intrusion detection systems and monitors the traffic flow, pattern and contents into and out of CERN networks in order to detect attacks. All access to zenodo.org happens over HTTPS, except for static documentation pages which are hosted on GitHub Pages.
- Data: Zenodo stores user passwords using strong cryptographic password hashing algorithms (currently PBKDF2+SHA512). Users' access tokens to GitHub and ORCID are stored encrypted and can only be decrypted with the application's secret key.
- Application: We are employing a suite of techniques to protect your session from being stolen by an attacker when you are logged in and run vulnerability scans against the application.
- Staff: CERN staff with access to user data operate under CERN Operational Circular no. 5, meaning among other things that
    - staff should not exchange among themselves information acquired unless it is expressly required for the execution of their duties.
    - access to user data must always be consistent with the professional duties and only permitted for resolution of problems, detection of security issues, monitoring of resources and similar.
    - staff are liable for damage resulting from any infringement and can have access withdrawn and/or be subject to disciplinary or legal proceedings depending on seriousness of the infringement.

2.4.3 Data Security in Testbeds

The data security in testbeds has to compliant to the GPDR and the complementary Directive 2002/58/EC [1] on privacy and electronic communications (ePrivacy Directive), which concerns the processing of personal data and the protection of privacy in the electronic communications sector and states specific requirements concerning the protection of personal data and privacy of the users of electronic communication services.

The testbeds of the SPIRIT platform consist of network infrastructure and application frameworks. The network infrastructure handles mainly authorization data but the application frameworks for telepresence applications process personal data, e.g., video, audio, and control information.

The use of data generating monitoring systems within the SPIRIT platform, e.g., latency measurements, which can be used in or interfaced to applications, will be limited to specific experiments. When data is stored for later analysis, the data is protected at least by means of pseudonymisation and encrypted storage. Access to it is limited to authorized personnel.

For each testbed and application framework instance a privacy & security person is appointed to act as a contact for any data security and data protection issue regarding this component.

Funded by the Horizon Europe Framework Programme of the European Union

For the requirements to be met by the SPIRIT testbeds see section 2.5.1.1

During the project the information in this section will be extended.

2.4.4 EU classified information

At the present time and in the foreseeable future no handling of EU classified information is expected. If during the project classified information will be generated or processed, Article 19 and Article 22 of Commission Decision 2015/444 [4] on the security rules for protecting EU classified information (March 2015) will be followed.

2.5 ETHICS

The whole consortium commits in full on strictly adhering to all the European GDPR regulations. All data subjects, at any point in time, will be able to execute their data rights by contacting the consortia through the website.

The project will comply with key EU juridical frameworks such as 2002/58/EC [1], the (EU) 2016/680 [2], also known as General Data Protection Regulation (GDPR) and the Charter of Fundamental Rights of the European Union 20212/C326/02 [3]. Any action taken within the project needs to be compliant with all fundamental rights enshrined in this Charter.

Although as such the project does not contain any serious or complex ethics issue, leading to an ethics clearance, in response to the Ethics Summary Report, the consortium will appoint an external ethics advisor to check the compliance of potential ethics issues.

This ethics advisor with expertise in Horizon Europe Ethics guidelines and in GDPR requirements, will be appointed to report on human participants and personal data protection. The advisor will be consulted at least on the following points:

- recruitment procedures, informed consent forms and information sheets
- guidance on the handling of personal data specific to the project in compliance with GDPR.

2.5.1 Collecting personal data from tests and experiments

Data collection activities (interviews, surveys, etc.) will be designed to maintain privacy according to the General Data Protection Regulation (GDPR). Personal data will not be requested unless this is necessary. Vulnerable groups like minors and individuals unable to freely provide an informed consent will be excluded. Participation is voluntary. Participants will be given the possibility to decline and withdraw their participation at any time.

All personal data will be stored on secure servers with access control. Personal data will be handled by authorised personnel, and no one will have access to the data unless this is necessary to carry out the project work. On demand by the participants, their data will be deleted.

