interconnect

interoperable solutions connecting smart homes, buildings and grids

WP11 – Project Management

D11.2

Data Management Plan

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant agreement No 857237

DOCUMENT INFORMATION

DOCUMENT	D11.2 – Data Management Plan
TYPE	Report
DISTRIBUTION LEVEL	Public
STATE	EC Approval
DUE DELIVERY DATE	01/06/2020
DATE OF DELIVERY	31/05/2020
VERSION	V3.0
DELIVERABLE RESPONSIBLE	INESC TEC
AUTHOR (S)	David Rua (INESC TEC), Fábio Coelho (INESC TEC), Tiago Freire (INESC TEC), Vasco Dias (INESC TEC)
OFFICIAL REVIEWER/s	EDPC

DOCUMENT HISTORY

VERSION	AUTHORS	DATE	CONTENT AND CHANGES
0.1	David Rua, Fábio Coelho	17/04/2020	Initial version with ToC
1.0	Fábio Coelho, David Rua	30/04/2020	General contributions to the document
1.1	Fábio Coelho, David Rua	07/05/2020	General contributions to the document
1.2	Fábio Coelho, David Rua	15/05/2020	General contributions to the document
2.0	Tiago Freire, Vasco Dias	25/05/2020	Privacy and data protection considerations
2.1	Fábio Coelho, David Rua, Tiago Freire, Vasco Dias	26/05/2020	Internal revision and additional contributions
3.0	David Rua	31/05/2020	Final version for review

ACKNOWLEDGEMENTS

NAME	PARTNER
Olivier Genest	Trialog
Eliana Valles	Sensinov
Leen Peters	ThinkE
Quentin Lancrenon	ThinkE
Stefano Fava	PlanetIdea
Maria Sakali	Heron
Donatos Stavropoulos	Gridnet

DISCLAIMER:

EXECUTIVE SUMMARY

This document presents the Data Management Plan (DMP) of the InterConnect Project and it overviews on the data management procedures and good practices to be followed by the consortium in all field or demonstration activities.

Contributions were requested to consortium partners in the identification of the data protection issues. The Ethical and Data Protection Committee (EDPC) was involved in analysing the reported issues and related context in the sense of harmonizing the DMP in an iterative process.

This document will be subjected to regular updates to ensure compliance with the different project activities, namely those involving external participants. As mentioned throughout the document a set of additional annexes will be introduced to make this DMP a comprehensive and up-to-date live document.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS AND ACRONYMS

Abbreviation	Description
AB	Advisory Board
AMGA	Annotated Model Grant Agreement
CA	Consortium Agreement
DC	Data Controller
DM	Data Manager
DMP	Data Management Plan
DP	Data Processor
DPC	Data Protection Coordinator
DPIA	Data Protection Impact Assessment
EC	European Commission
EDPC	Ethics and Data Protection Committee
GA	Grant Agreement
GDPR	General Data Protection Regulation
IPR	Intellectual Property Rights
PDM	Project Data Manager
PiDM	Pilot Data Manager
SC	Steering Committee
TIC	Technical and Innovation Committee
TRL	Technology Readiness Level
WP	Work Package

1 INTRODUCTION

This document presents the Data Management Plan (DMP) of the InterConnect Project that received funding from the European Union's Horizon 2020 Research and Innovation program under the Grant Agreement (GA) number 857237 and compiles the data management procedures.

The DMP is a reference document that should be followed by the consortium partners when referring to data management activities and related procedures. In this will be the first version of a live document to be updated regularly or whenever a significant change in the procedures needs to be reported and known by the consortium partners. This document reflects the project snapshot at the date of delivery.

Contributions were requested to consortium partners in the identification of the data protection issues. The Ethical and Data Protection Committee (EDPC) was involved in analysing the reported issues and related context in the sense of harmonizing the DMP. Contributions are compiled in the Annex section of this document

2 DATA MANAGEMENT STRUCTURE

The consortium has set several supporting bodies and committees to establish monitoring and control of several aspects of the project. First and foremost we should mention the Steering Committee as the supervisory body for the execution of the Project which shall report to and be accountable to the General Assembly, as well as the Project Coordinator acting as the intermediary between the Parties and the Funding Authority. On its turn the Technical and Innovation Committee, led by TNO, is responsible for managing the consortium risks.

One of such bodies is the Ethics and Data Protection Committee (EDPC) which is a body that assures the proper handling of the aspects related with data and ethics issues of the project. The EDPC is composed of Data Protection Officers (DPO) or Data Protection Responsible Person (when a DPO is not formally designated) representing each of the 11 Work Package (WP) leaders as well as the leaders of each of the project 7 pilots. This committee will support the project consortium regarding any ethical questions and relevant data management issues in particular in what refers to personal data protection implications. In this context one of the responsibilities of EDPC is to monitor compliance with Data Protection Law and identify the Work Packages which may bring more serious concerns from a data protection law standpoint. The EDPC is led by the Data Protection Coordinator (DPC) and as a body reports to the Project Coordinator.

2.1 PROJECT DATA MANAGERS

Project Data Managers (PDMs) nominated by each project Partner, have the overall responsibility, in close collaboration with of the Project Coordinator and the EDPC, for ensuring that the Data Management Plan (DMP) is rightly implemented, according to the plan and the applicable rules, as well as for carrying out periodic reviews of the DMP.

2.2 DATA PROTECTION COORDINATOR

The Data Protection Coordinator (DPC) is the lead person of the EDPC selected by the coordinator as its own representative on data and ethics issues. INESC TEC has appointed Vasco Dias, which serves as DPO of several institutions, including INESC TEC, and has a

solid background in the area with recognized experience and public intervention in such matters.

The DPC main responsibility is to monitor the project compliance with the GDPR and to evaluate and incurring ethical issues as a result of the project activities. In order to do this, the DPC will:

- Assist the PDM on the DMP implementation and on the periodic reviews of the DMP and of the data processing activities;
- Collect information to identify processing activities;
- Analyse and check compliance of any processing activities;
- Inform, advise and issue recommendations;
- Assist and provide advice to the controller in terms of whether or not to carry out an assessment, the risk-based methodology to use, mitigating controls and whether or not it has been carried out accurately and the conclusions comply with the GDPR;
- Maintain the record of processing activities under the responsibility of the controller.

2.3 WORK PACKAGE DATA MANAGER

Given that data can be collect within each WP activities for those where that will happen, each of the WP and pilot leaders assume the position of WP Data Managers (WPDM) or Pilot Data Managers (PiDM) within the Project and will be responsible for managing the data collection procedures. Table 1 summarizes the foreseeable WPs and Pilots where data collection is expected to take place.

TABLE 1: WP AND PILOTS DATA COLLECTION

WP	Related Data Collection Activities	Leading Partner
WP1	• Preparation of services to the exploited in the project pilots • Technologies and solutions preparation • Identification of user-requirements • Definition and explanation of project use-cases (business, high-level, system, etc.)	EEBUS
WP6	• Preparation of pilot project • Characterization of sites, buildings and electric grids • Collection of data of potential participants • Project key-performance indicators quantification	THINK-E
WP7	• Implementation of pilot activities	**WP**: INESC TEC

	• Regular data collection regarding the operation of devices, systems, buildings, and grid infrastructures	**Pilots**: EDPD, THINK-E, EEBUS, iCity, PLANET, GRIDNET, YNCREA
WP8	• Integration of third parties on cascading funding • Data collection from demonstrators and prototype implementations towards joint energy and non-energy services	FBA
WP9	• Collection of data regarding the implementation of a long-term sustainable development of services and technology solutions.	WINGS ICT

In accordance with the Consortium Agreement (CA) each Partner designated a person in charge for monitoring personal data processing activities in the Project, which is represented at the EDPC.

To this end, an extraordinary meeting of the General Assembly takes place after the beginning of the Project, and at the latest before the end of the first year of the Project. The members of the Steering Committee can call on their respective internal experts (data protection officers in particular) for this meeting, which will aim to define precisely the rules and responsibilities relating to the protection of personal data and the implementation of the regulations. The minutes of this meeting will be prepared by the chairman of the meeting and communicated to the Parties, who will accept or amend it according to the procedures provided in the CA. Furthermore, a permanent EDPC, will support the consortium regarding any ethical questions and relevant data management issues.

2.4 DATA CONTROLLER AND DATA PROCESSOR

Regarding the responsibilities for the processing of personal data, Article 4 of the GDPR establishes the following definitions:

(7) 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

(8) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

Additionally, Article 26 states:

(1) Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective

responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.

On the other hand, as pointed out by the Article 29 Working Party in its option of 1/2010, adopted on 16 February 2010, on the concepts of "controller" and "processor": "*the mere fact that different subjects cooperate in processing personal data, for example in a chain, does not entail that they are joint controllers in all cases, since an exchange of data between two parties without sharing purposes or means in a common set of operations should be considered only as a transfer of data between separate controllers.*".

As a first general assessment, given the aforementioned and the activities planned in the Project proposal, one may assume that personal data collected will be under the supervision of either a single controller or various controllers, depending on the number of partners that will be involved in the collection, processing and storage of each dataset. Thus, the roles played by project partners will vary greatly according to the nature and context of the personal data processing activities at stake at each given WP or activity.

The establishment of a Data Sharing Agreement between the project Partners, as provided in the Consortium Agreement, represents an important factor in this regard, contributing decisively for the correct definition of the roles and responsibilities of the Partners with relation to the protection of personal data. The same applies to the rigorous and timely identification of datasets and the mapping of data flows across the project activities, for which regular revisions of the DMP play a key role.

The above mentioned Data Sharing Agreement will also allow for the establishment of common rules and principles in compliance with data protection principles enshrined in the applicable data protection legal framework, namely, data minimization, transparency and lawful processing principles, as well as the respect for a data protection by design and by default approach.

It is worth to mention that the DCs will play a key role in the project's data management, as they will be the party(ies) responsible for following best practices in research as regards the pseudonymization or anonymization techniques applied to personal before storing and sharing it with the other partners and, where applicable, a DP. It is also a DC obligation to evaluate the need to conduct Data Protection Impact Assessments (DPIAs) when required by law in the light of data processing activities that imply higher risks for data subjects.

In this regard the Consortium shall align its practices and procedures with article 89º nº 1 of GDPR, which states that the processing of personal data for scientific research purposes shall be subject to appropriate safeguards for the rights and freedoms of data subjects, in particular by ensuring that technical and organizational measures are in place, including pseudonymisation whenever suitable, in order to comply with data protection principles such as data minimisation. The GDPR further specifies that *"Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner".* Further details on this matter are provided in other sections of the present DMP.

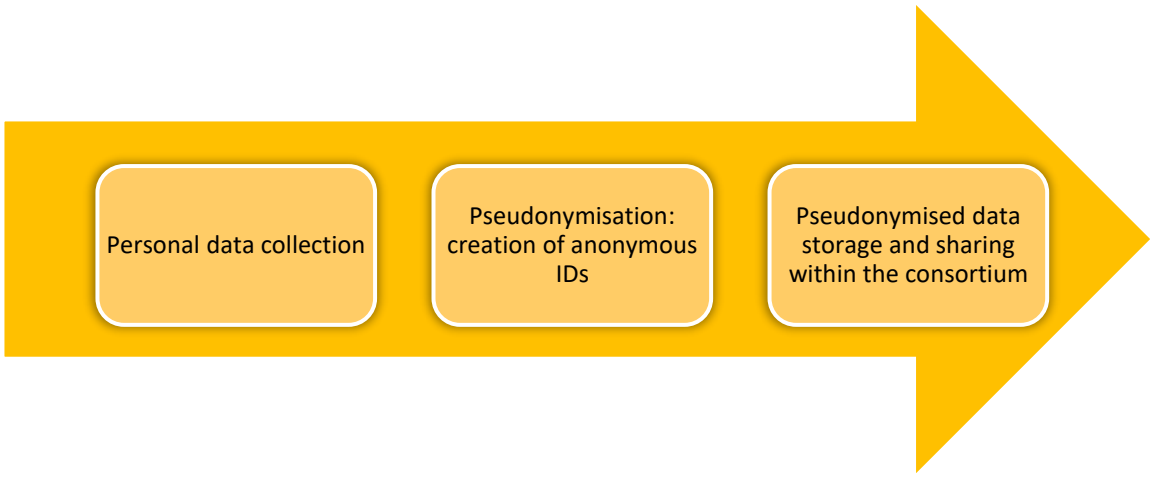

FIGURE 1: DATA PROCEDURE

In summary:

- **Data Controller** (DC) – entity that owns the data and can act as data controller
- **Data Processor** (DP) – entity that processes data and does not own them

3 DATA SUMMARY

Providing interoperability and enabling cross-device or cross-platform services is set as the ultimate challenge within InterConnect project. Enabling the availability of cross-domain services, that serve both Energy related use cases, but also ICT centric use-cases requires several levels of data availability, including the identification of devices, services or platforms and their capabilities, but most importantly, content aware data, specific to services or consumers.

