i-STENTORE

innovative Energy Storage TEchnologies TOwards increased Renewables integration and Efficient Operation

D1.3 DATAMANAGEMENT PLAN

30 June 2023

Co-funded by the European Union

Grant Agreement No.	101096787
Project Acronym/Name	i-STENTORE: innovative Energy Storage TEchnologies TOwards increased Renewables integration and Efficient Operation
Topic	HORIZON-CL5-2022-D3-01-11
Type of action	HORIZON-IA
Service	CINEA/C/02
Duration	36 months (starting date 1 January 2023)
Deliverable title	Data Management Plan
Deliverable number	D1.3
Deliverable version	1.0
Contractual date of delivery	30 June 2023
Actual date of delivery	30 June 2023
Nature of deliverable	DMP
Dissemination level	Public
Work Package	WP1
Deliverable lead	ED
Author(s)	Ioannis Mandourarakis (ED), Nikos Bilidis (ED)

Abstract	This Deliverable will summarize the Data management and IPR protection procedures that will be followed during the course of the project. It will provide the analysis of the Data management policy and the Data management lifecycle for the datasets that will be collected, processed or generated by the project.
Keywords	Data Management, Privacy, Security, IPR, Protection, datasets

CONTRIBUTORS

Ioannis Mandurarakis	ED
Nikos Bilidis	ED
Name	Organization

PEER REVIEWERS

Pedro Rodriguez	LIST
Vaggelis Marinakis	NTUA

REVISION HISTORY

TABLE OF ABBREVIATIONS AND ACRONYMS

API	Application Programming Interface
CA	Consortium Agreement
DB	Database
DMP	Data Management Plan
DOI	Digital Object Identifier
DPIA	Data Protection Impact Assessment
EC	European Commission
EU	European Union
ESS	Energy Storage System
FAIR	Findable, Accessible, Interoperable, Re-usable
GA	Grant Agreement
GDPR	General Data Protection Regulation
HESS	Hybrid Energy Storage System
IDS	International Dataspaces
IoT	Internet of Things
IPR	Intellectual Property Rights
OA	Open Access
PDF	Portable Document Format
RA	Reference Architecture
RES	Renewable Energy Source

SGAM	Smart Grid Architecture Model
SLA	Service Level Agreement
WP	Work Package

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

A quite significant challenge to be tackled in Research and Innovation projects is Data Management, i.e., the practice of collecting, storing, organizing, sharing and maintaining data through structured procedures and an efficient, planned manner, to enhance accessibility, performance and timeliness.
The work presented in the current document is part of i-STENTORE's Work Package 1 (WP1) Task 1.4 "Ethics, exchange requirements specifications and Data Management", provided as deliverable D1.3, which summarizes the Data Management and IPR protection procedures to be followed during the course of the project. It provides the analysis of the respective policies and the data management lifecycle for the datasets to be collected, processed or generated by the project.
The Data Management Plan (DMP) is a document that serves as an important project output since it provides the necessary details regarding i-STENTORE's data gathering and/or generation, storage, meta-processing and sharing, during the project and afterwards. It follows the Horizon Europe Guidelines in F.A.I.R. (Findable, Accessible, Interoperable, Re-usable) Data Management and has used the European Commission's DMP template as a guideline. The DMP is expected to be regularly updated over the project's course, given that significant changes have arisen, such as (but not limited to) new data regulations and/or changes in the consortium policies (e.g., the realm of data sharing, de-identification, back-tracing or anonymization).
All data will be produced from available information, from activities and from project's trusted partners, from external evaluators and various third-party beneficiaries covering various use cases. The given plan aims to outline a comprehensive strategy for the production and handling of all data and project-related documentation.
Datasets will be anonymised for impact assessment and research purposes. All the personal data will be treated in line with the REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 and it will be accessible for authorised users only (validated via authentication processes).

1 INTRODUCTION

Research and innovation projects such as i-STENTORE can potentially produce a plethora of data, and in some cases voluminous information to be exchanged. As to the origin of the data, it is mostly based on the given field of study which, particularly for i-STENORE, can stem from laboratory tests, to simulations, to field research and scientific investigations/observations. The collaborators of i-STENTORE will be contributing to an array of important information, including open datasets, open-source coding, scientific publications and/or white-papers, anonymized survey results and more, via Open Access (OA) channels. This is why it is crucial to underline at this point that each member of the respective consortium needs to actively maintain an equilibrium between openly publishing information and findings related to the project and to safeguard any sensitive data, abiding to the GDPR regulations and understanding that any mishandling could potentially lead to legal implications.

1.1 DATA PROTECTION LEGISLATIVE FRAMEWORK

The i-STENTORE consortium is fully aware of the ethical implications of the proposed research and respects the ethical rules and standards of Horizon Europe, and those reflected in the Charter of Fundamental Rights of the European Union. Where necessary, the i-STENTORE consortium confirms its abidance to national and international laws including Regulation (EU) 2016/679[1] of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, the Directive on Privacy and Electronic Communications (2002/58/EC)[2], Directive on Protection of Privacy in the Telecommunication Sector (97/66/EC)[3], The Universal Declaration of Human Rights[4] and the Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data[5]. Article 19 "Ethical principles" of Regulation No. 1291/2013/EC of the European Parliament[6] and of the Council which states the fundamental principles of the Horizon Europe Ethics in research.

1.2 DELIVERABLE PURPOSE

A DMP should be considered a record which provides an illustration of the research data handling throughout the duration of a project, starting from its inception to its completion. According to this, over its three-year span the i-STENTORE project will produce a series of outcomes to further deployment. More specifically, the threefold purpose of this DMP is a)

[1] https://eur-lex.europa.eu/eli/reg/2016/679/oj
[2] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058
[3] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31997L0066
[4] https://www.un.org/en/about-us/universal-declaration-of-human-rights
[5] https://www.coe.int/en/web/data-protection/convention108-and-protocol
[6] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:347:0104:0173:EN:PDF

to describe the standards that ensure the proper encapsulating, editing, redrafting, preserving and distributing (for reuse of verification purposes) of the various datasets, b) to describe the means and methods that adhere to determining, categorizing (public or classified), organizing, curating, storing and disseminating the data to be created, processed and amassed, and c) to guarantee that the aforementioned actions can conform to any current or future ethical and legal stipulations.

1.3 TARGET AUDIENCE

The target audience for this deliverable is:

- Partners and Advisory Group in the i-STENTORE project
- European Commission
- EU Parliament
- Other Horizon Europe or energy related projects (clustering activities)
- Organisations and experts involved in the i-STENTORE case studies
- Other relevant organisations (both public and private), including associations of relevant stakeholders

1.4 STRUCTURE OF THE DOCUMENT

This deliverable is structured as follows:

- **Section 1** provides the introduction of the deliverable.
- **Section 2** presents the i-STENTORE data management strategy and relevant procedures (including open access, interoperability, data re-usability, and in more detail the definitions about the purpose of data collection, the types and formats of collected and generated data, the vocabulary use and terminology and the quality assurance process).
- **Section 3** analyses matters related to data classification, archiving, performance, protection and security.
- **Section 4** discusses about the Data Management Implementation
- **Section 5** discusses about the FAIR data principles.
- **Section 6** mentions the mediums of archiving and channels of communication/dissemination.
- **Section 7** covers the allocation of resources.
- **Section 8** discusses on privacy, IPR and data security.
- **Section 9** presents specific ethical aspects of the project
- **Section 10** provides the summary and conclusions of the deliverable.

2 DATA MANAGEMENT STRATEGY AND PROCEDURES

As already mentioned, a DMP defines the data management lifecycle for the information to be generated, collected, processed, stored and shared in a Horizon Europe project. In order for a DMP to make research data findable, accessible, interoperable and reusable, it needs to contain various details about the data management during (and after) the project. All the respective considerations relate to:

- the identification of the data types to be created, processed and/or generated, the owners of the respective procedures and the roles and groups of entities that will find this data useful,
- the identification of the methodologies and standards to be utilized,
- the metadata specifications that will render the data traceable and comprehensible,
- clarifying measures in regards to access and sharing of the data,
- outlining the ways that the data will be conserved, including provision after the project's completion,
- the indications regarding the archiving and preservation of the project's open datasets.

Table 1 that follows focuses in clarifying a series of important fixed terms.

TABLE 1: CLARIFICATIONS OF TERMS

Research data	Research data shapes the bedrock of all research results (excluding the ones exclusively theoretical), encompassing the data to be collected and/or observed and/or generated and/or acquired mainly from commercial, governmental and other entities. This data undergoes extensive analysis and synthesis in order to generate the anticipated novel research outcomes, which, subsequently will form the basis for research papers, and finally, submitted to various academic channels for publication.
Open research data	Openly accessible research data can typically be managed (i.e., to be accessed, and/or exploited and/or reproduced and/or disseminated), free of charge.
Secondary data	Secondary data are data that already exist, as a result of some primary gathering or processing (metadata), which was conducted regardless of the research to be conducted.
Open access	Open access is defined as the principle that research information must be accessible to relevant users, on equal terms, and at the lowest possible cost. Access must be easy, user-friendly and, if possible, internet-based.
Metadata	Metadata is data used to describe other data. It summarizes basic information about data, which can make finding and working with instances of data easier. An example of metadata is any calculation results from big sets of data, like statistical results, citing data, sums, medians, aggregated information, inferred conclusions, etc.