2.5.1.1 GPDR and the ePrivacy Directive

Application providers of practical tests and experiments shall verify for their specific application that their implementation meets the requirements of the GPDR and the ePrivacy Directive. These applications will be initially provided by the project partners to develop the Spirit Platform further, but the following section also applies to the Open Call phases.

Funded by the Horizon Europe Framework Programme of the European Union

The following requirements must be met by the network infrastructure and the application frameworks.

- Authentication of identities: Each identity accessing the system will be authenticated and appropriately authorised to be able to use it.
- De-activation of authentication credentials: Personal authentication credentials shall be de-activated if they have not been used for at least six months.
- Purpose limitation: As set out by article 5 of the GDPR, the SPIRIT platform will process personal data only for security purposes, unless the data controller configures the system to pursue other legitimate, specific, and explicit purposes, determined at the time of collection of the data.
- Regular monitoring of security: The SPIRIT platform will regularly monitor the system's status in terms of security for personal data as required by article 32 of the GDPR.
- Data breach information: The SPIRIT platform must immediately inform its users of any breach to personal data leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed as required by articles 33 and 34 of the GDPR.
- Security of processing: SPIRIT application frameworks will protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access through the implementation of technical and organisational measures to ensure a level of security appropriate to the risk as required by article 32 of the GDPR.

In addition to the security requirements of the SPIRIT platform, application providers shall meet the following requirements for their application data, too.

- Right of access: The SPIRIT Applications shall support providing to every data subject, without excessive delay or expense, confirmation as to whether or not data relating to him/her are being processed and information as to: the purposes of the processing; the categories of data concerned; the recipients to whom the data are disclosed; the envisaged period of storage for the data; and the existence of automated decision-making processes within the system. The legal source of this requirement is article 15 of the GDPR.
- Right of erasure: The SPIRIT Applications must ensure that the right of erasure exercised by data subjects towards the data controller is enforced, when the conditions set out by article 17 of the GDPR are met.
- Data portability: As detailed by article 20 of the GDPR, SPIRIT Applications must be able respond to requests for data portability lodged by the data subjects. This entails that the data subject shall receive the data in a structured, commonly used, and machine-readable format.

These lists might be extended during the project.

2.5.1.2 Information letter and consent form

The participants of tests and experiments will be given an information letter and a consent form (on paper or electronically). The information letter will provide information about:

The type of data that will be collected during the study.

- How the data will be collected (interview, automatic data collection, etc.)
- What the data will be used for. The information letter will explain the purpose of the project and the expected results. It will also be explained that published information always will

Funded by the Horizon Europe Framework Programme of the European Union

be anonymous, and that no personally identifiable information will be published in any way.

- How the data collected will be handled. The information letter will explain that personal data will be treated in full confidentiality and will be registered and stored in a secure manner. The data will be de-identified before it is processed (name or other characteristics serving to identify person will be replaced by a number and the list of identifiers will be kept separate from the data).
- When the personal data will be deleted.
- Who will have access to the data. The information letter will state that data will be handled by a very limited number of authorised personnel and that confidentiality will be regulated by legal agreements. The data will be de-identified before it is discussed and processed within the project.
- The rights of the participants. The information letter will state that participation is voluntary and that participants have the right to see the data collected about them and that they can withdraw from the study at any time without any obligation to explain their reasons for doing so (contact information for such requests will be provided).

2.5.2 Managing contact information

Contact information will never be shared with third parties, and only the essential information needed will be kept and stored. On request from external parties, the project will provide information on the personal information the project is managing related to this party, as well as provide opportunity to correct or delete information (upon withdrawal of consent).

2.5.3 Managing Open Call internals

In the Open Call application phase to select Financial Support to Third Parties (FSTP) as experimenters the project pursues the following goals.