InterConnect sets it-self as a catalyst and a promoter of data protection principles and good practices, by providing tools and methodologies within the consortium and rendering the capability to share and manage data that is essential for the provision of interoperability, while at the same time adhering to the highest levels of data security. Given the large spectrum of candidate use-cases, the amount of large scale pilots and, consequently, the number of associated partners, InterConnect involves the processing of a varied set of categories of data, whose availability should be detailed according to the following table.

Category	Description
Device data	Data related with a device, exposing a service or features/capabilities of a device
Service data	Data related with a service, in the strict sense of advertising capabilities or providing means to connect with foreign services or devices.
Metadata	Data reflecting usage of features, performance or other metrics generated via interacting with a service, or feature.
Operational data	Data related with a device or service, whose contents include advanced content with measurements, instructions, requests, etc. Typically adheres to a communication standard or message marshalling according to a given specification.
User data	Data that relates to a user of a device or service, that often identifies a user directly or indirectly or that holds personal data or that unveils user preferences or patterns.
Business data	Data related to a business use case or partner.
Log data	Data that is generated after a given feature is used. The accumulation of this type of data unveils usage patterns that can be used to solve technical problems, but alto to characterise service usage.
KPI data	Data that reflects aggregated or non-aggregated measurements or performance compliance of a given feature of service.

TABLE 2: DATA TYPES BREAKDOWN

The data categories should reflect the realm of importance and the level of data security, or the need to pre or post-process data, making sure that data travels according to what has been pre-established to a specific data type.

3.1.1 DATA SHARING VIA STANDARDS AND ONTOLOGIES

The provision of interoperability via a multi-vendor approach necessarily goes through sharing data and metadata for service discovery and feature exchange. Considering an ontology as means to expose an interface in which all entities can relate, understand and unlock services, allows a common ground by defining a dictionary and rationale understandable by all engaged parties. However, installing a common interface does not preclude the idea of an absolute data sharing format that is conformed to a pre-established set of datasets or protocols (proprietary, legacy or open). A separation between the available capabilities in each party, and the actual data sharing for business oriented purposes often exists.

Ontologies like SAREF build a flexible hierarchy, composed from a pre-established set of entities and properties, which are then mapped by distinct devices or platforms to characterize their particular features and capabilities. On the one hand, an ontology can in it-self be considered as a dataset, in the sense that it has a structure and that there are field values that characterize and identify entities. On the other hand, using and conforming to an ontology does not necessarily implies that a given party is required to consider all available properties, rendering it as a flexible and customizable array of features. The data models, and consequently the datasets considered for semantic purposes should be addressed from a device, digital platform or service point of view, and particularized for pilots.

Semantical data sharing, collection, processing and forwarding should be considered as inherent to InterConnect project's architecture and its interoperability toolbox and should be tied together with specific data models for data exchange.

Detailing the specific data, conforming models, specific data exchange protocols, access criteria, data control and processing capabilities will be detailed in future installations of this deliverable, as they derive from architectural specific assessment.

The provision of interoperability powered by ontologies and similar standards does not preclude data that is either created and/or held by parties (e.g., IoT Device, Digital platform that aggregates services, standalone service, etc) to be shared upwards. Consumer, business, KPI or performance related data shall be kept within its original domain (e.g., IoT Device, Digital platform that aggregates data, service server, service associated database, etc) and exchanged only by means of a pilot feature, basic interoperability service or explicit consent; all managed by the interoperability toolbox.

3.2 DATASET CATALOGUE

The DMP will unfold as a living document as specific datasets are identified and catalogued. For this purpose, INESC TEC will hold a repository where the cataloguing of datasets should be added and managed throughout the execution of the project. The repository is based on CKAN where partners will adhere and add all relevant information to allow categorisation, cataloguing and update. WPDM and PiDM are responsible for data management and maintenance falling within the scope of their responsibility.

3.2.1 CREATING A DATASET DESCRIPTION

Creating a dataset will be available to all partners, according to a workflow defined within the project's EDPC – Ethics and Data Protection Committee. The data is established after a joint data collection effort within the consortium, surveying available capabilities according to the template described in section 3.2.2. The next version of this document will detail the dataset insertion workflow.

3.2.2 DATASET DESCRIPTION

At the time of this document it is not possible to fully grasp the characteristics of the datasets that will be used throughout the project. However to infer on the datasets the following template was used, as proposed by the EC, to identify the issues related to the different components of the DMP. This template was used by the project partners to address the typical issues associated to each component of the DMP considering the data collection and data management activities in which each one of them will be involved. The contributions can be found in the Annex

DMP component	Issues to be addressed	Explanation
1. Data summary	• State the purpose of the data collection/generation • Explain the relation to the objectives of the project • Specify the types and formats of data generated/collected • Specify if existing data is being re-used (if any) • Specify the origin of the data • State the expected size of the data (if known) • Outline the data utility: to whom will it be useful	
2. FAIR Data 2.1. Making data findable, including	• Outline the discoverability of data (metadata provision) • Outline the identifiability of data and refer to standard identification mechanism. Do you make use of persistent and unique identifiers such as Digital Object Identifiers?	

provisions for metadata	• Outline naming conventions used • Outline the approach towards search keyword • Outline the approach for clear versioning • Specify standards for metadata creation (if any). If there are no standards in your discipline describe what type of metadata will be created and how	
2.2 Making data openly accessible	• Specify which data will be made openly available? If some data is kept closed provide rationale for doing so • Specify how the data will be made available • Specify what methods or software tools are needed to access the data? Is documentation about the software needed to access the data included? Is it possible to include the relevant software (e.g. in open source code)? • Specify where the data and associated metadata, documentation and code are deposited • Specify how access will be provided in case there are any restrictions	
2.3. Making data interoperable	• Assess the interoperability of your data. Specify what data and metadata vocabularies, standards or methodologies you will follow to facilitate interoperability. • Specify whether you will be using standard vocabulary for all data types present in your data set, to allow inter-disciplinary interoperability? If not, will you provide mapping to more commonly used ontologies?	
2.4. Increase data re-use (through clarifying licences)	• Specify how the data will be licenced to permit the widest reuse possible • Specify when the data will be made available for re-use. If applicable, specify why and for what period a data embargo is needed • Specify whether the data produced and/or used in the project is useable by third parties, in particular after the end of the project? If the re-use of some data is restricted, explain why • Describe data quality assurance processes • Specify the length of time for which the data will remain re-usable	
3. Allocation of resources	• Estimate the costs for making your data FAIR. Describe how you intend to cover these costs • Clearly identify responsibilities for data management in your project • Describe costs and potential value of long-term preservation	
4. Data security	• Address data recovery as well as secure storage and transfer of sensitive data	
5. Ethical aspects	• To be covered in the context of the ethics review, ethics section of DoA and ethics deliverables. Include references and related technical aspects if not covered by the former	
6. Other	• Refer to other national/funder/sectorial/departmental procedures for data management that you are using (if any)	

4 DATA HANDLING AND SHARING WITHIN THE PROJECT

This section sets out how the partners will handle the different datasets. It also defines data flows between project partners.

4.1 DATA HANDLING

This section summarily describes the procedures for data handling to be used by the InterConnect consortium when dealing with the sensitive data collected from the seven different demonstrators of the project running in: Portugal, France, Belgium, Netherlands, Germany, Italy and Greece.

4.1.1 DATA COLLECTION

Data collection in the project will be carried-out through different initiatives such as surveys, testing activities, sensing and metering, in each of the different demonstrators concerning the following topics:

- User preferences (comfort, convenience, indoor quality, optimization criteria, etc.)
- Energy use (energy consumption, energy production, etc.)
- Available controllable devices (settings, configurations, usage-patterns, etc.)
- Electric mobility (type of vehicle, charging type, charging rate, etc.)
- Mobile devices (type of device, model, operating system, etc.)
- other

At this stage the level of detail regarding the data collection strategy is still limited as it will depend on the type and number of buildings that will be used in the demonstration activation of the project pilots, as well, as the type of devices and systems available in each one of them. Moreover, from the grid side the same rationale applies as feeders, secondary substations and even substations will be selected at a later stage.

4.1.2 DATA PROTECTION

Project partners as data controllers will be responsible for ensuring the lawful processing of the respective datasets as well as for the implementation of security, technical and organizational measures to ensure the security of project data and avoid its alteration, loss, and / or unauthorized access, given the state of technology, the nature of the data stored and the risks they are exposed to, whether from human action or the physical or natural. Moreover, the need for conducting data protection impact assessments will be assessed by the project partners as data controllers and discussed in detail within the EDPC.

Following the provisions already defined in the Consortium Agreement, through the establishment of a specific data sharing agreement, the project partner will be able to further specify rules and procedures regarding data processing activities in the project, in order ensure compliance with data protection principles and legal framework. It is envisaged that the EDPC will play a decisive role in the negotiation of such important data management instrument.

Nonetheless, among the best practices implemented in the consortium, all data exchanged between the participants and the InterConnect partners shall be duly protected by the use of certifiable, anonymized, encoded or encrypted data exchange mechanisms. Pseudonymisation schemes will be used to prevent the direct association between the pilot participants and the collected or exchanged information. Authentication and security certificates will be used to guarantee high levels of data protection. All data will be encoded using UTF-8 and sent through a JSON structure at specific time frames and similar methods.

4.1.3 DATA STORAGE

Data sets generated or processed in the project will be safely stored in private servers hosted securely by different partners of the consortium using the necessary data protection schemes and suitable organization and technical measures, or managed by project partners and hosted in professional data centres.

No international data transfers are envisaged in the project. At any event, and before a data transfer to third countries or international organizations may take place in the ambit of the project, the partner responsible for such data communication shall ensure compliance with the rules provided in the Chapter V of the GDPR.

Later details regarding will be updated as soon as final architectural decisions are taken into account, as outputs of distinct work packages. As an overall goal, data storage will be kept in

the departing domain, that is, under the storage location selected by each partner. Data sharing and consequently data storage outside that realm will be treated as a special, being detailed and documented.

4.1.4 DATA RETENTION

The data stored in the different servers of the InterConnect consortium partners is protected by redundancy and replication procedures that allow recovery in case of software or hardware failures. Data retention periods shall be defined by each data controller according to the applicable legal framework and in line with a data minimization principle.

4.1.5 DATA DESTRUCTION

Specific and documented data protection procedures for the destruction of data will be discussed and defined within the consortium, with the support of the EDPC, in order to ensure its compliance with GDPR and the applicable legal framework. Due consideration shall be given to participants rights as data subjects, as well as to derogations or limitations that may apply in the specific context of scientific research.

At any event, whenever a data destruction procedure takes place, proof of data destruction will be provided by each partner involved in such data elimination request/ processing activity.