Research data repositories	Research data repositories are defined as online archives (digital data storage platforms) for preserving (and sharing) research data. Such information can be subject based and/or thematic, institutional or centralised.

2.1 DATA SUMMARY

In compliance with the Guidelines on FAIR Data Management in Horizon Europe, a DMP plays a crucial role in guaranteeing effective data management. Hence, it is important to address the kinds of data expected to be produced during the project:

1) **Data derived from readily available sources** like industry reports on pertinent topics in the power sector and industry evolutions or other subjects relevant to the project's objectives.
2) **Data resulting from activities carried out by project partners and external evaluators**, including evaluation reports, surveys, review documents, focus group discussions, priority setting for the project, technical data processing, business process development, among other tasks executed to reach the project's targets.
3) **Data created involving third-party beneficiaries and use cases**, such as specifics of projects submitted under any circumstances, interview records, and presentations.

2.1.1 State of Purpose of the Data Collection / Generation

The i-STENTORE project will accumulate data from a variety of sources, which include project partners, stakeholders, and various other external contributors. The related data activities such as the collection, the storage, and the processing of information submitted by all project applicants is considered crucial.
The data, in all formats, will be utilized for three primary objectives:

- To assess deliverables and proposals,
- To evaluate impact, and
- To conduct meaningful (academic and business) research.

2.1.2 Types and Formats of Data Generated / Collected

Furthermore, a central aspect of the DMP involves outlining the nature of Open Access[7] (OA) that will be provided for the data. OA pertains to the strategy of offering (online) access to academic content that is free for the user and can be reused. 'Scientific' encompasses all academic fields. When applied to research and innovation, 'Scientific information' can refer to:

[7] Guidelines to the Rules on Open Access to Scientific Publications and Open Access to Research Data in Horizon 2020, https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-data-management/data-management_en.htm

- Peer-reviewed academic research articles (published in academic journals), or
- Research data (data that underpins publications, managed data, and/or raw data).

Open Access to scientific publications denotes free online access for any potential reader/user.
The two main paths to OA include:

- Self-archiving or 'green' OA – the author or a proxy stores (deposits) the published article or the final peer-reviewed manuscript in an online repository before, at the same time as, or after publication. In some cases, some publishers may require an embargo period before OA is permitted.
- OA publishing or 'gold' OA - an article is instantly published in an OA format. In this specific model, the cost of publication is transferred away from subscribing readers. The most typical business model involves one-time payments by the respective authors.

Research data denotes information, notably facts or figures, gathered for analysis and used as a basis for reasoning, discussion, inferring or calculation. In a research setting, data can include various statistics, a plethora of experiment results, interdisciplinary measurements, multiple fieldwork observations, online or offline survey results and/or interview recordings, and images. The main emphasis is shed upon research data that exists in a digital format. The users can typically access and/or mine and/or utilize and/or reproduce and/or share/disseminate openly accessible research data without charge. Figure 1 illustrates the process flow for defining the OA type in academic publications and research data. The OA mandate comprises two steps, a) depositing publications in repositories and b) providing OA to them.

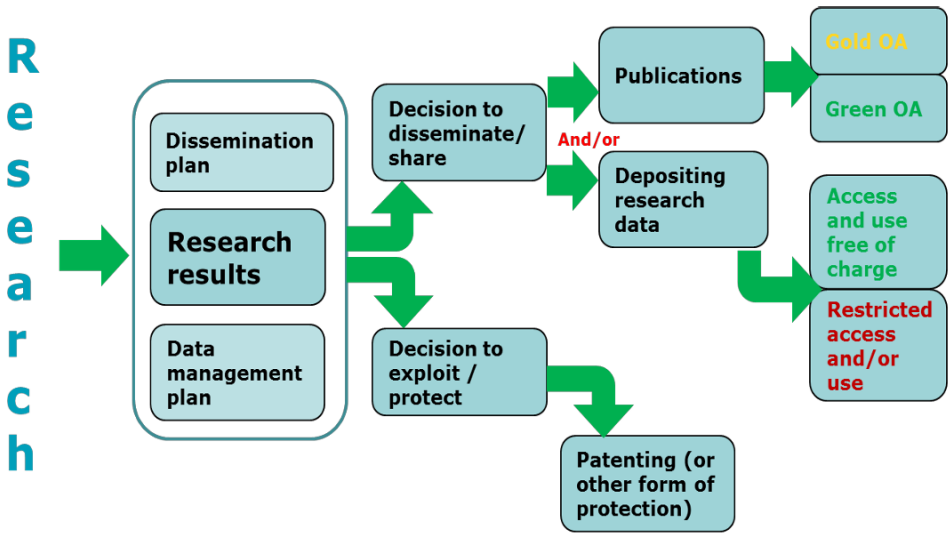

FIGURE 1: OPEN ACCESS STRATEGY FOR PUBLICATIONS AND RESEARCH DATA[8]

i-STENTORE is expected to generate, and process a variety of data. All generated data will be stored in an easily accessible way by both humans and software, as appropriate. To offer

[8] https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-pilot-guide_en.pdf

a comprehensive snapshot of the different data sets that are presently being generated and will be produced in the i-STENTORE project, the subsequent table depicts the type of data, the data's origin, the associated work package number, and the expected format for data storage. Table 2 that follows presents the dataset overview, focusing on the data types, origin, format and respective work package for the expected data.

TABLE 2: DATASET OVERVIEW

#	Data type	Origin	WP#	Format (indicative)
1	Stakeholder contacts collection	Publicly available data	1,2,3,6	.xls, .pdf
2	Quantitative survey data	Primary Data	2,5	.xls, .csv, .txt, .pdf
3	Expert interview data	Primary Data	1,5,6	.xls, .csv, .txt, .pdf
4	Demo generated data	Primary Data	4,5,6	.xls, .txt, .doc, .csv, .pdf
5	Workshops data	Primary Data	3,4,6	.doc, .xls, .pdf
6	Validation cycles data	Primary Data	3,4,5,6	.xls, .csv

2.1.3 Vocabulary Use

The vocabulary used in the project is a very standard and common language within the business creation culture and the logistics. Vocabulary won't represent any barrier for data interoperability and re-use.

2.1.4 Third parties use of Data

Third parties to the project will be the external evaluators.
Both previously defined categories are for the purposes of the Open Call.
The plan is to permit external evaluators to access a limited selection of records from the data set during the evaluation stage. Before they are given access to the data, these evaluators will be required to sign an *'Experts Evaluators Code of Conduct'*, *'External Evaluation Fundamentals'*, and a *'Declaration of confidentiality and no conflict of interest'*. This access will be provided online for a specified time duration, with secure authentication protocols in place.

2.1.5 Data Quality Assurance Process

The principle of data quality stipulates that all information must be **precise** and **current**. This means that the processing of personal data will adhere to EU, national, and international legislation, incorporating the "data quality" principles outlined below:

- Processing of data should be sufficient, pertinent, and not superfluous.
- Data must be precise and continually updated.
- Data should be processed in a fair and lawful manner.
- Data should be processed respecting the rights of the data subjects.
- Processing of data should be performed securely.
- Data should be retained only as long as necessary for the sole purpose of the project.

The data quality assurance process will be led in accordance with the REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

2.1.6 Expected Data Volume (if known)

The anticipated outcomes of the research will include the creation of research datasets (such as the results of technologies, demo services, etc.), publications, suggestions for new services through the Open Call, dissemination materials, and more. However, due to the substantial scale of the project, the breadth of its work, and its complexity, it is currently impossible to accurately estimate the expected size.

2.2 DATA RE-USABILITY

Data will be promptly disclosed and posted on the project's website or other storage spaces, such as ProofHub (mostly focused on collaboration purposes), the research data online repository (Zenodo) i-STENTORE's code repository and the project communication channels. Everyone will have access rights, enabling them to duplicate, share, or modify (by remixing, transforming, or building upon the existing material) the data.

2.2.1 Re-use of existing data

The project involves consistent data collection throughout its duration, but **it doesn't include the utilization or integration of previously amassed research or personal data**. Furthermore, it is not projected to share data with non-EU members who aren't part of the consortium.