- **Transparency**: Provide clear and concise information to FSTP applicants about the processing of their personal data, including the purpose of the processing, types of data collected, recipients of the data, and their rights regarding their personal data. This information should be communicated through a transparent privacy notice or policy.
- **Data Minimization**: Only collect and process the personal data necessary for the evaluation and processing of FSTP applications. Minimize the data collected to the specific and relevant information required for the purpose.
- **Data Security**: Implement appropriate technical and organizational measures to protect the personal data obtained from FSTP applicants. This includes measures such as encryption, access controls, regular security assessments, and secure storage of the data.
- **Legal Basis**: Ensure that you have a lawful basis for processing personal data obtained from FSTP applicants. This could be based on the applicant's consent, contractual necessity, legal obligations, legitimate interests, or other applicable legal grounds.

Funded by the Horizon Europe Framework Programme of the European Union

3 DATA MANAGEMENT FOR OPEN CALL EXPERIMENTS

Another goal of the SPIRIT data management is to provide mechanisms to enable open research data from the outputs of experiments running within the SPIRIT testbeds to be made publicly available in open access form.

At present it is not possible to provide a detailed initial data management plan concerning the data that will be generated within the project by third party experimenters. Each experiment that generates open research data will need its own DMP which will be a clear requirement for the third party. Participants to the open calls will be requested to fill in a template based on the "EU Grants: Data Management Template (HE): V1.0 – 05.05.2021" or, if any, more updated versions.

The following table contains the initial questionnaire that needs to be answered by the third parties as part of the experiment proposal (initial DMP) and a final, more detailed version (final DMP). As indicated in the table, some questions are mandatory (marked with M) and others optional (marked with O) for both versions of the DMP.

Sect.	DMP Category and Question	Initial DMP	Final DMP	Guidelines
0 Experiment information				
	Name of the experiment	M	M	Include details
	Experimenter's organisation	M	M	Include details
	Experimenter(s) name(s)	M	M	Include details
	Open Call ID	M	M	Include details
	Experiment start date	M	M	Include details
	Experiment end date	M	M	Include details
	Testbed used	M	M	Include details
	SPIRIT Mentor(s)	M	M	Include details
1 Data Summary				
	Will you re-use any existing data and what will you re-use it for?	M	M	State the reasons if re-use of any existing data has been considered but discarded. If any external data is anticipated before the experiment starts, state it here. If any external data has been used during an experiment, it must be stated, along with any license terms or stipulations.

Funded by the Horizon Europe Framework Programme of the European Union

	What types and formats of data will the project generate or re-use?	M	M	Initially this can be an estimate. In the final DMP this should be a statement of the formats, so it can go into the metadata
	What is the purpose of the data generation or re-use and its relation to the objectives of the project?	M	M	This should be the abstract of experiment from proposal including objectives of collecting the experiment data
	What is the expected size of the data that you intend to generate or re-use?	O	M	Initially this can be an estimate. In the final DMP this should be the actual size of the data.
	What is the origin/provenance of the data, either generated or re-used?	M	M	This is the expected source of the data before the experiment runs, and the actual source of data once the experiment is complete.
	To whom might your data be useful ('data utility'), outside your project?	O	O	If there are any expected users of the data, state them.
2. FAIR data				
2.1 Making data findable, including provisions for metadata				
	Will data be identified by a persistent identifier?	M	M	Initially, this should be a statement committing that the experiment data will be discoverable. When the experiment is complete, the experiment data's Digital Object Identifier (DOI) and metadata should be cited
	Will rich metadata be provided to allow discovery?	M	M	Include details
	What metadata will be created? In case metadata standards do not exist in your discipline, please outline what type of metadata will be created and how.	M	M	Initially, this should be citations of the metadata schemas that are planned to be used, with indications of what will go into the fields (e.g. the title of the experiment etc). After the experiment, this should be a citation to the actual metadata used for the data.
	What disciplinary or general standards will be followed?	M	M	Include details
	Will search keywords be provided in the metadata to optimize the possibility for discovery and then potential re-use?	M	M	This should always be YES - there will be or are keywords for search terms. The keywords should be stated here.
	Will metadata be offered in such a way that it can be harvested and indexed?	M	M	This should always be YES