A data destruction certificate template will be approved by the consortium and included as annex to this DMP in its next versions.

4.2 DATA RESPONSIBILITY

As a general rule, the direct responsible for each dataset, regarding data capture, metadata production, data quality, storage and backup, data archiving and data sharing and deletion will be the respective DC or DCs.

The WP DMs are responsible for ensuring, together with the respective DCs, that the datasets of their WP are managed in compliance with the DMP. In addition, the WP DM shall be the point of contact for any compliance activity, in particular where personal data are involved, and for the preparation and/or the implementation of the procedures established at the consortium level, with the support of the EDPC .

The PDM has the overall responsibility of ensuring that the DMP is implemented in compliance with the GDPR and carrying out periodic reviews of the DMP and data processing activities.

The DPC will assist the PDM on the implementation of the DMP and on the periodic reviews of the DMP and of the data processing activities.

4.3 DEMONSTRATORS ACTIVITIES

The project demonstration activities are associated to each of the pilots that will run in different countries, as part of WP6 and WP7, as well as in associated pilots or other smaller demonstrators related to the cascading support that provides technical and financial support to third-parties within WP8. Preparatory activities are also envisaged within the scope of WP1 in the definition of the project use-cases.

4.3.1 PROJECT PILOTS:

4.3.1.1 PORTUGAL (SMART GRID INFRASTRUCTURE AS AN ENABLER OF NEW BUSINESS DEMAND TO INTEGRATE DSF IN E-MARKETS)

Overall Objectives

- Exploit different energy services (P2P, flexibility management, etc.) for households, buildings, and energy communities.
- Exploit interoperable digital platforms for energy and non-energy services based on cloud and hybrid connectivity solutions
- Validate and flexibility platforms and the data exchange interfaces within the DSO infrastructure and demonstrate the compliance with CIM standards and potential for wide adoption at the EU level

Unique features

- Combines both residential and non-residential end-users, DSO, ICT solutions providers and electricity retailers
- Extending SAREF to a new generation of interoperable BEMS system for non-domestic end-users
- Offer technical conditions to test a standardized DSO interface between smart grid operation and market players

Use cases / demonstration activities

- DSF management at the local level for P2P trading, energy efficiency and e-mobility business services

- Integration of DSF in wholesale market bidding strategies considering consumers from different segments (residential, commercial buildings and supermarkets)
- Demonstrate the DSO standardized interface enabling a set of standardized flexibility products for DSO needs that is fully interoperable with legacy systems such as SCADA/DMS level and with Interoperable marketplace toolbox
- Validation of SAREF and extensions for buildings

Level of standardization and interoperability: SAREF version will be implemented, as well as SAREF4ENER and SAREF4BLDG extension. Grid systems are supported by the plethora of CIM-based standards.

Available technologies and infrastructure

- 250 households in 5 sites equipped with HEMS, storage, PV & smart appliances from SENSIBLE, UPGRID, InteGrid projects
- 12 non-residential/commercial buildings covering 5 different geographical regions in Portugal. Include industrial thermal loads, HVAC, PV and EV chargers
- Advanced DMS/SCADA grid management functions from FP7 evolvDSO and H2020 InteGrid projects.
- Grid and market hub platform implemented in H2020 InteGrid project

New technologies

- BEMS, IoT platform, interoperable controllable appliances
- Blockchain-based platform for P2P markets
- Flexibility platform and DSO standardized interface

4.3.1.2 BELGIUM (ENABLING ENERGY COMMUNITIES)

Overall Objectives

- Demonstrate the added value of a common ontology in 8 complementary set-ups
- Integrate energy and non-energy services and evaluate the added value for the stakeholders
- Implement and demonstrate future business model such as P2P exchange and dynamic tariffs (also for heat) in local energy communities

Unique features

- Includes multi-energy industrial and residential sites

- Interacts with one of Flanders largest cooperation projects on energy systems which includes the DSO, all Flemish research institutes and 25 of Flanders' most active companies in the energy sector and backed up with support of the Flemish Energy Agency and the Regulator for the gas and electricity market

Use cases / demonstration activities

- Nanogrid with a single building hosting an office and a housing unit, optimising local energy streams including solar, P2G, V2G, smart appliances, heat pump and storage
- Demonstrating local energy communities from technical legal, economic and social perspective. Validation of P2P trading and its integration in distribution network operation.

Level of standardization and interoperability: integration of 220 SAREF compliant household appliances, adding a SAREF wrapper around over 30 energy and non-energy services and implementing interoperability interfaces for the 8 different digital platforms that will be demonstrated

New technologies

- SAREF compliant appliances, heat pumps and uni- & bi-directional chargers
- Energy management systems at building & neighbourhood level as well as interacting with the grid
- P2P services and standardized interface with the distribution network

Available technologies and infrastructure

- 636 households with electric boilers, heat pumps and/or electric heating; 51 buildings and 60 EV charging points
- Mix of commercial-educational and residential functions in a single building to deep retrofit with different communication technologies on site
- Small scale public buildings and local energy community with direct electric resistance heating
- 80 households are connected to a district heating network, with a district heating network substation and integrated electric booster in each housing unit
- New Nearly Zero Energy Buildings development with 200 new connections in the timeline of InterConnect, district heating & cooling with ice storage, heat pumps, PV and electrical storage
- Industrial energy community with partially existing and partially new buildings, new district heating networks and solar park, including battery storage.

- Advanced algorithm with AI and P2P designed in matching funding Flemish project context
- Science park EV charging set up with 1.3 MW of EV chargers

4.3.1.3 GERMANY (DSF SERVICES FOR SUPPORTING THE GRID AND LOCAL ENERGY OPTIMIZATION)

Overall Objectives

- Explore flexible tariffs to deferral network expansion
- Optimize use of energy with maximum comfort at lowest cost
- Interaction between Demand Side Management, Demand Response Management and Neighbourhood Management (e.g. power contracting, P-max set points from the DSO)

Unique features

- Usage of SPINE as communication language between smart devices and CEM
- Usage of SAREF4ENER as common ontology and API extensions for the communication language
- Integration of existing communication technologies like IEC 61850 to enable CEM / grid communication

Use cases / demonstration activities

- Manage flexibilities to provide grid services (e.g., overload and underload scenarios) through a bi-directional communication from grid to device level and to optimize energy costs in hotels
- Demand Side Management based on variable tariffs (spot prices, variable grid fees, etc.), provide grid services (e.g. avoid grid peak loads with power limitation set points)
- A CEM will aggregate energy demands/offers, manage flexibilities and power limitation set-points from the grid

Level of standardization and interoperability: EN50631 as SPINE extract for white goods; SPINE data model available; SPINE as 100% SAREF4ENER compatible.

Available technologies and infrastructure

- 50 residential homes/apartments (Norderstedt); 15 hotels (Kassel)
- Existing infrastructure in Norderstedt and existing projects NEW 4.0 technology
- DiTour-EE technology

New technologies

- Service / marketplace level: SAREF4ENER API
- Grid control level: IEC 61850 and alternative communication mappings to SPINE / CEM
- Aggregation platform, CEM, BEMS
- EV charging station in 50 households (extension) and 15 hotels plus smart appliances

4.3.1.4 NETHERLANDS ((RE)DEVELOPED DOMESTIC AND MULTI-TENANT BUILDINGS BOOSTING IOT CONSUMER CENTRED SERVICES)

Overall Objectives

- Assess user engagement in energy and non-energy services implying the cooperation and sharing of data between neighbours (including social housing)
- Demonstrate interoperability of different systems especially from an urban operator perspective, e.g. energy, mobility, connectivity and quality of live
- Optimising the use of PV energy for the community by matching with smart devices

Unique features

- Implementation over a smart city infrastructure with range of sensor devices and fibre optic communication infrastructure.
- IoT technologies available for large-scale rollout of software and services, making use of local information (DSO/network, smart meter, etc.)
- Test interoperability with latest available technology like DC Houses, EV smart charging, etc.

Use cases / demonstration activities

- Demonstrate the engagement of residents in relation to sharing their (individual) data for enabling new energy and non-energy data-driven services
- Demonstrate (on large-scale) consumer centred applications based on multi-modal data from plug-and-play IoT devices/appliances/EVs/local storage/sensors
- Demonstrate the optimal operation and use of mixed types of energy flexibility of home appliances, EV and local storage using IoT technologies, considering grid constraints and RES
- Demonstrate digital platforms and services based on the WP2 interoperability architecture and defined (pre) standards
- Enable P2P energy markets so that residents can exchange energy, while still preventing grid congestion

Level of standardization and interoperability: consider the use of open standards like USEF and OCPI (Open Charge Point Interface). SAREF compliant InterConnect reference architecture will be adopted.

Available technologies and infrastructure

- 2 buildings, one with 150 125 apartments, and the other with a mix of approx. 50 apartments and approximately 120.000m2 of commercial space
- Robust smart city fibre optic infrastructure with a connection to a Smart City Data Centre (H2020 Triangulum project)
- Smart EV charging infrastructure is available and all sort of sensors are installed in public and private (in-house) space (H2020 Interflex)

New technologies

- IoT gateways, sensing and smart appliances
- New AI based technologies for improved energy awareness and other user-centric machine learning services

4.3.1.5 ITALY (IMPLEMENTATION OF ADVANCED DSF SCENARIOS IN SOCIAL HOUSING RESIDENTIAL DWELLINGS)

Overall Objectives

- Test and demonstration of an interoperable (SAREF compliant) HEMS for domestic apartments, involving two different manufacturers of home appliances
- Demonstrate the interoperability and data exchange between systems and devices in the Planet District App, through the Interoperable marketplace toolbox and standardized interface
- Exploit different energy and non-energy services, including flexibility services for grid support

Unique features

- Potential to test economic and social benefits from reducing energy poverty in social houses
- Involvement of the social manager on site in the validation of user acceptance of energy and non-energy services

Use cases / demonstration activities

- Demonstrate the implementation of SAREF and interoperability between smart devices, HEMS, the energy manager and cloud services and District App for social innovation and energy management
- Showcase the benefits of IoT assisted energy management by involving many different types of appliances
- Validation of user acceptance and understanding of consumer behaviour for actively engaging in DSF through adequate incentives (energy cost, social responsibility, etc.)