2.2.2 Increasing data re-use through clarifying licences

2.2.2.1 Open Science: Open Access to Scientific Publicaitons

Project beneficiaries are obligated to provide open access to peer-reviewed scientific papers linked to their results. This specifically involves ensuring that:

- A machine-readable digital version of the published work or the final peer-reviewed manuscript accepted for publication is deposited in a reliable scientific publication repository no later than the publication date.
- The publication deposited in the repository is immediately available with open access, under the most recent version of the Creative Commons Attribution International Public Licence (**CC BY**) **or a license offering similar rights**; for monographs and other long-text formats, the license may exclude commercial use and derivative works (**such as CC BY-NC, CC BY-ND**).
- Any information regarding research outputs or any other tools and instruments required to verify the scientific publication's conclusions is provided via the repository.

Beneficiaries (or authors) must maintain enough intellectual property rights to fulfill the open access requirements.
The metadata of the deposited publications must be made open under a Creative Common Public Domain Dedication **(CC 0) or an equivalent**, conforming to the FAIR principles (especially being machine-actionable), and must provide at minimum, information about the following: publication (author(s), title, date of publication, publication venue); Horizon Europe or Euratom funding; grant project name, acronym, and number; licensing terms; persistent identifiers for the publication, the authors involved in the action and, if possible, for their organizations and the grant. If applicable, the metadata must include persistent identifiers for any research output or any other tools and instruments required to validate the publication's conclusions.
Only full open publication fees are applicable.

2.2.2.2 Open Science: Research Data Management

As soon as feasibly possible and within the deadlines outlined in the DMP, the data must be deposited in a trusted repository. If required by the call conditions, this repository must be part of the European Open-Source Cloud Portal[9] (EOSC) and adhere to EOSC requirements. Beneficiaries are also expected to ensure open access, via the repository, to the deposited data as soon as possible. This is to be achieved under the most recent version of the Creative Commons Attribution International Public License **(CC BY)** or Creative Commons Public Domain Dedication **(CC 0**) or an equivalent license, while adhering to the principle of 'as open as possible as closed as necessary'.

[9] https://eosc-portal.eu/

However, open access to some or all data might not be provided if it conflicts with the beneficiary's legitimate interests, including commercial exploitation, EU competitive interests, or any obligations under the Grant Agreement (GA). Any such instances must be justified in the DMP. Information regarding any research output or other tools required to reuse or validate the data should also be provided via the repository. Furthermore, metadata of the deposited data must be open under a Creative Commons Public Domain Dedication **(CC 0) or equivalent**, while safeguarding legitimate interests or constraints and aligning with the FAIR principles, particularly being machine-actionable. The metadata should provide information about datasets, Horizon Europe or Euratom funding, grant project name, acronym, and number, licensing terms, and persistent identifiers for the dataset, authors involved in the action, and, if possible, for their organizations and the grant. When applicable, the metadata must include persistent identifiers for related publications and other research outputs.

2.2.2.3 Open Science: Additional Practices

Should the call conditions necessitate extra obligations concerning open science practices, the beneficiaries are required to comply with these stipulations. In situations where additional duties are imposed by the call conditions regarding the validation of scientific publications, beneficiaries must provide access, digital or physical, to data or other results required for validating the conclusions of scientific publications. This should be done while protecting their legitimate interests or constraints, unless they have already provided (open) access at the time of publication.
If the call conditions dictate additional open science obligations during a public emergency, beneficiaries, upon request by the granting authority, must promptly deposit any research output in a repository and provide open access to it **under a CC BY license, a Public Domain Dedication (CC 0), or an equivalent**. However, if providing access would contradict the beneficiaries' legitimate interests, they are expected to grant non-exclusive licenses under fair and reasonable conditions to legal entities needing the research output to address the public emergency. These beneficiaries must also commit to rapidly and widely exploiting the resulting products and services at fair and reasonable conditions. This provision is applicable up to four (4) years following the end of the action.

2.2.3 Data re-usability time-length

The Consortium is committed to keeping the data usable for as long as feasible following the project's completion. An initial duration of five (5) years has been set; nonetheless, this period could be extended with the agreement of the partners.

2.3 DATA SOURCES AND ACQUISITION

The data that will be gathered in the frame of the i-STENTORE project comprise both publicly accessible data and internal (operational data), which are mostly generated and collected by the partner entities, including information of pilot and research organisations.
The main data sources for the i-STENTORE project include:

- Data being sourced from various documents, such as:
  - Inputs emergent from surveys conducted with stakeholders that participate in the pilots, during the requirement gathering and the validation of the i-STENTORE solution.
- Operational data created during the execution of the project:
  - Public and Open data, including energy usage, weather conditions, ESI data collected via sensor monitoring, etc.
  - Internal data related to the pilots, including energy monitoring data, network data, demand response data, smart meter readings, storage plant production data and any data that capitalize the storage assets, among others.
  - User data from various terminals and applications, SCADA, storage-centric information, user consumption profiles, system descriptions, which will be further analysed and detailed to the extent required by the project's specifications.
  - Data from i-STENTORE dissemination, promotion and branding activities (e.g., website traffic, visitors and other website analytics, webinars participants), and so forth.

3 DATA MANAGEMENT REQUIREMENTS

The process of managing data in the i-STENTORE project is construed as a strategic method applicable to each outcome generated or gathered throughout the project's lifespan. This method stipulates provisions for various data management dimensions such as data categorization, data storage, data performance, data protection and security, adherence to FAIR data management principles, and data ethics.

3.1 DATA CLASSIFICATION

For apt data handling, datasets must be initially segmented into public and non-public categories. The classification of these diverse datasets can be done by addressing the following queries:

1. **Does an outcome deliver considerable value to others or is it required to comprehend a scientific conclusion?**
   A positive answer to this query classifies the result as public (qualified for open access). A negative response categorizes the result as non-public. For instance, code specifically tailored to the i-STENTORE platform (like database initialization) typically lacks scientific interest for others and does not make any significant contribution.

2. **Does an outcome encompass personal data that goes beyond the author's name?**
   An affirmative answer to this question classifies the result as non-public. Personal data, excluding the name, must be expunged if it is to be published in accordance with the project's ethical guidelines.
3. **Can an outcome enable the recognition of individuals even in the absence of their names?**
   This step is also supervised by the project's legal/ethical framework, as we pledged in the i-STENTORE project to deploy encryption techniques and securely store personal data. Datasets will be anonymized for research and impact assessment purposes. The collection of personal data within the project will be minimal and will require the informed consent of participants regarding the use of their personal data. Personal identities will be safeguarded via anonymous codes. A positive answer to this question classifies the result as non-public.
4. **Can an outcome be misused for a purpose that is generally undesirable to society or contravenes societal norms and the project's ethics?**
   A positive answer to this question classifies the result as non-public.
5. **Does an outcome involve one or more project partners' business or trade secrets?**
   An affirmative answer to this question classifies the result as non-public. Any business or trade secrets must be excised in line with all partners' stipulations before it can be published.
6. **Does an outcome mention technology that is part of an ongoing, project-related patent application?**
   An affirmative answer to this query classifies the result as non-public. Naturally, results may be published once the patent application is submitted.
7. **Does an outcome compromise any project partner's security interests?**
   A positive answer to this question classifies the result as non-public.

This is a straightforward method to determine the different types of data outlined in the DMP. The obligations of the i-STENTORE consortium partners regarding the dissemination of project results are explained in the respective section.

3.2 DATA ARCHIVING REQUIREMENTS

As the technical solution for i-STENTORE evolves and matures, an increasing volume of data will be incorporated into the platform. This data could encompass information of public interest (for example, weather data), operational data obtained from smart meters at pilot sites, or consumer/demand data from existing or newly enrolled entities. For the initial two categories, the data will be integrated into the system at significantly high rates, which will lead to a considerable amount of data. Conversely, such data tends to be highly valuable when it is recently acquired for the creation of real-time services, while after a brief period post-integration, it is primarily used for static analysis and batch-processing analytics. Furthermore, the likelihood of updating such data is minimal, especially after several days.
This kind of data will be made accessible (read-only permissions) in batches to users, provided they are authorized to access it. The access to data will be managed through an

identity management component. This component ensures a user's authentication to i-STENTORE and permits access to the requested resources only if the access policies for these resources align with the request. Naturally, the data owners will establish the access policies for each dataset.
In terms of any potential personal data keeping, if needed it will be stored for a certain duration before being deleted. The collection of personal data within the project will be limited to the submission phase, and participants' informed consent for the use of their data will be obligatory. Personal identities will be shielded through the use of anonymous codes. The linkage between real names and codes will only be accessible to project partners who will store the records securely.
Later in the project timeline, the consortium will consider the possibility of anonymising some data post-project for further research purposes. Consequently, if personal data collection is involved in the project, i-STENTORE will develop two distinct consent forms: one for data collection activities during the pilot demonstrations, and another for the period following the project. The latter consent form aims to secure the data owners' consent to anonymise the data they provide, making them accessible for future research purposes (which will be explicitly detailed in the consent form).