Funded by the Horizon Europe Framework Programme of the European Union

2.2. Making data accessible				
	Repository: Will the data be deposited in a trusted repository?	M	M	include or cite the repository
	Repository: Have you explored appropriate arrangements with the identified repository where your data will be deposited?	M	M	Cite the documentation
	Repository: Does the repository ensure that the data is assigned an identifier?	M	M	Include details
	Repository: Will the repository resolve the identifier to a digital object?	M	M	Include details
	Data: Will all data be made openly available?	M	M	If certain datasets cannot be shared (or need to be shared under restricted access conditions), explain why, clearly separating legal and contractual reasons from intentional restrictions.
	Data: If an embargo is applied to give time to publish or seek protection of the intellectual property (e.g. patents), specify why and how long this will apply, bearing in mind that research data should be made available as soon as possible.	M	M	Include details
	Data: Will the data be accessible through a free and standardized access protocol?	M	M	Include details
	Data: If there are restrictions on use, how will access be provided to the data, both during and after the end of the project?	N/A	N/A	The default position of SPIRIT is that data should be open, not restricted, so this should not apply
	Data: How will the identity of the person accessing the data be ascertained?	N/A	N/A	This is the responsibility of the repository.
	Data: Is there a need for a data access committee (e.g. to evaluate/approve access requests to personal/sensitive data)?	N/A	N/A	SPIRIT will not have a Data access committee
	Metadata: Will metadata be made openly available and licenced under a public domain dedication CC0? If not, please clarify why. Will	M	M	Include details

Funded by the Horizon Europe Framework Programme of the European Union

	metadata contain information to enable the user to access the data?			
	Metadata: How long will the data remain available and findable?	M	M	Include details
	Metadata: Will metadata be guaranteed to remain available after data is no longer available?	M	M	Include details
	Metadata: Will documentation or reference about any software be needed to access or read the data be included?	M	M	Include details
	Metadata: Will it be possible to include the relevant software (e.g. in open source code)?	M	M	Include details
2.3 Making data interoperable				
	What data and metadata vocabularies, standards, formats or methodologies will you follow to make your data interoperable to allow data exchange and re-use within and across disciplines?	M	M	Initially, include a statement of the formats intended for the data, together with citations of their definitions if applicable
	Will you follow community-endorsed interoperability best practices? Which ones?	M	M	Include details
	In case it is unavoidable that you use uncommon or generate project specific ontologies or vocabularies, will you provide mappings to more commonly used ontologies?	M	M	Description of the mappings, if applicable.
	Will you openly publish the generated ontologies or vocabularies to allow reusing, refining or extending them?	M	M	Include details
	Will your data include qualified references to other data (e.g. other data from your project, or datasets from previous research)?	M	M	Include details
2.4. Increase data re-use				

Funded by the Horizon Europe Framework Programme of the European Union

	How will you provide documentation needed to validate data analysis and facilitate data re-use (e.g. readme files with information on methodology, codebooks, data cleaning, analyses, variable definitions, units of measurement, etc.)?	M	M	Initially, this should be a statement of the intended license, which at least must permit open access. Once the experiment is complete, the data must be licensed under terms that permit open access, and the license must be named here
	Will your data be made freely available in the public domain to permit the widest re-use possible? Will your data be licensed using standard reuse licenses?	M	M	Include details
	Will the data produced in the project be useable by third parties, in particular after the end of the project?	M	M	The data should be reusable by third parties.
	Will the provenance of the data be thoroughly documented using the appropriate standards?	M	M	Include details
	Describe all relevant data quality assurance processes.	M	M	Include details
3. Other research output				
	Consider and plan for the management of other research outputs that may be generated or re-used throughout their projects. Such outputs can be either digital (e.g. software, workflows, protocols, models, etc.) or physical (e.g. new materials, antibodies, reagents, samples, etc.).	M	M	Include details
	Consider which of the questions pertaining to FAIR data above, can apply to the management of other research outputs, and should strive to provide sufficient detail on how their research outputs will be managed and shared, or made available for re-use, in line with the FAIR principles.	M	M	Include details
4. Allocation of resources				
	What will the costs be for making data or other research outputs FAIR in your project (e.g. direct	M	M	The experimenter can claim additional costs for opening data over and above