Level of standardization and interoperability: HEMS that uses multi-standard data models for the interoperable integration of protocols like KNX, BACNET (Building Automation and Control NETworks), etc., in light of the SAREF philosophy. MQTT strategies will be sought to ensure the interoperability with the digital ICT platforms. IoT sensors for energy management working on LoraWan

Available technologies and infrastructure

- 480 social apartments in Milan
- IoT for smart metering (electricity and thermal consumption with heat pumps)
- App for social innovation actions and energy management

New technologies

- Additional smart home devices, installed by Smabit that allows monitoring of air quality, humidity level, private video surveillance, etc
- Additional Whirlpool's smart home appliances that allows to control electric consumption peaks and interact with IoT power devices

4.3.1.6 GREECE (IMPLEMENTATION OF ADVANCED DEMAND RESPONSE SCENARIOS IN RESIDENTIAL SETUPS):

Overall Objectives:

- Demonstrate an integrated residential setup in a large residential community (>1000 customers)
- Demonstrate DSF services, through the active participation of large communities in energy markets
- Demonstrate the integration of home appliances with related home comfort and building automation services

Unique features:

- Involves the coordination of distributed generation and DSF provided by residential end-users
- Testing of two interoperable home-IoT platforms

Use cases / demonstration activities:

- Demonstrate the implementation of SAREF in two different home-IoT solutions and the offered interoperability across a wide range of legacy and smart appliances, the energy manager and cloud services
- Showcase resulting AI/cloud-based applications &services (optimized DR decisions, energy forecasting, optimized EV charging)
- Characterization of user acceptance and consumption behaviour through mobile apps, employing gamification and incentives mechanisms

Level of standardization and interoperability: extending the pilot home-IoT platforms to enable SAREF compatibility and the interface between end-users and smart grid

Available technologies and infrastructure:

- 1000 houses of HERON customers with existing appliances, HVAC, lighting, etc. and part with smart meters; 150 residential customers with installed PV systems;
- 50 + 20 households equipped with GRIDNET's and COSMOTE's smart-home systems.
- 14 EV private charging stations

New technologies:

- DR platform and flexible contracts for consumers
- HERON customers will be equipped with the SAREF-ized home-IoT solution of GRIDNET and COSMOTE and SAREF compliant smart appliances

4.3.1.7 FRANCE (DEMAND FLEXIBILITY FOR SUPPORTING THE GRID IN NORMAL AND EMERGENCY OPERATION - AN END-USERS FOCUSED APPROACH)

Overall Objectives

- Implementation and demonstration of energy ontology for interoperability between smart grids actors (retailers, aggregators, DSO and end-users)
- Validation of IoT architecture and its possible interaction with smart metering infrastructure

- Business cases demonstrating the economic and social needs to have end users' contribution to DSF. Explore new multi-energy services (e.g. electricity, heat, water)

Unique features

- Covers the whole chain, from the DSO grid monitoring, to the end-user's appliances, considering local energy communities and microgrid.
- Includes social studies and living labs to test the end-users' participation in flexibility services and its enabling technologies
- H2020 Interflex flexibility platform, allowing residential cons. participation through a plug-and-play interoperable solutions

Use cases / demonstration activities

- Optimal activation of available local flexibilities in preventive or emergency scenarios, using interoperable ICT solutions. Two different architectures will be tested: the flexibility function architecture from Smart Grid Architecture Model (SGAM) and one relying on existing smart meters infrastructure.
- Experiment novel energy and non-energy services related to the adoption of DSF by end-users and Smart-Grids actors. Following potential experimentations will include electric vehicle charging, storage, self DER consumption.

Level of standardization and interoperability: every installed technology (e.g., appliances, aggregator's platform, CEMs) will implement SAREF ontology.

Available technologies and infrastructure

- 250 households, 20 tertiary/commercial buildings, 1 school
- ENEDIS flexibility platform, that allows the DSO to link the forecasted grid voltage profiles with an aggregator flexibility offer
- Flexibility aggregation platform from ENGIE to compute available local flexibility
- Smart buildings with remote control of lights, heat and stores
- Smart meters in each of the 3 sites including DER and Electric vehicles

New technologies

- Smart appliances will be installed in some selected households, together with HEMS, PV and storage
- B2C flexibility solutions at local level
- Interoperability implementation for flexibility platform for DSO and aggregators' solutions
- Smart Charging solutions for fleet and individual EV

4.3.2 THIRD-PARTY DEMONSTRATORS AND PILOT:

The InterConnect project contemplates a Financial Support to Third Parties (FSTP) in the form of grants to other beneficiaries, third parties other than consortium members, to strengthen activities of the project. This is a cascading funding that will be made available to enhance the project outreach of the produced results and at the same time incentivize other organizations to provide developments and results on their own, aligned the project mission. Funding Box Association (FBA) is the main responsible partner for the FSTP initiatives.

The FSTP regulation is set by the part K of the General Annexes of the Work Programme [2], where it is established that the consortium needs to set the selection process of organizations (third parties) to which financial support will be granted.

The FSTP will be ensured through financial support in the form of a **grant** to support the activities of the other beneficiaries and in the form of **non-financial support services** to organizations in the form of Technical and Business Mentoring, to enhance the support from a technical and business perspective.

This form of support intends to support two types of initiatives:

- **Prototypes**: “Interoperable-by-design prototypes”
- **Demonstrators**: “Interoperable-by-adoption demonstrators”

In the Prototypes initiatives, small and innovative ICT players are expected to develop novel services/applications for smart homes and grids, with a clear societal and economic value, on top of the Interoperability Toolkit provided by the InterConnect project.

In the Demonstrators initiatives, small demonstrators are expected to be produced where the adaptation of non-native interoperable applications and services will be carried-out by means of the Interoperability Toolkit. Those services and/or applications, running on top of the InterConnect pilots and associated pilots, will allow for the validation and acceptance of end-users.

Additional information about the related aspects of data handling and sharing within the consortium and with third-parties will be set in more detail at a later stage of the project.

4.4 DATA SHARING WITHIN THE PROJECT

This section sets out a description of data sharing among project partners (i.e., not with third parties).

A “privacy by design” and a “security by design” approach will be followed in InterConnect, regarding the collection and processing of personal data.

As already mentioned above, DCs will pseudonymise personal data before storing and sharing it with other partners (regardless of being qualified as DCs or DPs in each case scenario).

It was already mentioned that a general data sharing agreement will be signed by all partners. Once negotiated and concluded such general data sharing agreement will be presented as an Annex to the present DMP in its subsequent versions.

The entities that will store each dataset (data holders) and share them with other partners (data recipients) for executing the activities listed in the work plan shall be duly identified and mapped in order to get a general overview of the data holders and data recipients per WP as well as the main reason for sharing the respective datasets.

Regular reviews of the DMP will update and keep on track data sharing activities within the consortium.

4.5 METADATA AND MAKING DATA INTEROPERABLE

With respect to each identified dataset, the responsible party (DC) or parties (DCs) shall indicate the following:

- the data format used;
- any applicable data standard;
- if the data produced is interoperable.

To the extent possible, all data collected within the project shall conform to international data standards, metadata vocabularies and ontologies, and methodologies enabling the data to be more easily interoperable and thus sharable.

4.6 DATA SECURITY

This section sets out a summary description of security measures to be applied to the datasets. Each dataset shall include a reference to a security level and detail specific security measures applied, especially if personal data is processed.

For the purpose of the project, the following security levels were defined:

Level	Type	Handling / security measures
Very high	Sensitive personal data generated in the project and confidential information or SW code specifically marked as trade secret.	This data may not be shared even among project partners, except where provided for in specific data sharing agreements. This data should be encrypted in storage and communications.
High	Proprietary SW, personal data, confidential information not specifically marked as a trade secret.	This data may be shared among project partners for the performance of the project as provided for in the CA.
Medium	Unique datasets relating to project performance and results.	This data may be shared among project partners and with external entities upon agreement of the InterConnect project partners.
Low	Environmental and building data and other general data used as benchmarks, etc.	This data may be shared among project partners and with external entities upon agreement of the InterConnect project partners.

TABLE 3: DATA SECURITY CLASSIFICATION

The DCs should also include, in the tables of Annex II, the following information:

- Level of confidentiality of the data;
- Risks to data security and how will these be managed;
- Access control to keep the data secure;
- Compliance with security standards, e.g. ISO 27001;
- Access mechanisms by project collaborators to access the data securely;
- Repositories' structure and characteristics, for data preservation;
- The option for certified repositories for long-term preservation and curation;
- List of DPs that will process the dataset on their behalf.

5 ACCESS, SHARING AND REUSE OF DATA

InterConnect is focused in sharing and opening as much data collected within the project as possible, within the limits imposed by confidentiality obligations and privacy protection requirements.

5.1 DATA SHARING PRINCIPLES

The following principles will apply to all the data collected in InterConnect project:

- All data collected in the course of the project will be made available to project partners, except datasets classified with a security level “Very High”. For these, a specific data sharing agreement between involved partners is required. Regarding personal data, the DCs will pseudonymise personal data before storing and sharing it with the respective DPs.
- All data supporting scientific publications will be anonymised and made available to support dissemination of project achievements. If the data cannot be anonymised, the data will be pseudonymised and may be made available on a case-by-case basis subject to confidentiality and data privacy obligations.
- When there is no risk to confidentiality, privacy and future exploitation models of project technologies, the data will be made available to all under FAIR principles (see section 5.3).
- The PDM, together with the DPC and the WPDM, shall identify, among other issues, those datasets that may be shared and/or opened, as well as anonymization / pseudonymisation procedures to be implemented and other technical and organisational measures tailored to specific issues related with datasets that may be of interest to the scientific community and to the general public.
- Sharing data is not the same as opening the data. The PDM, together with the DPC and the WPDM, shall determine the conditions on sharing (on request, etc.) and for making data fully open or re-usable for academic purposes (see questions below that will be considered for data sharing).
- The data may be made available under fully open data licenses (CC0, ODBL), or under licenses for academic non-commercial use only, in accordance with the rules established within the consortium.

Based on the above principles, data sharing within the project will be defined taking into account the answers to the following questions:

- With whom will the project share the data, and under what conditions and how?
- When will the project make the data available?
- How will potential users find out about the data?
- Will the project share data via a repository, handle requests directly or use another mechanism?
- Does sharing the data raise privacy, ethical, or confidentiality concerns? Can a plan be put in place to protect or anonymize data, if needed?
- Who holds intellectual property rights for the data and other information created by the project? Will any copyrighted or licensed material be used? Do project partners have permission to use/disseminate this material?
- Are there any patent- or technology-licensing-related restrictions on data sharing?
- Will the project permit re-use, redistribution, or the creation of new tools, services, datasets, or products (derivatives)? Will commercial use be allowed?

5.2 RESTRICTIONS ON DATA SHARING

InterConnect will be collecting data that is either personal or contains technology or business secrets that are useful for the future exploitation of the technologies developed by the project partners. Accordingly, not all data may be subject to public release. For data disclosure conditions will be settled according to the existing law, stipulated regulation, and the interest of involved parties, including project partners.

For each dataset, the DCs shall set out the restrictions on sharing of the data in the tables of Annex II, including:

- Expected difficulties in sharing the data (personal data, confidentiality of the dataset) and means for overcoming these;
- Technical limitations or requirements (infrastructure, software, etc.);
- Purpose related limitations (commercial/non-commercial, scientific only, etc.);
- Temporal limitations (embargos).

5.3 INTRODUCTION TO FAIR

Data in H2020 projects should follow the 'FAIR' guidelines, which means that data should be findable, accessible, interoperable and re-usable [1]. These principles precede implementation

choices and do not necessarily suggest any specific technology, standard, or implementation solution.

Data from InterConnect project shall be accessible and re-usable among project partners using standardized or de-facto formats. This is a requirement to ensure interoperability and harmonization of data formats that may eventually facilitate opening the data.

The PDM, together with the DPC and the WPDM, will evaluate how the data may be further shared and reused under the FAIR principles.

5.3.1 MAKING DATA OPENLY ACCESSIBLE

The following questions will be addressed for each identified dataset in order to clearly mark which data is openly accessible:

Which data produced and/or used in the project will be made openly available as the default? If certain datasets cannot be shared (or need to be shared under restrictions), explain why, clearly separating legal and contractual reasons from voluntary restrictions.

- How will the data be made accessible (e.g. by deposition in a repository)?
- What methods or software tools are needed to access the data?
- Is documentation about the software needed to access the data included?
- Is it possible to include the relevant software (e.g. in open source code)?
- Where will the data and associated metadata, documentation and code be deposited? Preference should be given to certified repositories that support open access where possible.
- Have you explored appropriate arrangements with the identified repository?
- If there are restrictions on use, how will the access be provided?
- Is there a need for a data access committee?
- Are there well-described conditions for access (i.e. a machine-readable license)?
- How will the identity of the person accessing the data be ascertained?

The corresponding answers will be included in the updated version of the DMP in the datasets descriptions.

5.3.2 MAKING DATA FINDABLE, INCLUDING PROVISIONS FOR METADATA

The following questions will be addressed with the purpose of making accessible data findable:

- Is the data produced and/or used in the project discoverable with metadata, identifiable and locatable by means of a standard identification mechanism (e.g., persistent and unique identifiers such as Digital Object Identifiers (DOI))?
- What naming conventions will be followed?
- Can search keywords be provided that optimize possibilities for re-use?
- What versioning (numbers) will be used?
- What metadata will be created?
    - In case metadata standards do not exist, what type of metadata will be created and how?