3.3 DATA PERFORMANCE

As previously mentioned in Section 2.1, i-STENTORE will handle a vast amount of diverse data derived from various sources and providers. The consistent availability of this data is a vital factor, which may bring about high computational and performance demands.
The full i-STENTORE framework will be installed at the pilot sites in controlled settings, distinct from 'production' environments. It will employ a dedicated data processing infrastructure designed for experimental purposes, managing large volumes of historic and real-time data, potentially anonymised or simulated. This approach reduces the reliance on the computational resources of an integrated system, shifting the data processing and analysis computational load to the pilot sites.
Moreover, the i-STENTORE platform is designed with an architecture that separately addresses each stage of the data flow within the platform, namely data interoperability and standardisation, data streaming, and data storage.
i-STENTORE will accumulate a wealth of data from various sources, including IoT and other sensors, historical records, pilot sites' private databases, public databases' open data, survey and questionnaire data, among others. Regarding data interoperability and standardisation of IoT and sensor data, captured data will be converted by IoT and System adapters into NGSI (Next Generation Service Interfaces) data models and stored in the FIWARE Data Broker[10]. This stage will handle data standardisation, utilizing community smart data models as much as possible. As a result, the architecture's upper layers, where processing occurs, comprise existing or newly developed software tools reusable by the community, promoting

[10] https://www.fiware.org/about-us/

industry standardisation. The upper layer will include components for monitoring, simulation, task scheduling, reasoning, analytics, and optimization engines. Each service can access specific data relevant to its purpose and can send back processed data to the unified data collection system. Data sovereignty rules will apply to the data collected from all layers to the data broker. Each data consumer will be individually granted or denied access permissions. Compliant with industry security standards, authorization components will be employed.

3.4 DATA PROTECTION AND SECURITY

Processing of personal data will follow the REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and until valid, the repealing Directive 95/46/EC (General Data Protection Regulation - GDPR).
As a result of the Data Protection Impact Assessment (DPIA), stipulated in Article 35 (1) of the GDPR, necessary organisational and technical strategies will be deployed to ensure the security of personal data. This includes methods such as anonymisation, pseudonymisation, encryption during storage and transmission, hashing, tokenization, and the use of key management practices to protect data across all applications and platforms. The personal data collected as part of the project will be strictly confined to the project's objectives, and participants' informed consent for data use will be mandatory.
Work package 1 (Tasks 1.3 1.4) of the i-STENTORE project is centred on upholding the ethical norms that are integral to the project's goals, methods, procedures, tasks, and results. These ethical standards are predominantly associated with personal data handling and, therefore, data protection. For this reason, this document will not explore the specifics related to data protection procedures.
Operational data that is internally gathered or produced by partners during the entire project duration will be stored in data repositories located on each partner's individual servers. These servers will be securely housed in locked rooms, with stringent access controls in compliance with relevant security standards, and they will employ cutting-edge security measures. Repository access will be exclusively provided to authorized individuals at both the physical and network levels. If datasets are contained within databases, only authorized users with unique usernames and passwords can gain access, adhering to the rules of access privileges. Database backups will be encrypted and retained on the premises of each respective organization. Regular backups of data from devices will be made and stored in devices that adhere to the same security standards and protocols as the primary server.
The transfer of data will adhere to established best practices, which include encrypting files and securely transmitting the corresponding keys or passwords.

Processing of document-based data will be supported via a dedicated platform (ProofHub). According to their privacy policy[11] and security information[12]:

- it employs "*..state of the art technology to maintain high standards of data security and ensure that … communications are secure, and businesses are protected..*",
- "*..all data is encrypted via SSL/TLS when transmitted..*",
- "*..On hourly basis, data gets backed up and copies of the data are saved and secured at an off-site location for disaster recovery*"[13], while "*database backups are encrypted..*",
- "*..items and files deleted are moved to trash from where they are purged after 15 days*" unless we empty the trash manually in which case "*data is purged immediately..*",
- "*..data is saved on reliable servers and written to multiple disks and stored in multiple places to remove even the minutest point of failure..*",
- access to data is granted "*..only to authorized team members..*",

Moreover, ProofHub enables document-based data to be accessible either in a read-only format or downloadable format, thus preventing unauthorized users from accessing the information. Additionally, it supports file versioning[14]. Documents with limited access will be kept in a secured cabinet within the organization's facility.

4 DATA MANAGEMENT IMPLEMENTATION

This section provides an overview of the specific provisions, foreseen for the management of each project dataset and databases (DBs) in table form.

[11] https://www.proofhub.com/privacy
[12] https://www.proofhub.com/security
[13] https://help.proofhub.com/plus/account/security-backup-data/
[14] https://help.proofhub.com/plus/files/file-versioning-2/

TABLE 3: I-STENTORE DATA MANAGEMENT IMPLEMENTATION

Dataset	Classification	Archiving	Safety & Security	FAIR	Privacy & Data protection
Project Public deliverables	Public	Each public deliverable will be published openly on the i-STENTORE webpage (following European Commission review and approval). All earlier versions of it will be archived on the project's internal ProofHub repository.	N/A	Public deliverables uploaded on the project website with the appropriate metadata	N/A
Open-Source Software Components	Public	Software developers will share their code base on their own public repository e.g., GitHub.	N/A	Source code deposited in GitHub or some other type of public repository	N/A
Scientific Publications	Public	• i-STENTORE website • publicly accessible disciplinary repositories (like Zenodo)	N/A	Publications indexed in the project website and the project's dedicated Zenodo with the appropriate metadata	N/A
Pilots' Public Data	Public	Data will be stored in the project DB in two different ways: i) near-real time for data coming from active sensors connected to the platform, and ii) in asynchronous mode for data coming from different pilots' sources such as files or historical DBs.	Project DB will be under a private network accessible only to project members and secured under the cloud provider security policy.	Data will be translated to NGSI models and stored in the FIWARE Data Broker.	Potential anonymisation (suppression, generalisation, etc).
Pilots' Private Data	Confidential	Data will be stored in each pilot partner database (on premises)	Individual security mechanisms and policies of each beneficiary.	N/A	N/A

5 FAIR DATA

Specifically for Horizon Europe projects a FAIR DMP template[15] has been designed to be applicable to any project of that nature (refer to Annex A). The FAIR data principles aimed at swiftly disseminating the data outcomes of a research project[16] are presented in Table 4 that follows.

TABLE 4: DATA MANAGEMENT ACCORDING TO FAIR PRINCIPLES DATA SOURCE AND ACQUISITION

FAIR Data Principles	
Data should be **Findable**	F1. (Meta)data are assigned a globally unique and persistent identifier. F2. Data are described with rich metadata (defined by R1 below). F3. Metadata clearly and explicitly include the identifier of the data they describe. F4. (Meta)data are registered or indexed in a searchable resource.
Data should be **Accessible**	A1. (Meta)data are retrievable by their identifier using a standardised communication 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.
Data should be **Interoperable**	I1. (Meta)data use a formal, accessible, shared, and broadly applicable language for knowledge representation. I2. (Meta)data use vocabularies and definitions that follow FAIR principles. I3. (Meta)data include qualified references to other (meta)data.
Data should be **Reusable**	R1. (Meta)data are richly described with 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 detailed provenance. R1.3. (Meta)data meet domain-relevant community standards.

As mentioned, the FAIR DMP template covers a set of questions that need to be covered with a level of detail appropriate to the project, like done in section 2.3.1. The current document will address all the issues that are proposed by the template, like Data Summary, FAIR data, Allocation of resources, Data protection and security, Ethical aspects, any further support in developing the DMP and other related issues.
The international FAIR Principles have been formulated as a set of guidelines for the reuse of research data. The acronym FAIR stands for findable, accessible, interoperable, and reusable research data.

[15] Guidelines on FAIR Data Management in Horizon 2020, http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf
[16] https://www.go-fair.org/fair-principles/

i-STENTORE Reference Architecture (RA) takes the opportunity to contribute towards the creation of a digital platform acting as a VPP for the intelligent management of Energy Storage assets. The RA will lead the development of the i-STENTORE Digital Platform supporting the effective and trusted sharing of data among participants covering all requirements to support future data marketplaces:
(A) **Data Interoperability**: open source, standardized, and domain agnostic SGAM-based architecture ensures the interoperability of data between different systems.
(B) **Data Sovereignty and Trust**: The IDSA and FIWARE Conceptual Architectures will be leveraged to ensure not only an open-source implementation for technological interoperability but also to enhance trust & sovereignty, data value and governance building blocks, adapting to the specific cases related to Energy Storage (ES) applications and interfacing with legacy equipment.
(C) **Data value creation**: Following a path of standardisation activities Open APIs (based on the industry initiatives and bodies like NGSI-LD and/or Context Information Management API, defined by ETSI ISG CIM) will contribute to extend Context Information Management.
The FIWARE NGSI Marketplace will be used to:

(i) define new data asset types;
(ii) register offerings which typically means providing the description of the asset, the data models, the endpoints, the terms, and conditions of exchanging data including SLAs, legal clauses, and pricing schema;
(iii) enable navigation and search/discover existing offerings based on selected criteria.