Funded by the Horizon Europe Framework Programme of the European Union

	and indirect costs related to storage, archiving, re-use, security, etc.) ?			their experiment budget, up to a specified limit. In order to claim the costs, the experimenter must provide an indication in the initial DMP and the actual costs in the Final DMP.
	How will these be covered?	M	M	Note that costs related to research data/output management are eligible as part of the Horizon Europe grant (if compliant with the Grant Agreement conditions)
	Who will be responsible for data management in your project?	M	M	The person responsible for the data management should be named in both the initial and final DMP.
	How will long term preservation be ensured?	O	O	This is the responsibility of the repository. The repository should provide a long-term data retention policy that describes how long data is kept for, as well as any notification procedures for disposal.
	Discuss the necessary resources to accomplish this (costs and potential value, who decides and how, what data will be kept and for how long)?	O	O	Addressed in the above question.
5. Data security				
	What provisions are or will be in place for data security (including data recovery as well as secure storage/archiving and transfer of sensitive data)?	N/A	N/A	This is the responsibility of the repository. The experimenter may base their choice of repository on its reputation and any guarantees a repository provides regarding security and integrity.
	Will the data be safely stored in trusted repositories for long term preservation and curation?	N/A	N/A	This is the responsibility of the repository.
	A qualified reference is a cross-reference that explains its intent.	O	O	1 For example, X is regulator of Y is a much more qualified reference than X is associated with Y, or X see also Y. The goal therefore is to create as many meaningful links as possible between (meta)data resources to enrich the contextual knowledge about the data.
6. Ethics				
	Are there, or could there be, any ethics or legal issues that can have an impact on data sharing?	M	M	Legal, ethical and data protection issues must to be described in the initial DMP that forms part of the experimenter's proposal before the experiment runs, together with procedures for correct compliance with

Funded by the Horizon Europe Framework Programme of the European Union

				the applicable laws including the implications of storing the data for the long term in an open repository.
	Will informed consent for data sharing and long term preservation be included in questionnaires dealing with personal data?	M	M	The experimenter must specify methods for acquiring informed consent in their initial DMP.
7. Other issues				
	Do you, or will you, make use of other national/ funder/ sectorial/ departmental procedures for data management? If yes, which ones?	M	M	list and briefly describe them?

Funded by the Horizon Europe Framework Programme of the European Union

4 CONCLUSION

The partners' formal approval and release of this deliverable within the consortium signify a binding commitment to abide by the data management strategy and the procedures outlined therein.

The Data Management Plan is a dynamic document that will grow and adapt throughout the project's progression as new insights and considerations arise regarding data collection, generation, and handling. Updates to the DMP will be included in the project reports to ensure stakeholders are informed. At the project end an updated and expanded version of the DMP will be prepared to accurately reflect the project's data management status.

Funded by the Horizon Europe Framework Programme of the European Union

REFERENCES

[1] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [Online] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN

[2] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [Online] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&qid=1677247286030&from=EN

[3] European Parliament, the Council and the Commission. Charter of Fundamental Rights of the European Union 20212/C326/02 [Online] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN

[4] Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information. [Online] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015D0444&from=EN

[5] European Commission. Guidelines on FAIR Data Management in Horizon 2020. [Online] https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf

[6] OpenAIRE. European Open Science Infrastructure, for open scholarly and scientific communication. [Online] https://www.openaire.eu/

[7] Zenodo. Open-access repository. CERN. OpenAIRE. [Online] https://zenodo.org/

Funded by the Horizon Europe Framework Programme of the European Union