The corresponding answers will be included in the updated version of the DMP in the datasets descriptions.

5.3.3 INTEROPERABILITY

Data must be interoperable within and among partners, and the issue of data interoperability has been covered in Section 4.5. This interoperability extends to data that is being made open and accessible under the FAIR principles.

5.3.4 INCREASE DATA REUSABILITY

In order to make the accessible data reusable, the following questions will be addressed:

- How will the data be licensed to permit the widest re-use possible?
- When will the data be made available for re-use?
    - If an embargo is sought to give time to publish or seek patents, specify why and how long this will apply, bearing in mind that research data should be made available as soon as possible.
- Is the data produced and/or used in the project useable by third parties, in particular after the end of the project?
    - If the re-use of some data is restricted, an explanation needs to be provided.
- How long is it intended that the data remains re-usable?
- Are data quality assurance processes described?

The corresponding answers will be included in the updated version of the DMP in the datasets descriptions.

6 DATA HANDLING AFTER THE PROJECT

This section describes how data will be stored, preserved and curated after the project ends.

For each identified dataset, the answers to the following questions will be addressed and included by the DC or DCs in the updated DMP:

- Retention/Destruction
  - What data must be retained/destroyed for contractual, legal, or regulatory purposes?
  - How long should the data be retained? 3-5 years, 10 years, 6 months after the Project or other suitable retention policy? As a general rule personal data shall be retained no longer than is necessary for the purpose.
  - What is the cost of any data retention and archiving?
- Long-term reuse
  - Does the data have long-term scientific, technical, social or business value?
  - What are the foreseeable direct uses of the data?
  - What are the foreseeable research uses for the data?
- Archiving
  - How will you be archiving the data?
    - Will you be storing it in an archive or repository for long-term access?
      - If not, how will you preserve access to the data?
  - Is a discipline-specific repository available?
- Preparation and documentation
  - How will you prepare data for preservation or data sharing? Will the data need to be anonymised/pseudonymised or converted to more stable file formats?
  - Are software or tools needed to use the data?
    - Will these be archived?
  - What documentation is also required, to make the archived data useful?
  - What is the cost of this preparation?

Once the datasets utilization is fully defined in the InterConnect project an update to the DMP will be issued, with the datasets description update and how datasets that have long-term value will be preserved and curated beyond the lifetime of the InterConnect project. Plans for preparing and documenting data for sharing and archiving will also be further outlined. They

will also indicate long-term third-party repositories or the resources and systems that will be used to enable the data to be curated effectively beyond the lifetime of the project.

7 PRIVACY

This section provides a summary of privacy considerations relating to the processing of personal data that is collected and used in the InterConnect project.

General overview of the applicable regulatory framework will be considered:

- **European Union**:
  - REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) – GDPR.
  - DIRECTIVE 2009/136/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws
  - European Data Protection Supervisor
  - European Data Protection Board
- **Portugal**: Law n.º 58/2019, of 8 August (LPD). Data Protection Authority: Comissão Nacional de Protecção de Dados – CNPD, R. de São. Bento, 148-3° 1200-821 Lisboa.
- **France**: Law n° 78-17 of January 6th, 1978. Data Protection Authority: Commission nationale de l'informatique et des libertés - CNIL, 3 place de Fontenoy, TSA 80715, 75334 Paris Cedex 07.
- **Germany**: Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680. Data Protection Authority: Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Husarenstraße 30, 53117 Bonn (http://www.bfdi.bund.de/).
- **Belgium**: Act on the protection of natural persons with regard to the processing of personal data. Data Protection Authority: Rue de la Presse, Drukpersstraat 35, 1000 Brussels.
- **Netherlands**: - Netherlands, Implementation ACT GDPR (*Uitvoeringswet Algemene Verordening Gegevensbescherming*) dated May 25, 2018

- **Italy**: The European Regulation 2016/679 has been implemented in Italy with: *"DECRETO LEGISLATIVO 10 agosto 2018, n. 101": "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679*"
    - In addition to the above mentioned, some rules of the "*decreto legislativo 196 del 2003: Codice in materia di protezione dei dati personali*" are still effective.
    - The competent Structure over Data issue is the independent Authority named: "Garante per la Protezione dei dati personali."
- **Greece**: Data privacy Legal framework; the Data Protection Authority: (Hellenic Data Protection Authority – HDPA), Kifissias 1-3, 115 23 Athens, Greece.

7.1 KEY ISSUES

All personal data processing within the project must comply with applicable law. The GDPR [5] has been in-force May 2018, so the Project considers that, except for specific issues raised by a partner, the applicable framework must comply with the GDPR. While all the partners are accustomed to working within the framework of their national law under the EU DP Directive, the GDPR introduces certain changes.

Accordingly, the partners will ensure that:

- All personal data processing must comply with the GDPR principles. These include fairness, lawfulness and transparency; purpose limitation; data minimisation; data quality; security, integrity and confidentiality.
- The basis for processing personal data within the project is the informed consent (express, specific) of data subjects, as established by the GDPR.
- For each activity that involves data collection, the DCs and DPs are clearly defined (see Table 5 to Table 9).
- For the release of any data that includes personal data, not only must the released data be anonymised, but also such opening of the data and subsequent processing must fall within the limits permitted by the GDPR (informed consent, or for permitted "further processing").
- Each partner will notify to the PDM and the DPC who is the person responsible for data protection within its organisation.
- While the project will carry out certain user profiling activities, these activities do not lead to automated decision that affect citizens but are inputs to applications and energy

efficiency technologies. Thus, the project considers that this type of profiling complies with Articles 5 and 22 of the GDPR.

- Record keeping of all personal data processing activities in compliance with GDPR.

7.2 GUIDELINES

The following guidelines are provided from the project's perspective while partners recognise that each entity must comply with their current and future privacy regulation as it applies to them, i.e. the guidelines focus on data protection implementation issues due to the interrelations of the partners and personal data within the scope of the project, not each partner's own compliance programme.

- For the purpose of being able to legally process and access and share data among project partners, a proper legal grounds will be defined for each demonstration site, to guide data collection and ensure that the data can be used and shared within the scope of the project.
- The project will not process any data from children nor any sensitive personal data.
- Security measures indicated with respect to each personal dataset must comply with applicable minimum measures set out by applicable law for the protection of personal data.
- Partners shall apply privacy by design principles in designing the applications that collect and process personal data.
- No data will be stored outside the European Economic Area (EEA).
- For the purpose of releasing any project data as open data, released data shall be fully anonymised, and the PDM, together with the DPC and the WPDMs, will study the most appropriate anonymization mechanism to implement.
- Any sharing of datasets outside the project partners must
    a) have the prior authorization of the respective DC or DCs and other parties involved in processing that data
    b) comply with applicable privacy law on data transfers (communication to third parties).
- Any data breaches, and any supervisory authority and data subject notifications, relating to project data, will be communicated to the PDM and to the DPC, who will promptly communicate these breaches to the relevant partners.

8 RESOURCES AND PLANNING

8.1 RESOURCES

The foreseen resources dedicated to implementing data management within the project in line with this plan and they are associated to the WPs where data collection may take place, as referred to earlier, as well as in the WP11 Project Management activities.

8.2 PLANNING

The calendar for implementing this data management plan is as follows:

Dates	Objectives	Comments
M8	Establish the Data Management Plan to the EC to establish the initial conditions and recommendations to be followed by the project	The DMP was planned to be delivered on M6 of the project but incurring delays led to the first version provided in this document to be delivered in M8
M9; M15; M21; M27; M33; M39; M45.	Update to project datasets	Regular updates every 6 months of the project datasets structures and data discrimination.
M12; M18; M24; M30; M36; M42; M48	Update to the DMP	Regular updates to the DMP in order to reflect updated information about the project data issues.

TABLE 4: DATA MANAGEMENT PLAN CALENDARIZATION

As mentioned in Table 4, the DMP will be a live document with regular updates, based on internal activities and discussions

9 OTHER ASPECTS

In this section, other aspects of data management in InterConnect including the ethics and IPR management are addressed.

9.1 ETHICAL ASPECTS

Given that certain parts of data processing in InterConnect may raise certain ethical or legal issues, with particular emphasis on data protection and privacy issues, a specific body was created to support the consortium dealing with them. The Ethics and Data Protection Committee (EDPC) is a body that assures the proper handling of the aspects related with data and ethics issues of the project. The EDPC is composed of Data Protection Officers (DPO) or Data Protection Responsible Persons (when a DPO is not formally designated) representing each of the 11 Work Package (WP) leaders as well as the leaders of each of the project 7 pilots. This committee will support the project consortium regarding any ethical questions and relevant data management issues in particular in what refers to personal data protection implications. In this context one of the responsibilities of EDPC is to monitor compliance with Data Protection Law and identify the Work Packages which may bring more serious concerns from a data protection law standpoint. The EDPC is led by the Data Protection Coordinator, the DPO of INESC TEC, Vasco Dias, whose email adress is: dpo@inesctec.pt

A more precise description of the Ethics and Data Protection Board can be found in section 2.

In effect most of the possible ethical implications of the project relate to the processing of personal data and user profiling, and subsequent data sharing. Specific deliverables dedicated to ethical and legal matters will be prepared and issued during the project.

For the purpose of this DMP, the following principles apply:

- Only personal data collected according to law may be processed by the consortium partners;
- Whenever informed consent is used as the legal grounds for processing, such consent shall be designed and collected in accordance with GDPR criteria, besides complying with international ethical requirements commonly accepted (v.g Helsinki Declaration) and furthermore, they shall also contemplate, as separate consents, data storage and sharing;
- Datasets created for the project may not be used for any other purpose than the project scientific goals;

All datasets must be anonymised, or at least pseudonymised, to the maximum extent possible.

9.2 INTELLECTUAL PROPERTY RIGHTS

The InterConnect Intellectual Property Rights (IPR) management strategy will be performed in a differentiated fashion in different stages of the project, as described below:

- **Grant agreement phase**: The consortium agreement (CA) signed by all the consortium partners will specify the terms and conditions pertaining to ownership, access rights, exploitation of background and foreground, in compliance with the grant agreement and Regulation n°1290/2013 of December 11th, 2013. The consortium agreement will be based on the DESCA (Development of a Simplified CA Horizon 2020 Model CA with the necessary adaptations considering the specific context and the parties involved in InterConnect. In the CA, all partners will identify their pre-existing knowledge (background).
- **Project start:** As part of WP10, the project will establish a strong intellectual property (IP) management position directly at project outset, that will have a beneficial impact upon the project's success in exploiting the project outputs and products. This will allow the consortium and individual members to protect the inventions and knowledge generated "pre", "during" and "post-project", and will support the exploitation planning process, and the communication and dissemination activities.
- **During project:** As part of the exploitation planning, there will be a mapping exercise to identify existing patents or potentially overlapping IPR, together with an assessment of the new knowledge generated during the project. Following H2020 rules, knowledge will be the property of the partner (or joint property of the partners) generating the knowledge itself. Each partner will grant access rights to relevant background and foreground intellectual property and know-how to other partners so that they will be able to exploit their own intellectual property. Access to background will be on fair and reasonable terms.
- **Post-project:** IPR protection options will be formulated in the CA in line with the business plan defined in this proposal and further developed within the Exploitation Plan in WP10.

10 CONCLUSION

The Data Management Plan (DMP) is an extremely important document that regulates the procedures to be adopted by the InterConnect project considering data collection and data use within the different project activities.

This document presents the first version of the DMP and it typifies the data to be collect in the project as well as the handling and sharing procedures in WPs and Pilots. One important aspect is that data, as all information exchanged within the project, needs to be exchanged safely, securely, anonymized and interoperable.