All the aforementioned FIWARE functionalities ensure data manipulation in i-STENTORE based on FAIR principles (Findability, Accessibility, Interoperability, and Reusability).

5.1 MAKING DATA FINDABLE

All data management actions, like storage, processing, and mutual sharing of information among project participants will be facilitated via a dedicated platform, ProofHub, while the broader public engagement with the project's findings will be enabled and broadcasted through the official project website. In addition, all data will be archived on the project coordinator's private Dropbox cloud storage for a minimum duration of five (5) years post-project completion, with a possible extension of an additional two (2) years upon request. The same regards confidentiality, record keeping and impact evaluation with five (5) years for each, after the final payment (project end). The Extension of findings from other grants to this grant can extend to no more than two (2) years after the final payment (project end).
The adopted **naming convention** will succinctly detail the content, the data-collecting institution, and the month of publication. **Version control** will be invoked in instances where a participant wishes to withdraw their data; here, a version number will be incorporated into the file name.
The necessary technical steps will be implemented to ensure that data does not reveal the identities of individuals involved, and as such, identifiable data that lead to real names will not be distributed.

i-STENTORE utilizes ES data, related to various activities and collected (or metadata generated) from various sources (primarily monitoring sensors, actuators, and user interactions) throughout the renovation/digitisation intervention period.
As already mentioned, the i-STENTORE data sovereignty module will leverage and augment FIWARE components for data handling and distribution, establishing a data space with open data models, standardized APIs, and workable data sharing policies aligned with FAIR principles.

5.1.1 Discoverability of the Data

Data generated within the scope of i-STENTORE will be rendered traceable and locatable via unique identification protocols. All files will be distinctly identified through the utilization of standardized naming conventions and file versioning procedures. Moreover, any research data generated will be accompanied by metadata annotations, adhering to certain standards like the Dublin Core generic metadata standard[17], with the aim of describing a broad spectrum.
To ensure that i-STENTORE paves a path in alignment with the FAIR data principles, (meta)data will:

- Be associated with a unique and permanent global identifier
- Include comprehensive metadata for complete data interpretation, and
- Be catalogued in a source which serves and honours easy searching.

5.1.2 Data Identification Mechanisms

All documents will carry the project's name, along with a unique, enduring designator for the document type and number, which is provided by the coordinator for submission to the European Commission (EC). The version of the document will be incorporated both into its name and its title.
Each document's identification will encompass the task or deliverable number that corresponds to the document, followed by a succinct title of the activity or deliverable.
i-STENTORE will disseminate data through academic articles as well, in such instances, Digital Object Identifiers (DOIs) will be issued by the publisher. For other forms of written work, like reports and policy recommendations, DOIs will be allocated via the repository where they are archived (for instance, Zenodo).

5.1.3 Naming Conventions

In order to (i) bolster the searchability and discoverability of data, and (ii) offer insights into the content, status, and versioning of files, every produced data set (such as datasets,

[17] https://www.dublincore.org/specifications/dublin-core/dces/

deliverables, etc.) will adhere to a consistent naming protocol and will incorporate a table for version control.
The guidelines for naming project documents will be:

- select identifier names that are succinct yet meaningful,
- avoid using acronyms that are not universally recognized,
- refrain from using abbreviations or shortened forms,
- steer clear of characters that are language-specific or non-alphanumeric,
- append a two-digit numerical suffix to distinguish new versions of a document, and
- include dates in reverse order, using four digits for the year: YYYYMMDD.

For deliverables: **Project's name – Dx.y - [Name of the deliverable as described in the DoA]** being x - work package assigned to the deliverable y - the number of deliverables within the work package i.e.: "D1.3 - Data management plan".
For datasets: **Project's name – WP [Work Package number] P [Pilot number; pilot activity number] - T [Task number; description of the activity]** e.g., "WP2 T2.4 T2.6 – Reference Architecture tailored to an open and modular European energy system for optimized storage technologies use leading to increased flexibility".
i-STENTORE will employ user-friendly search keywords to promote the effective reuse of data by all stakeholders. The metadata standards that i-STENTORE adopts offer the ability to annotate both the data gathered/generated and its substance with keywords.
Typically, the keywords will encompass terms linked to the relevant subject matters, such as the energy efficiency, energy storage, hybrid storage systems, interoperability, innovative business models, electrical engineering, electronic engineering, information engineering, data spaces, equitable energy transition, energy sector capacity, intelligent contracting, energy efficiency policies. Additionally, project-specific keywords, like i-STENTORE, Horizon Europe, various standards, strategic initiatives etc., will also be used. The selected keywords will accurately mirror the content of the datasets and will avoid terms that only appear once or twice within them.

5.1.4 Approach towards Search keywords

Documents related to the activities of the project will be done following the templates agreed by the consortium, these templates include a keywords section to make documents findable.

5.2 OPEN-DATA ACCESSIBILITY

Subject to ethical considerations and participant consent, data will be as accessible as possible. I-STENTORE will employ FIWARE Identity Management through its data sovereignty module, which enables identification, authentication, and authorization of organizations and

individuals. Meanwhile, IDS Connector[18] ensures the exchange of data is trusted. Consequently, the data will be both **attainable** and **reliable**.

As to the scientific data production in the i-STENTORE project this will encompass the advancements regarding: (i) Enhanced learning data models that provide more detailed insights and enable the development of data-driven grid-supporting services. These services will leverage the vast amount of available and reusable energy storage assets, ensuring interoperability for network operators. (ii) Adoption of state-of-the-art storage technologies and innovative combinations in Hybrid Energy Storage Systems (HESSs). This will be achieved through the implementation of novel control, operation, and management methods and algorithms, resulting in more efficient co-optimization and facilitating increased integration of Renewable Energy Sources (RES) into the grid.

Different levels of dissemination will be applicable to i-STENTORE reports. Public reports will be disseminated via public platforms, whereas confidential reports will only be shared within the consortium. Scientific publications will be freely accessible and will be uploaded to public repositories. Partners will share data through a shared space. Some research data, especially those concerning demo users, are sensitive due to privacy and data protection concerns, and will therefore be kept confidential or anonymized before they are made accessible.

Where possible data will be made available subject to Ethics and participant agreement. However, the personally-identifiable nature of the data collected within i-STENTORE means that in most instances it would be difficult to release collected data.

Table 5 is highlighting which data a) are produced and used in the project and b) will be made openly available.

TABLE 5: DATASET AVAILABILITY

#	Data Type	Data openly available (y/n)	Justification
1	Stakeholder contacts collection	No	The data related to the stakeholder's contacts will not be published as primary data due to privacy and security concerns.
2	Public security services collection	Yes	
3	Digital security solutions collection	Yes	
4	Quantitative survey data	Yes	
5	Expert interview data	No	The data from the expert interviews (recordings, protocols and transcriptions) will not be published

[18] https://internationaldataspaces.org/offers/ids-components/

			as primary data due to privacy and security concerns. Anonymization is not considered as an alternative, because the sample size allows drawing conclusions on the respondents.
6	Focus groups data	No	The data from the focus groups (recordings, protocols and transcriptions) will not be published as primary data due to privacy and security concerns. Anonymization is not considered as an alternative, because the sample size allows drawing conclusions on the respondents.
7	Workshops data	No	The data from the workshops (recordings, protocols and transcriptions) will not be published as primary data due to privacy and security concerns. Anonymization is not considered as an alternative, because the sample size allows drawing conclusions on the respondents.
8	Validation cycles data	No	The data from evaluation survey will not be published due to privacy and security concerns. Anonymization is not considered as an alternative, because the sample size allows drawing conclusions on the respondents.

As it was indicated by the aforementioned information, the following data sets will be made openly accessible: Data type **#2** (Public security services collection), **#3** (Digital security solutions collection) and **#4** (Quantitative survey data). Table 6 describes the accessibility details of these particular datasets.

TABLE 6: DATASET ACCESSIBILITY

#	Data Type	Level of accessibility	Type of availability and required software tools	Information on metadata and additional data information

2	Public security services collection	Public	Filterable and searchable database; can be accessed with a state-of-the-art web browser	No metadata needed; additional information will be provided on the platform
3	Digital security solutions collection	Validated professionals	Filterable and searchable database; can be accessed with a state-of-the-art web browser	No metadata needed; additional information will be provided on the platform
4	Quantitative survey data	Public	Cleaned primary data; can be accessed with SPSS, PowerBI, Excel or any similar data analysis tool.	No metadata needed; additional information will be provided on the platform

5.2.1 Methods or software needed to access the data

No specific software tools will be needed to access the data, since anonymous data sets will be saved and stored in word, pdf or excel to facilitate its exploitation and guarantee their long-term accessibility.