As this stage several contributions from consortium partners were collected and validated by partners and the EDPC through a template document. Several round were undertaken between the EDPC and partners in order to clarify as detailed as possible the issues related to data management. The contributions made on the template are presented in the Annex 1 – Data Issues Identification.

Updated versions of the DMP as well as on the data structures and issues will be provided on a biannually fashion, or whenever justified.

11 QUALITY MONITORING AND ASSURANCE

The project consortium will implement measures of quality control to ensure continuous compliance and a high quality of work and results. These measures will establish format guidelines that need to be followed when producing output and establish review and correction procedures for formal deliverables.

The measures primarily concern the implementation of:

a) standardised style and content templates for internal and external project output (deliverables, reports, memorandums);
b) Reporting: Review, acceptance and feedback procedures for the deliverables;
c) Monitoring mechanisms.

Monitoring is put in place to support better performance and greater accountability as well as to ensure clear and accurate reporting on the results achieved and the progress made. Each activity's budgets, milestones and output indicators are the basis for active project monitoring and portfolio management. All activities are reviewed based on clear criteria on concrete milestones, which are listed in the table below.

Monitoring will be conducted against these standards defined by InterConnect for quality assurance:

- Monitoring of process: deviation of planed milestones completion < one month.
- Monitoring of financials: deviation from the initial cost foreseen less than 2%.
- Monitoring of results: timely and complete submission of deliverables; punctual delivery of reports.
- Monitoring of compliance: no audit requests from the EC; fulfilment of grant and contract requirements.

The deliverable D11.3 Quality and risk mitigation plan will provide more detailed information about quality and monitoring assurance.

REFERENCES

EXTERNAL DOCUMENTS

[1] Guidelines on FAIR Data Management in Horizon 2020, July 2016 [ONLINE]

[2] General Annex K of the Horizon 2020 Work Programme 'K. Actions involving financial support to third parties' [ONLINE]

[3] EC Annotated Model Grant Agreement 2019 [ONLINE]

INTERCONNECT DOCUMENTS

[1] InterConnect Grant Agreement number 857237.

ANNEX 1 – DATA ISSUES IDENTIFICATION

In this annex are presented the identification of data issues carried out by the project partners using the template table presented in section 3.2.2 from [1] .

1. INESC

DMP component	Issues to be addressed	Explanation
1. Data summary	• State the purpose of the data collection/generation • Explain the relation to the objectives of the project • Specify the types and formats of data generated/collected • Specify if existing data is being re-used (if any) • Specify the origin of the data • State the expected size of the data (if known) • Outline the data utility: to whom will it be useful	Scope WP2: • Metadata related with the provision on interoperability capabilities for software components (e.g., device identification, device features, device usage profiling, etc) Scope WP3: • Data model for an appliance or device (e.g., physical characteristics, usage data, etc.) • Data and functionalities of Customer/Building/Home Energy Management Systems (CEMS, BEMS, HEMS) Scope WP4: • Electric grid information (topology, operation scenarios) • SCADA systems data models • Data models for devices and systems from the electric grid • Application of standardized data format such as USEF and CIM Scope: WP5 • Identifying and categorizing all digital platforms, services and ICT interfaces from consortium partners; Identify and catalogue data models and data flows between digital platforms and external services (if existent) and devices; • Power the integration between the interoperability framework with all external borders of the digital platforms and services that end-up being selected for pilot installation. Regarding the cascade funding stage, this could be done with external parties, selected to enrol the project via that way, only for the purpose of providing interoperability. • Most digital platforms already provide standardized data models and use of ICT infrastructure. These shall be reused (e.g., JSON-LD, XML, APIs, SAREF endpoints and data model, etc) • The origin could be a digital platform, or service, comprised or isolated from a digital platform or device, or conceptual constructions discussed during project meetings;

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant agreement No 857237

		• Size is not possible to quantify at this stage; • Data shall be used to sponsor and ensure interoperability of services within the scope of the interoperability framework to be developed and deployed. Ultimately it will be of utmost relevance to all consortium partners and stakeholders cleared through the cascade funding stage; Scope WP6 and WP7: • Data collected in domestic and tertiary buildings from sensing devices and systems • Data collected from the grid operation from DMS • Energy use data (e.g., energy consumption, renewable generation, etc.) • Non-energy use data (e.g., comfort, convenience, air quality, etc.) Scope WP8: • Data models and digital platforms made available to other partners of the project to implement solutions and services in the scope of the Support to Third Parties
2. FAIR Data 2.1. Making data findable, including provisions for metadata	• Outline the discoverability of data (metadata provision) • Outline the identifiability of data and refer to standard identification mechanism. Do you make use of persistent and unique identifiers such as Digital Object Identifiers? • Outline naming conventions used • Outline the approach towards search keyword • Outline the approach for clear versioning • Specify standards for metadata creation (if any). If there are no standards in your discipline describe what type of metadata will be created and how	Scope WP3: • Services will be made discoverable along with their features (e.g., metadata, ontology conform data); Scope WP5: • All metadata related with services and APIs available to allow its discovery from the interoperability framework, until the border naturally exposed when crossing home/building/grid/cloud (or deployment) realms; • Not possible to identify at this stage; • Not possible to particularize at this stage, but with great confidence will be compliant with SAREF and/or significant SAREF4 – X ontologies; • Ontology specific; • Versioning will be implemented and map as much as possible versioning for the software component from where it is originated; • Metadata will conform to either ontology specific recommendations and/or industry relevant ICT standards;

2.2 Making data openly accessible	• Specify which data will be made openly available? If some data is kept closed provide rationale for doing so • Specify how the data will be made available • Specify what methods or software tools are needed to access the data? Is documentation about the software needed to access the data included? Is it possible to include the relevant software (e.g. in open source code)? • Specify where the data and associated metadata, documentation and code are deposited • Specify how access will be provided in case there are any restrictions	Scope WP3: • At this time is unclear. Services will be made available for use within the interoperability features. Clear awareness on what datasets and data will be exposed will only be available ahead. (e.g., flexibility data, aggregated service data, service metadata) Scope WP5: • At this time it is not clear. It is expected that business and/or corporate specific mechanisms concerning the digital platforms from partner could/would be maintained proprietary, but metadata allowing to service features and discoverability strictly essential to ensure interoperability will be made available; • REST API and ICT interfaces such as that will be used. The extent and what exactly they will expose (families of services, or the actually services exposed via the digital platforms) is still up for discussion. Documentation will be in place together with digital aids to sponsor the adoption of interoperability; • Documentation will be deposited in the project repository which could be opened or not according to the consortium decisions. The digital aids for adoption will be made digitally available after authentication mechanisms are validated during development. It is expected that open data to sponsor integration of new platforms will be made available ahead; • Restrictions will be put in place if needed, but they cannot be identified at this stage. Scope WP6 and WP7:
2.3. Making data interoperable	• Assess the interoperability of your data. Specify what data and metadata vocabularies, standards or methodologies you will follow to facilitate interoperability. • Specify whether you will be using standard vocabulary for all data types present in your data set, to allow inter-disciplinary interoperability? If not, will you provide mapping to more commonly used ontologies?	Scope WP3: • All data formats from devices (ex.) and systems (e.g., HEMS, BEMS, CEMS) will have interoperable interfaces based on SPINE, SAREF, et.c Scope WP4: • Data formats will be based on the most important standards in the field (e.g. IEC 61850) which rely on open format such as CIM, USEF, etc. Scope WP5: • All interoperability will be achieved via the ontology identified within WP2. Assessing interoperability is also foreseen to be aided via distributed ledger technologies to be put in place by the project; • YES. Scope WP6 e WP7:

		• Services will need to conform to the ontology interface, sharing their capabilities and features. • At this time is unclear how data can be disclosed, however anonymization strategies may be employed to allow data from the pilots to be publicly available.
2.4. Increase data re-use (through clarifying licences)	• Specify how the data will be licenced to permit the widest reuse possible • Specify when the data will be made available for re-use. If applicable, specify why and for what period a data embargo is needed • Specify whether the data produced and/or used in the project is useable by third parties, in particular after the end of the project? If the re-use of some data is restricted, explain why • Describe data quality assurance processes • Specify the length of time for which the data will remain re-usable	Scope WP2, WP3, WP4, WP5, WP6 and WP7: • Licencing will be done according to the GA and the CA firmed between the consortium partners and further measures will be put in place, trying to convene the Intellectual Property workshop carried out by INESCTEC to the consortium in line with the exploitation plan; • Can't be detailed if and when at this stage. • YES. Via conforming to the ICT APIs based on the exposed ontology (SAREF) foreseen;
3. Allocation of resources	• Estimate the costs for making your data FAIR. Describe how you intend to cover these costs • Clearly identify responsibilities for data management in your project • Describe costs and potential value of long-term preservation	Scope WP5: • Costs will be disclosed within Wp2 to Wp5 and Wp7; • Data protection will be handled by the partners who will designate responsible persons form data management, coordinated in each WP by the relative leader; • In what specifically relates to personal data, the entities DPO's (compliance officers or equivalent) will intervene whenever required within the consortium via the Ethics and Data Protection Committee. Moreover, a data sharing agreement between project partners will be established, further to what is provided in the CA, which will rule on matters concerning personal data handling and sharing among the project partners. • Long-term preservation will be judged ahead;
4. Data security	• Address data recovery as well as secure storage and transfer of sensitive data	Scope WP2, WP3, WP4, WP5, WP6, WP7: • Data security will be ensured to keep confidential document strictly confidential (inclusing concepts, data sources, data sets, etc) with redundant and fault-tolerant mechanisms;

		• During project and pilot deployment, security and privacy compliance for operational data will be met according to the specific components where data are generated and/or according to its destination, trying as much as possible to only disclose data that is strictly necessary for complying with the overall goals to which the data transfer is associated.
5. Ethical aspects	• To be covered in the context of the ethics review, ethics section of DoA and ethics deliverables. Include references and related technical aspects if not covered by the former	Scope all WPs: • Possible ethical, data protection and privacy issues shall be identified and assessed by the partners with the support of the EDPC, which will revise and comment on the DPM final drafts. • A data sharing agreement will be settled by the partners comprising principles and rules concerning the handling and sharing of personal data, in compliance with the applicable legal framework. • The necessity of a DPIA shall be assessed by the partners. • Identify and address existing international data transfers within the consortium
6. Other	• Refer to other national/funder/sectorial/departmental procedures for data management that you are using (if any)	• Specific procedures are set for the data exchange between countries in the Consortium Agreement • There is a unanimous agreement between partners, including those for third countries, to follow the guidelines and regulations set in the GDPR • Data Protection Law on 9 November 2018 (published in the Official Gazette of the Republic of Serbia, no. 87/2018) as an official regulation toward the data protection equivalency to the EU regulation. Its content is largely harmonized with the GDPR. It is fully effective as of 21 August 2019

2. EEBUS

Did not answer or was not able to complete the information in time.