5.2.2 Deposit of data, associated metadata, documentation and code

For the data resulting from the activities of the project, each WP leader will be responsible for depositing and securing the data. An additional instance of all finalized forms of deliverables will be kept on the coordinator's ProofHub (and in some maintenance cases in their Dropbox) account.

5.3 DATA INTEROPERABILITY

The principle of interoperability demands data to be machine-readable and the terminology to be consistent. In adherence to the principle of Data Interoperability, i-STENTORE employs an open-source, standardized, and domain-agnostic Open APIs, which facilitate seamless data interoperability across different systems.
The project will devise appropriate protocols for the creation of data and metadata, along with relevant vocabularies. For i-STENTORE, ensuring data interoperability is crucial as it aims to create semantic Data Models and ontologies. The evaluation of standards and interoperable Data Models within the project will take place in WP3, enabling easier sharing of data from diverse sources.

5.3.1 Interoperability of Data Assessment

The robust Interoperable Data Governance Middleware of i-STENTORE encompasses the Function, Information, and Communication Layers of the SGAM architectural model, providing a powerful framework for the digital platform. Partners will be responsible of storing the data in a comprehensive format and adapted to the real and current needs of the possible practitioners interested in using, merging or exploiting the data generated throughout the project. The assessment of data interoperability will be updated in future reviews in order to guarantee the i-STENTORE data fits the needs of a specific scenario (such as data infrastructures, interests or purpose of data.

5.3.2 Interdisciplinarity and Transdisciplinarity

i-STENTORE aims to foster knowledge co-creation among individuals from diverse fields, transcending traditional disciplinary boundaries. The project inherently embraces an interdisciplinary approach, as it brings together expertise from various scientific domains to develop a comprehensive, interconnected, and reliable storage-enabled European power system. Table 7 presents the various disciplines and the respective WP(s) that these are integrated in the data management of i-STENTORE. The consortium of partners supporting these disciplines encompasses a wide range of data creation and processing of the related knowledge and expertise, ensuring the comprehensive coverage required for the successful implementation of all planned activities.

TABLE 7: DATASET KNOWLEDGE AREAS

Discipline(s)	WP(s)
Sociology (for ensuring consumer acceptance and engagement)	2, 5
STEM i.e., Physics, Mathematics, Data and Computer science (along with specific areas of science related to energy, financial, engineering, industry, water, agriculture and mobility sectors for the design of the tools and systems)	2, 3
STEM for the Demos purposes	4
Economics (for the development of viable business models)	2
Economics (for the exploitation plans)	6
Education science (for organising and implementing workshops / capacity building activities)	6
Political sciences (for better understanding of regulatory measures)	2, 5
Decision making process and pursuing collaborative multi-level governance	1, 6

6 DATA ARCHIVING IMPLEMENTATION

While defining the datasets, significant emphasis is also placed on selecting the platform for archiving and preserving the datasets infrastructure. In the process of selecting a repository, it's crucial to take into account factors like whether the repository[19]:

[19] How to select a data repository? https://www.openaire.eu/opendatapilot-repository-guide

- Issues a unique and persistent identifier to each dataset submitted. This is critical for sustainable citations of data and publications, ensuring that research outputs across various repositories can be traced back to specific researchers and grants.
- Creates a dedicated page for each dataset, furnished with metadata that facilitates discovery, understanding, linking to publications, and citation. This enhances the visibility of research and encourages data reuse.
- Offers usage tracking features such as access and download statistics, which can help gauge how the data has been utilized.
- Cater to the community's needs and preferably holds a 'trustworthy data repository' certification, showcasing an explicit commitment to long-term data availability.
- Fulfils specific data requirements (for instance, accepted formats; access, backup and recovery provisions; and service sustainability). The data repository's policy pages should typically contain most of this information.
- Gives clear instructions on how to cite the deposited data.

6.1 I-STENTORE WEBSITE

The consortium behind i-STENTORE made an early decision to establish a dedicated webpage (implemented by D6.2) for the project. The webpage's design and development were undertaken by consortium partner F6S. The webpage lays out the project's goals, overall methodology, participating partners, pilot studies, and progression status. A "News and Events" section offers regular updates, and a specified area for publications allows for the download of public deliverables, reports, and white papers.

To ensure wide-reaching dissemination of the project outcomes, F6S employs digital marketing strategies that include content for: social media platforms like LinkedIn, Twitter; press releases, interviews, videos, and infographics aimed at local, national, and global media outlets; blog posts, pivotal messages, and ad content. Partners with existing newsletters are periodically featuring i-STENTORE articles.

The F6S platform and its social media channels are used to spotlight significant milestones and open-access journal publications. All these materials are part of D6.1, D6.4-D6.5. When invited by CINEA[20], the project participates in joint information sharing and dissemination activities to enhance visibility and create synergies among Horizon Europe-supported initiatives.

All documents are uploaded in the universally accessible portable document format (PDF). Every download is supplemented with basic metadata, such as the document's title and type.

[20] https://cinea.ec.europa.eu/index_en

F6S routinely backs up all data related to the webpage. Users can access all information on the i-STENTORE website without needing to create an account, and the site will undergo regular backups and be maintained by F6S during the project lifetime and for a minimum of 3 years beyond the project's lifetime.

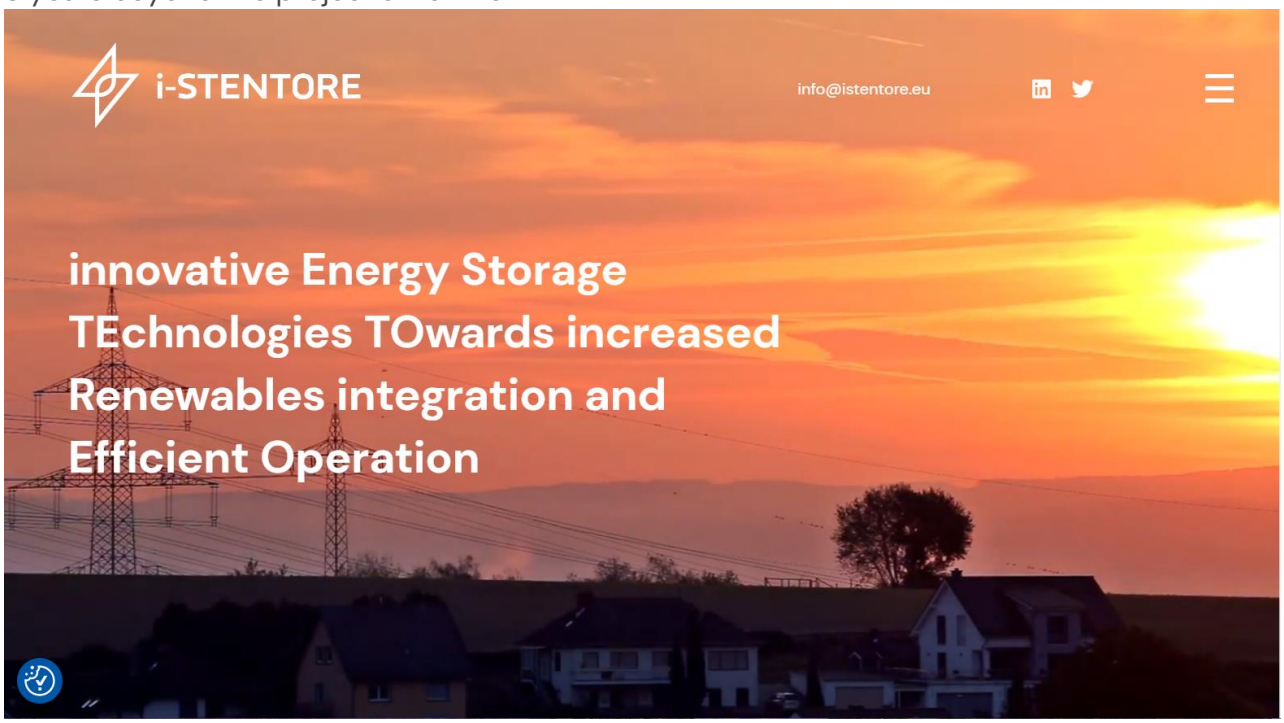

FIGURE 2: 1ST SCREENSHOT OF I-STENTORE'S HOME PAGE (UPPER PART).

FIGURE 3: 2ND SCREENSHOT OF I-STENTORE'S HOME PAGE (MIDDLE PART).

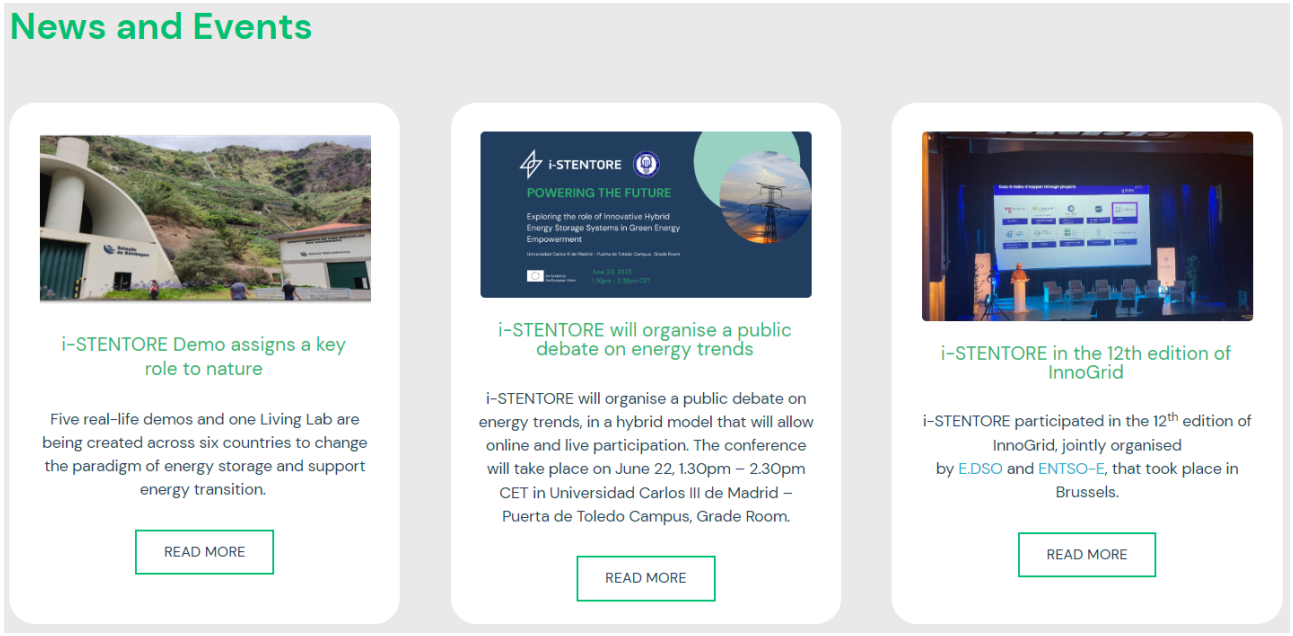

FIGURE 4: 3RD SCREENSHOT OF I-STENTORE'S HOME PAGE (LOWER PART).

Web link: http://istentore.eu/

6.2 PROOFHUB AND DROPBOX

ProofHub[21] is a software solution designed for project management that was developed by ProofHub LLC in 2011. It's a browser-based application that features an array of tools aimed at fostering team collaboration. ProofHub includes a task and deadline calendar, file storage spaces, chat functions, and the capability to establish distinct topics for concurrent activity streams.
Dropbox[22] is a cloud-based file hosting service that allows users to store, synchronize, and share files and folders across different devices and with other users over the internet.
As the coordinator of the project, ED has procured the service of ProofHub for the i-STENTORE project and Dropbox for internal maintenance and backup. ProofHub will be utilized for the project's internal storage of project-associated data and Dropbox for ED's respective backups. Access to the i-STENTORE's ProofHub system is exclusively managed by ED and only authorized i-STENTORE partners are granted entry.

6.3 ZENODO

Zenodo[23] is a research data archive/ online repository which helps researchers share research results in a wide variety of formats for all fields of science. It was created through EC's OpenAIRE+ project[24] and is now hosted at CERN using one of Europe's most reliable hardware infrastructures. Data are backed nightly and replicated to different locations. Zenodo supports not only the publication of scientific papers or white papers, but also the publication of any structured research data (e.g., using XML). Zenodo provides a connector to GitHub that supports open collaboration for source code and versioning for all kinds of data. All uploaded results are structured by using metadata, like for example the contributors' names, keywords, date, location, kind of document, license, and others. Considering the language of textual metadata items, English is preferred. All metadata is licensed under CC license (Creative Commons 'No Rights Reserved'[25]). The property rights or ownership of a result does not change by uploading it to Zenodo.
All public results related to scientific publications that will be produced during the I-STENTORE project will be uploaded to Zenodo for long-term storage and open access.

[21] https://www.proofhub.com/
[22] https://www.dropbox.com/home
[23] https://en.wikipedia.org/wiki/Zenodo
[24] https://www.openaire.eu/
[25] https://creativecommons.org/share-your-work/public-domain/cc0/

6.4 CODE REPOSITORY: GITHUB

Under the umbrella of the i-STENTORE technical solution, two distinct types of repositories will be used for storing the developed programming code. Certain proprietary tools will be housed in one or several private repositories or infrastructure owned by specific project partners. Access to these will be extended to all members of the consortium or to a select group associated with the specific tool.
For the storage of open-source components, the i-STENTORE technical team is evaluating a range of open-source code repositories, including GitHub. GitHub[26], a renowned online repository, is built to support the development, management, and version control of distributed source code. Predominantly utilized for managing source code data, it facilitates global collaboration among developers and offers certain capabilities for documentation and issue tracking.
GitHub offers a blend of paid and free service plans. The free service plan allows for an unlimited number of public, OA repositories with an unlimited number of collaborators. However, private repositories that aren't publicly accessible necessitate a paid service plan. Many open-source projects prefer GitHub for freely sharing their results. The platform employs metadata like contributor usernames, keywords, timestamps, and data file types to organize the projects and their outputs. As per the terms of service, GitHub Inc. asserts no intellectual property rights over the provided material. Textual metadata items are preferably in English.

6.5 PROJECT COMMUNICATION CHANNELS

Besides the i-STENTORE website, project-specific Web 2.0 channels have been launched aiming at extending the visibility of the project's activity. These include i-STENTORE accounts on:

- LinkedIn: https://www.linkedin.com/company/i-stentore/
- Twitter: https://twitter.com/iSTENTORE_EU/status/1622842050839281665

6.6 I-STENTORE PLATFORM

In terms of data management, i-STENTORE is envisioned to be a platform where a multitude of datasets (both structured and unstructured) from various energy storage data sources are gathered on a daily basis. These datasets will be ingested either in batches for facilitating services based on aggregate analytics and historical data or via data streaming technologies to support near real-time services. Following ingestion, the data will undergo processing to enhance its quality, homogenization and modelling to facilitate efficient sharing with users,

[26] https://en.wikipedia.org/wiki/GitHub

and conversion into a format understandable by data analytics services. The data will then be moved to storage, where it can be queried and used by energy analytics services and users.
A critical aspect of the data management services is the security and access control component. Its primary function is to ensure that only authenticated and authorized users and services can access the required resources. For instance, if a user is not logged in to the platform, the access control component will deny access to the requested resources. Similarly, authenticated users who lack permission to a requested resource will also be denied access. User data necessary for this functionality will be stored in a relational database. On the security front, which will be further discussed on Section 8, the implemented security framework will offer features like data encryption, vulnerability detection and mitigation, as well as monitoring and auditing of the various entities' behaviour. As the i-STENTORE project is still in its early stages, all discussions related to the platform are currently theoretical and preparatory, and hence more specific details cannot be provided at this point.

7 ALLOCATION OF RESOURCES

The costs of data storage and maintenance are not going to require extra funding once the project ends. As per the value of the data, it is important to take into account that the topics covered by the project respond to a current need of the energy sector and customers' needs. Therefore, data coming of this project will have a direct impact in the coming years, but might not be of relevance as the challenges are being tackled or replaced by other priorities.
The Project Coordinator bears the responsibility for maintaining the project document repository, while the Scientific Coordinator ensures the quality of all scientific data outcomes. Each partner, on the other hand, is accountable for the recoverability of the data they generate. As already stated, at this stage, the costs associated with making the data FAIR (Findable, Accessible, Interoperable, and Reusable) cannot be estimated since it depends on the volume of data that will be generated.

8 DATA PROTECTION AND SECURITY

8.1 PRIVACY AND DATA PROTECTION

8.1.1 Removing Personal Identifiers

Datasets will be anonymized for research and impact assessment purposes. The collection of personal data within the project, if needed, will be confined to project submission, and participants' informed consent for the usage of their personal data will be necessary. Personal

identities will be safeguarded through the use of anonymous codes, with the association between real names and codes known only to project partners who will secure the records in a safe location. The connection of applications will be encoded and made accessible to external evaluators through this coding. In the event that data must be transferred to partners outside the EU, we will secure approvals from the appropriate Data Protection Office, except for countries that are recognized as providing sufficient protections regarding privacy, fundamental human rights and freedoms, and the exercise of associated rights. On request, the partners will provide the European Commission (EC) with all copies of approvals/notifications concerning the processing of personal data by the competent institutional Data Protection Office. Personal data will be encrypted and stored securely.
The personal data protection processes will follow the REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data, and until valid, the repealing Directive 95/46/EC (General Data Protection Regulation).