3. TNO

DMP component	Issues to be addressed	Explanation
1. Data summary	• State the purpose of the data collection/generation • Explain the relation to the objectives of the project • Specify the types and formats of data generated/collected • Specify if existing data is being re-used (if any) • Specify the origin of the data • State the expected size of the data (if known) • Outline the data utility: to whom will it be useful	**The purpose of the data collection/generation:** In InterConnect, TNO will collaborate with VolkerWessels (NL pilot leader) in the Dutch pilot in which data collected from a newly built residential building in Eindhoven will be used in the project for validation purposes. The validation will concern innovations and systems developed in InterConnect. **The relation to the objectives of the project (*objectives should be listed centrally in this doc)*:** The data collected by TNO in InterConnect relates to main objective 2 and 3 of the project: **Objective 2:** Demonstrate through large -scale pilots the implementation of a digital marketplace composed by different platforms and showcase the satisfaction of energy users needs with cost-effective solutions, allowing different market agents to create their value, and simultaneously **Objective 3:** Ensure high levels of cybersecurity and data privacy. Co-creation involving citizens to design energy and non-energy services and applications that foster the active participation in new business models and grid operation, while ensuring comfortable, efficient, sustainable and healthier living environments **Specify the types and formats of data that can be generated/collected:** • Monitoring of electricity, cooling, heating and Domestic Hot Water consumption at residential property and Building Heating Network level • Indoor Temperature and presence of residents • Working conditions of heat pumps and solar systems • Comfort profiles of occupants • User and stakeholder needs and requirements • Surveys and questionnaires • Metadata on interoperability **Specify if existing data is being re-used (if any):**

		We do not plan to directly use any data from prior activities. But maybe we experiment first with data from an earlier VolkerWessels H2020 Triangulum project. **Specify the origin of the data:** • Device level (white goods, heat pumps, inverters,…) • Building Energy Management Systems • Sensors at residential level, DHN and boiler room level • Residents (collected through surveys or apps) • Additional third parties services (weather data,…) **The expected size of the data (if known):** • The dataset that TNO and the Dutch pilot will be working with is derived from approximately 100 households. **Outline the data utility: to whom will it be useful:** • Site stakeholders (residents, iCity) to validate the site‘s business case • Project stakeholders to validate the project’s objectives
2. FAIR Data 2.1. Making data findable, including provisions for metadata	• Outline the discoverability of data (metadata provision) • Outline the identifiability of data and refer to standard identification mechanism. Do you make use of persistent and unique identifiers such as Digital Object Identifiers? • Outline naming conventions used • Outline the approach towards search keyword • Outline the approach for clear versioning	The definition of metadata is one of the objectives of work package 2 and task 2.4 which is led by TNO. As far as FAIR data management is concerned, the guidelines of the Go Fair initiative will be considered and applied where possible. At this stage (April 2020) a fully detailed plan is not yet available. For now, we refer to https://www.go-fair.org/fair-principles

	• Specify standards for metadata creation (if any). If there are no standards in your discipline describe what type of metadata will be created and how	
2.2 Making data openly accessible	• Specify which data will be made openly available? If some data is kept closed provide rationale for doing so • Specify how the data will be made available • Specify what methods or software tools are needed to access the data? Is documentation about the software needed to access the data included? Is it possible to include the relevant software (e.g. in open source code)? • Specify where the data and associated metadata, documentation and code are deposited • Specify how access will be provided in case there are any restrictions	• To be discussed and decided. Personal data will not be made available in an open fashion in accordance with GDPR as well as any national legislation that applies. • Data that will be made available will be accessible through technical interfaces such as, but not limited to, API's. • Methods and software tools needed to access data are to be detailed at a further stage. Documentation will be made available in due time. • Where the data and associated metadata, documentation and code are deposited will also be considered at a later stage. • Access in case there are any restrictions to data will be dealt with on a case-by-case basis on request and after approval of relevant stakeholders.
2.3. Making data interoperable	• Assess the interoperability of your data. Specify what data and metadata vocabularies, standards or methodologies you will follow to facilitate interoperability. • Specify whether you will be using standard vocabulary for all data types present in your data set, to allow inter-disciplinary interoperability? If not, will you provide mapping to more commonly used ontologies?	Interoperability and the definition of metadata vocabulary /ontology is one of the main objectives of work package 2 and task 2.4, and the pilot site managed by VolkerWessels/iCity will implement the semantic interoperability solution defined in WP2.

2.4. Increase data re-use (through clarifying licences)	• Specify how the data will be licensed to permit the widest reuse possible • Specify when the data will be made available for re-use. If applicable, specify why and for what period a data embargo is needed • Specify whether the data produced and/or used in the project is usable by third parties, in particular after the end of the project? If the re-use of some data is restricted, explain why • Describe data quality assurance processes • Specify the length of time for which the data will remain re-usable	To be discussed and decided in a later phase.
3. Allocation of resources	• Estimate the costs for making your data FAIR. Describe how you intend to cover these costs • Clearly identify responsibilities for data management in your project • Describe costs and potential value of long-term preservation	A more detailed cost estimation will be provided at a later stage, but will adhere to the following structure. I. Costs for data collection II. Costs for data documentation III. Costs for data storage IV. Costs for data access and security V. Costs for data preservation VI. Costs for data availability and reuse VII. Overall (OPEX) Responsibilities for data management will most probably be VolkerWessels for the pilot activities that have a direct involvement of TNO.
4. Data security	• Address data recovery as well as secure storage and transfer of sensitive data	TNO has a detailed set of security policies and regulations, in which a wide range of topics is addressed. These include the following aspects and can be provided in full detail on request: Physical regulations • Fysiek.01 - FSCC-locations and Verboden Plaatsen

		• Fysiek.02 - Access requirements and visitor regulations at TNO locations • Fysiek.03 - Badges • Fysiek.04 - Visit Authorisation Request (VAR) • Fysiek.05 - Physical storage • Fysiek.06 - Photography and filming Data management • Informatie.01 - Clean Desk regulation • Informatie.02 - Labelling of classified information • Informatie.03 - Classifications and their application • Informatie.04 - Handling matrix • Informatie.04A - Handling matrix • Informatie.04A1 - Handling matrix TNO Classifications • Informatie.04A2 - Handling matrix Government Classifications • Informatie.05 - Transport and dispatch Information Technical measures • IT.01 - Conditions for connection to the TNO network • IT.02 - Acceptable Use Policy • IT.03 - Account Logon Policy • IT.04 - Anti-Virus-software IT.05 - Back-up and retention periods • IT.06 - IT operating assets • IT.07 - Management • IT.08 - Internet-accessible systems policy • IT.09 - IT continuity management • IT.10 - Cryptographic control measures • IT.11 - Data storage • IT.12 - Use of IT resources

		• IT.13 - Approved means of encryption • IT.14 - Mail forwarding IT.15 - Mobile IT devices • IT.16 - Classification of IT services • IT.17 - Classification of IT documents • IT.18 – Screen lock • IT.19 - Software maintenance • IT.20 - TLS Policy • IT.21 - IT access security • IT.22 - Granting powers in IT systems • IT.23 - Password policy • IT.24 - Working outside of TNO locations IT.25 - Domain names and Certificates for websites Organisational policies • Organisatie.01 - Risk countries • Organisatie.02 - Classification of facility (IT) systems • Organisatie.03 - Subcontractor • Organisatie.04 - Security incident handling process Personnel policies • Personeel.01 - International employee, intern, PhD candidate or temporary employee • Personeel.02 - List of Positions Involving Confidentiality • Personeel.03 - Placement of an employee without Dutch nationality on a Dutch State secret project • Personeel.04 - Travelling to risk countries • Personeel.05 - Request for Visit (RfV) • Personeel.06 - Starting with a VOG while awaiting a VGB • Personeel.07 - Certificate of Good Conduct (VOG) • Personeel.08 - Declaration of No Objection (VGB)

		Privacy • TNO privacy policy • TNO privacy statement https://www.tno.nl/en/about-tno/contact/corporate-legal/privacy-statement • TNO procedure personal data breaches • TNO data protection impact assessment procedure • TNO has appointed a DPO (data protection officer)
5. Ethical aspects	• To be covered in the context of the ethics review, ethics section of DoA and ethics deliverables. Include references and related technical aspects if not covered by the former	Will be covered in the context of the ethics review, the ethics section of the DoA and ethics deliverables.
6. Other	• Refer to other national/funder/sectoral/departmental procedures for data management that you are using (if any)	In accordance with departmental procedures, TNO has a procedure to review all research that involves research participants and/or their personal data by a internal HR review committee.

4. VITO

DMP component	Issues to be addressed	Explanation
1. Data summary	• State the purpose of the data collection/generation • Explain the relation to the objectives of the project • Specify the types and formats of data generated/erconcollected	**The purpose of the data collection/generation:** **The relation to the objectives of the project (*objectives should be listed centrally in this doc)*:** The data collected at the Cordium pilot site will be used to implement/validate the main objective n°2, and specific objectives n°2, n°3, n°4, n°5, n°7 (by reusing services). **Specify the types and formats of data generated/collected:** • Monitoring of electricity, cooling, heating and DHW consumption at dwelling and DHN level

	• Specify if existing data is being re-used (if any) • Specify the origin of the data • State the expected size of the data (if known) • Outline the data utility: to whom will it be useful	• Indoor Temperature and presence at dwelling level • Working conditions of heat pumps and PV • Comfort profiles of occupants • User and stakeholder needs and requirements • Surveys and questionnaires • Metadata on interoperability **Specify if existing data is being re-used (if any):** Not at this time. **Specify the origin of the data:** • Device level (whitegoods, HP,…) • BEMS at dwelling level • BMS at site level • Substation • Sensors at dwelling level, DHN and boiler room level • Residents (surveys) • Additional third parties services (weather data,…) **The expected size of the data (if known):** • Unknown **Outline the data utility: to whom will it be useful:** • Site stakeholders (residents, Cordium) to validate the site's business case • Project stakeholders to validate the project's objectives
2. FAIR Data 2.1. Making data findable, including provisions for metadata	• Outline the discoverability of data (metadata provision) • Outline the identifiability of data and refer to standard identification mechanism. Do you make use of persistent and unique identifiers such as Digital Object Identifiers? • Outline naming conventions used	The definition of metadata is one of the main objectives of work package 2, and the pilot sites managed by VITO will implement the semantic interoperability insolution defined in WP2.

	• Outline the approach towards search keyword • Outline the approach for clear versioning • Specify standards for metadata creation (if any). If there are no standards in your discipline describe what type of metadata will be created and how	
2.2 Making data openly accessible	• Specify which data will be made openly available? If some data is kept closed provide rationale for doing so • Specify how the data will be made available • Specify what methods or software tools are needed to access the data? Is documentation about the software needed to access the data included? Is it possible to include the relevant software (e.g. in open source code)? • Specify where the data and associated metadata, documentation and code are deposited • Specify how access will be provided in case there are any restrictions	To be discussed and decided.
2.3. Making data interoperable	• Assess the interoperability of your data. Specify what data and metadata vocabularies, standards or methodologies you will follow to facilitate interoperability. • Specify whether you will be using standard vocabulary for all data types present in your data set, to allow inter-disciplinary	Interoperability and the definition of metadata vocabulary /ontology is one of the main objectives of work package 2, and the pilot sites managed by VITO will implement the semantic interoperability solution defined in WP2.