8.2 INTELLECTUAL PROPERTY RIGHTS (IPR) GUIDELINES

In the scope of the i-STENTORE project, the careful management of Intellectual Property Rights (IPR) is fundamental to optimize exploitation, dissemination of results, and the project's overall outcomes while simultaneously safeguarding intellectual property. Therefore, it's essential to identify the IPR of the datasets, software, tools, and knowledge that will either be utilized or produced during the project. This process includes understanding licensing schemes, usage terms, and access rights of these assets.
IPR management is addressed internally within the project. Concisely, it encompasses IPR administration at the Consortium level, dealing with issues related to access to the background, ownership of emerging results and innovations, access rights, and IPR protection in the context of dissemination activities.
The activities of WP6 and more specifically "Task 6.2: Exploitation, IPR and innovation management" will provide details of IPR and ownership of results to safeguard the rights of all partners. In particular, this deliverable will provide information on the ownership of background and foreground. In addition, it will describe how IPR will be safeguarded after the project's completion and concerns the ownership of the results that may be generated after the end of the grant period.
Furthermore, the obligations, rights and responsibilities of partners are described in Consortium Agreement (CA) signed by all partners. Issues regarding IPR, such as joint ownership of results or cases in which IPR are affected, are also prescribed in the CA. In addition, details about the background that each partner brings into the project are described in the CA.

8.2.1 Managing Open-Source Licenses

While the consortium is committed to open-source principles, it's important to note that not all components and modules can be offered as open-source due to their proprietary/legacy nature. The consortium will adopt a layered approach to managing the knowledge produced: Solutions will be protected by copyright using a licensing scheme that does not infract the respective companies' terms and conditions; Components that can be offered as open-source will be delivered under an appropriate license (e.g., CC-BY). The consortium will review the software licenses of all algorithms, components, and modules, and decide the license (or combination of licenses) under which the solutions will be released.

8.2.2 IPR Management with the Consortium

The dissemination and use of knowledge generated in i-STENTORE is guided by the terms of the Grant Agreement and the Consortium Agreement. It's agreed that the generated foreground will belong to the beneficiary performing the work. Beneficiaries will also identify the background needed for the project development in a written agreement, and may exclude specific background where suitable. The Management Board will maintain an IPR Directory for the project's lifetime, listing all items of knowledge related to the project work, and clearly stating its owner, nature, status, and dissemination and protection measures for each item. An initial version of the IPR directory will be created early after the project's start.

8.2.3 Patents Landscape Analysis

The project must evaluate if the project's results can be exploited without infringing existing patent claims and if its innovations can be patented. An initial review of the patents suggests that there are no patents/applications addressing hybrid energy storage system, which is our primary innovation.

8.3 DATA SECURITY

i-STENTORE Task 3.7 focuses on the data security aspect which will be guaranteed by creating a privacy and cybersecurity framework that ensures security, detailed access management, anonymization, and encryption across every element of the platform. Therefore, a variety of security methods will be implemented, including but not limited to, decentralization, authentication, authorization, auditing, policy-based management, and data encryption. A key-objective of Task 3.7 is to build a secure and operational platform that merges all these components, resulting in a prototype ready for validation.
Also, it is worth noting that data within i-STENTORE will be secure due to the implementation of the security protocols and frameworks as described earlier in the text. The data security concept primarily necessitates end-users' direct involvement in what is referred to as the 'storage-centric European Energy System,' leading to mutual benefits for all participants. The

i-STENTORE reference architecture with its given emphasis on the SGAM interoperability layers is also a step towards a mature, robust and secure data exchange platform solution.

9 ETHICAL ASPECTS

In order to ensure that all ethical aspects are considered and that the i-STENTORE project is compliant with all legal requirements and ethical issues, a general strategy has been designed by the Ethics Requirements that was defined by deliverables from WP1. This strategy involves an ad hoc monitoring process of the project development by applying the privacy-by-design approach trough a methodological design based on a "Socio-legal Approach." This is a risk approach to privacy and data protection issues in line with the new General Regulation for Data Protection (GDPR).

9.1 ETHICS OF OBJECTIVES, METHODOLOGY AND IMPACT

Within the i-STENTORE project, a range of protocols will be established to safeguard the privacy of participating end-users, should such a situation arise. The consortium managing the project will diligently regulate information access, implementing restrictions where necessary. Key provisions include:

- Adherence to ethical standards and guidelines equivalent to those of Horizon Europe, irrespective of the location of the i-STENTORE demonstrations.
- Provision of clear project descriptions and study objectives to all participants in an easily comprehensible manner.
- Emphasis on the voluntary nature of participation in the study.
- Full disclosure of privacy rights, the potential impacts on participants' lives, and the measures implemented to protect privacy, such as anonymization and secure data storage processes.
- Explanation of the duration and effort required for participation in any activity.
- Clarification of withdrawal rights, with the ability to request the destruction of any personal data.
- Provision of contact information for project stakeholders.

Compliance with ethical codes will be ensured by the consortium through continuous reporting processes. If human involvement is required in the project, participants will be informed about privacy, confidentiality, and compliance with national and EU legislation. Understandable Information Sheets and Informed Consent Forms will be provided, which detail the voluntary nature of participation, potential risks and benefits, and procedures for incidental findings.

Participants can ask questions, receive understandable answers, and withdraw themselves and their data at any time without negative consequences. Signed copies of these forms will

be provided to the subject or their legally authorized representative, with the original copies retained in the subject's research record.
Only anonymized or aggregated data, completely separated from individual identification and profiles, will be processed in relation to project workshops and events. During dissemination, the same types of data will be processed and made available. If personal data processing is necessary under specific circumstances, the responsible partner will appoint a Data Protection Officer to ensure GDPR compliance and provide evidence of authorization to process personal data before such data is accessed or used.
If required by European and national legislative frameworks, the appropriate competent authority will have to grant this authorization in the partner's country. In the event of using specific platforms like Twitter, LinkedIn, Facebook, Google Cloud etc., that might involve personal data, a Data Processing Addendum/Agreement for data processing will be obtained by the responsible partner.
Lastly, the i-STENTORE methodology doesn't involve clinical trials or children's participation, nor does it foresee environmental harm, stigmatization of specific social groups, adverse political or financial repercussions, misuse, etc., as potential impacts.

9.2 COMPLIANCE

The i-STENTORE consortium acknowledges the possibility that the project's activities might give rise to ethical, fundamental rights, privacy, and data protection concerns. It is, therefore, committed to adhering to the highest ethical, fundamental rights, and legal standards recognized at the European Union and International levels. Specifically, efforts will be made to ensure the proposal aligns with the key ethical principles and fundamental rights outlined in:

- The Helsinki Declaration Administrative forms,
- The European Code of Conduct for Research Integrity (ECCRI, 2011),
- The EU Charter on Fundamental Rights (CFREU, 2010),
- The UNESCO Universal Declaration on Bioethics and Human Rights (2005),
- The European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR, 1950),
- The Universal Declaration of Human Rights (UDHR, 1948).

Regarding the rights to privacy and personal data protection, i-STENTORE will adhere to:

- The General Data Protection (GDPR) Regulation (EU) 2016/679,
- The Data Protection Directive (1995/46/EC) and the Directive on Privacy and Electronic Communications (2002/58//EC),
- The EU Charter on Fundamental Rights (articles 7 and 8),
- The European Convention for the Protection of Human Rights and Fundamental Freedoms (article 8),
- The CoE Convention No. 108 for the Protection of Individuals concerning Automatic Processing of Personal Data (1981),
- The International Covenant on Civil and Political Rights (ICCPR, 1966).

The Consortium also recognizes the likelihood of changes to the European data protection framework during the project's lifetime and commits to compliance with any new privacy and

data protection regulations. Finally, the Consortium will adhere to all relevant national and local regulations applicable to the project activity.

10 CONCLUSIONS

This document introduces the plan that the i-STENTORE project will follow for data management and provides an initial analysis of the data sources that will be used or generated during the project as identified by the project consortium partners and the way the project results will be shared. By project results this deliverable defines any kind of information including scientific publications, white papers, Open-Source code, open datasets, anonymous interview results, or mock-up datasets used for gathering feedback from various entities that may be used or generated from the project. The collected datasets in the current version of the report are research data, related to the project's work packages and are managed according to their level of availability (public or sensitive/confidential). The i-STENTORE Data Management also follows the Guidelines on FAIR Data Management in Horizon Europe, i.e., data must be findable, accessible, interoperable, and reusable.
The current report will be a living document throughout the project. The DMP will be updated whenever significant changes arise, such as (but not limited to) new data, new innovations, patent filings, changes in the consortium members and others.

i-STENTORE

innovative Energy Storage TEchnologies TOwards increased Renewables integration and Efficient Operation

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Climate, Infrastructure and Environment Executive Agency (CINEA). Neither the European Union nor the granting authority can be held responsible for them.