	interoperability? If not, will you provide mapping to more commonly used ontologies?	
2.4. Increase data re-use (through clarifying licences)	• Specify how the data will be licenced to permit the widest reuse possible • Specify when the data will be made available for re-use. If applicable, specify why and for what period a data embargo is needed • Specify whether the data produced and/or used in the project is useable by third parties, in particular after the end of the project? If the re-use of some data is restricted, explain why • Describe data quality assurance processes • Specify the length of time for which the data will remain re-usable	To be discussed and decided.
3. Allocation of resources	• Estimate the costs for making your data FAIR. Describe how you intend to cover these costs • Clearly identify responsibilities for data management in your project • Describe costs and potential value of long-term preservation	**Estimate the costs for making your data FAIR:** • One of the main objective of the project is to define an interoperable marketplace toolbox and demonstrate this in the project pilots, the cost are covered by the objectives of the project. **Clearly identify responsibilities for data management in your project:** • **Local social housing company Cordium:** o User and tenant interaction (informing, collecting feedback) – Cordium has a social service that interacts with the tenants, this channel can be used to inform them and to gather feedback. • **VITO:** o Monitoring, processing and data analysis o Data storage during project lifetime **Describe costs and potential value of long-term preservation:** • To be analysed and estimated**.**
4. Data security	• Address data recovery as well as secure storage and transfer of sensitive data	The following technical and organizational measures are in place at VITO: Information Security Policies • VITO has a set of formal and up-to-date policies for information security defined by the senior

		management, published and communicated on a regular basis to all employees and relevant external parties. *(Measure under construction - H1 2019)* • The policies for information security are reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness. *(Measure under construction - H1 2019)* Organization of Information Security • All information security responsibilities are defined and allocated in line with the information security policies (DPO, decision-making structures, etc.) • VITO has a procedure stipulating the appropriate contacts with relevant authorities and external parties, concerning information security, whenever. (f.e. an incident procedure conforms the GDPR or a procedure conform the consulting of the DPA concerning a DPIA.) • VITO maintains appropriate contacts with special interest groups or other specialist, security forums and professional associations. The goals of such contacts are among others staying up-to-date, developing best practices, getting informed quickly when new threats arrive, getting access to specialized services and exchanging information and experiences. Human Resource Security • The contractual agreements with employees and contractors state the responsibilities for information security for both parties. The employee contract stipulates how to handle confidential information and makes mention of 3 levels of confidentiality. Furthermore, standard clauses are used (f.e. for Ph.D. students) as well as data processing agreements and NDA's (in case of external employees related to sub-processors). • All employees of the Organization and relevant contractors are aware of the risks and the importance of information security. On a regular basis, they receive appropriate awareness education among others via Lunch talks, newsletters (Channel V), intranet and a SharePoint site where information security aspects are discussed. • VITO has a formal and communicated disciplinary process in place to take action against employees who have, willingly or unwillingly, committed an information security breach. • Information security responsibilities and duties that remain valid after termination or a change of employment are defined, made enforceable, and communicated to the employee or contractor. Asset Management • An inventory of all assets associated with information processing, with exception of a few specific scientific applications, is stored in a CMDB (Configuration management database). • All assets have an owner included in the CMDB. • A standard acceptable use policy is being established, containing the rules for the storage, transfer, return,… of information depending on the level of data classification. *(Measure under construction - H1 2019)* Access control • VITO has established a formal access control policy based on functional business and information security requirements. It is documented and implemented. More details are described in the standard acceptable use policy. • Network authentication is active on all VITO networks, both wired and wireless. • Formal processes are implemented for user registration and de-registration to enable assignment of

		access rights. These are always started from an HR-procedure and are mostly subsequently executed in an automated way. • Access rights of all employees and external parties are deleted (or made inactive) at the termination of their contract or modified when their role in the organization changes. • Controlled access is applied systematically. Strong authentication and two-factor-authentication (f.e. on laptops with client-certificates) is already in use and will continue to be further implemented. • A password management system is operational for VITO Active Directory accounts and ensures high-quality passwords Physical and Environmental Security • A physical security perimeter is defined and used to protect areas that contain either sensitive or critical information and information processing facilities. • Secure areas are protected by appropriate entry controls to ensure that only authorized personnel are allowed access. • With very few exceptions, all offices are physically secured. Access to the datacenters is strictly supervised. • Physical protection against natural disasters, malicious attacks or accidents is designed and applied. • Equipment is protected from power failures and other disruptions caused by failures in supporting utilities. • Procedures for working in secure areas are designed and applied. • Power and telecommunications cabling carrying data or supporting information services are protected from interception, interference or damage. Cables are physically protected and there is a ClearPass-tool determining the access to the correct VLAN. • All equipment containing storage media shall be verified to ensure that any sensitive data has been removed or securely overwritten prior to disposal or re-use. More details are described in the standard acceptable use policy. Operations Security • The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance. • To minimize the risk of malware infections, tools are used like Firewalls, anti-virus-tools, application security management/access policy management tools, and network access management. • VITO has documented procedures on backup & restore specifying that backup copies of information, software and system images are taken and tested regularly in accordance with an agreed backup policy. Security of the Communication • All networks are secured. • Network segregation is configured via VLANs. • Precise procedures for security of information in transit will be further described in the standard acceptable use policy. *(Measure under construction - H1 2019)* • In case of information exchange with third parties, confidentiality clauses are added in the contract (like NDA's and data processing agreements in accordance with the GDPR). System Acquisition, Development, and Maintenance • The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.

		• The information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification. Encrypted connections are always used, like HTTPS or SFTP. • When operating platforms are changed, business-critical applications shall be reviewed and tested to ensure there is no adverse impact on Organizational operations or security. • Modifications to software packages are driven by request from the Business and implemented via SCRUM in a controlled way. Supplier Relationships • Information security requirements for mitigating the risks associated with supplier's access to the Organization's assets shall be agreed with the supplier and documented. This happens systematically – for GDPR compliance – for suppliers who operate as a data processor. For other suppliers, this is done whenever necessary. • VITO regularly monitors, reviews and audits supplier service delivery. • On a regular basis, there are meetings with the most important suppliers to discuss their service delivery Information Security Incident Management • VITO has formal rules for classifying an incident as a data breach or as a severe data breach in accordance with the GDPR. • VITO has a formal procedure for taking the necessary actions and reporting in case of an incident or data breach, in accordance with the GDPR. The responsibilities and concrete actions are defined in order to quickly react in an effective and structured way. This is communicated to the management, the data subjects, and the DPA, in accordance with applicable laws and regulations.
5. Ethical aspects	• To be covered in the context of the ethics review, ethics section of DoA and ethics deliverables. Include references and related technical aspects if not covered by the former	To be checked.
6. Other	• Refer to other national/funder/sectorial/departmental procedures for data management that you are using (if any)	To be checked with DPO.

5. EDPD

DMP component	Issues to be addressed	Explanation
1. Data summary	• State the purpose of the data collection/generation • Explain the relation to the objectives of the project • Specify the types and formats of data generated/collected • Specify if existing data is being re-used (if any) • Specify the origin of the data • State the expected size of the data (if known) • Outline the data utility: to whom will it be useful	• Data collection will be gathered, in compliance with GDPR Regulation, from around 250 LV customers (Load curve diagram, location and appliances assets). • Sensitive or exclusive data from grid network and individual customers location will not be made available to Interconnect Partners. • If data this falls under a) of n. º 1 of article 6 a freely, specific, informed and unambiguous consent from each LV participant/customers stating its agreement for processing its personal data for the stated purposes will be gathered. • The participation in Interconnect project by LV customers will be voluntary and will in principle be in effect for the all duration of the Project. • All LV data will be strictly in compliance with what is stated in articles 12-23 of the GDPR. • If necessary Partners involved in this exchange will sign an NDA. • In principle, there will not be a re-use of data, unless the customers to be involved in the InterConnect project were previously involved in H2020 projects or any other national initiative. Notwithstanding, those considerations will be expressly taken in consideration on possible partner´s NDAs or customers´ consent. • Data provided in interconnect Project will be useful to develop to enable flexibility schemes among different stakeholders, with particular interest to the development of agnostic and data compliant mechanism to interface system operators with active customers.
2. FAIR Data 2.1. Making data findable, including provisions for metadata	• Outline the discoverability of data (metadata provision) • Outline the identifiability of data and refer to standard identification mechanism. Do you	• Not possible to identify at this stage;

	make use of persistent and unique identifiers such as Digital Object Identifiers? • Outline naming conventions used • Outline the approach towards search keyword • Outline the approach for clear versioning • Specify standards for metadata creation (if any). If there are no standards in your discipline describe what type of metadata will be created and how	
2.2 Making data openly accessible	• Specify which data will be made openly available? If some data is kept closed provide rationale for doing so • Specify how the data will be made available • Specify what methods or software tools are needed to access the data? Is documentation about the software needed to access the data included? Is it possible to include the relevant software (e.g. in open source code)? • Specify where the data and associated metadata, documentation and code are deposited • Specify how access will be provided in case there are any restrictions	• In principle data might be made available via different protocols (MODBUS, RS485, …), API's or via FTP folder with the necessary security procedures fill adequate to be in compliance with the GDPR regulation.
2.3. Making data interoperable	• Assess the interoperability of your data. Specify what data and metadata vocabularies, standards or methodologies you will follow to facilitate interoperability.	• Still not available

	• Specify whether you will be using standard vocabulary for all data types present in your data set, to allow inter-disciplinary interoperability? If not, will you provide mapping to more commonly used ontologies?	
2.4. Increase data re-use (through clarifying licences)	• Specify how the data will be licenced to permit the widest reuse possible • Specify when the data will be made available for re-use. If applicable, specify why and for what period a data embargo is needed • Specify whether the data produced and/or used in the project is useable by third parties, in particular after the end of the project? If the re-use of some data is restricted, explain why • Describe data quality assurance processes • Specify the length of time for which the data will remain re-usable	• In principle, no data will be re-used
3. Allocation of resources	• Estimate the costs for making your data FAIR. Describe how you intend to cover these costs • Clearly identify responsibilities for data management in your project • Describe costs and potential value of long-term preservation	• Issue not yet closed.
4. Data security	• Address data recovery as well as secure storage and transfer of sensitive data	• It is not foreseen at the moment disclosure of sensitive data • In principle and if necessary a DPIA will be made.

5. Ethical aspects	• To be covered in the context of the ethics review, ethics section of DoA and ethics deliverables. Include references and related technical aspects if not covered by the former	• Possible ethical, data protection and privacy issues shall be identified and assessed in accordance with GDPR and transmitted to the Consortium via EDPC
6. Other	• Refer to other national/funder/sectorial/departmental procedures for data management that you are using (if any)	• All data procedures will be made strictly in compliance with GDPR Regulation.

6. VIZLORE FOUNDATION

DMP component	Issues to be addressed	Explanation
1. Data summary	• State the purpose of the data collection/generation • Explain the relation to the objectives of the project • Specify the types and formats of data generated/collected • Specify if existing data is being re-used (if any) • Specify the origin of the data • State the expected size of the data (if known) • Outline the data utility: to whom will it be useful	• Cataloguing all available and interoperable platforms, services and endpoints in the InterConnect ecosystem. Monitoring performance of the interoperability enablers developed in the WP5 and applied to the project pilots. • Implementation of interoperability framework for digital platforms, services and devices is key objective of the project. • Resource and service description metadata (formats like RDF, XML, JSON), performance logs collected by digital platforms, services, devices, interoperability enablers (APIs, service store, orchestrator, P2P framework). Data will be collected in different formats depending on monitored solution (i.e. JSON, XML, Common Log Format etc.). • To be decided with owners of the interoperable resources • Data origin are resource providers (providing metadata describing their interoperable resources) and log systems and custom performance monitoring enablers on digital platforms, service operators, devices and interoperability enablers developed within the project.

		• Unknown precise size at the moment. The metadata describing the resources and services will be in range of KB. The system and process log data size will depend on the size of the instances (instances of reference architecture) and their number. The strategy is to utilize cloud platform with scalable database so that the disk/storage and DB size can scale with the number of system instances. Strategy for analysing log data will be derived so that log data for a defined period are stored (i.e. 2 months) while analysed log data are archived in a separate data archive. • Used for improving performance of the interoperability enablers generated within the project and made available to all project partners and 3rd party integrators. Providing overview of all interoperable resources and endpoints in unified way.
2. FAIR Data 2.1. Making data findable, including provisions for metadata	• Outline the discoverability of data (metadata provision) • Outline the identifiability of data and refer to standard identification mechanism. Do you make use of persistent and unique identifiers such as Digital Object Identifiers? • Outline naming conventions used • Outline the approach towards search keyword • Outline the approach for clear versioning • Specify standards for metadata creation (if any). If there are no standards in your discipline describe what type of metadata will be created and how	• Metadata will be provided for key interoperable resources and made available and discoverable through REST APIs and web dashboards developed within the project. • We will investigate appropriate approaches for data and resources identification. • Naming conventions will be in line with **SAREF ontology** • Applied ontology will guide specification of search parameters • Versioning of datasets will be provided based on standard approaches. • Metadata will be specified in line with SAREF ontology, other possibilities will be explored as well (standards and best practices for IoT and smart grid).
2.2 Making data openly accessible	• Specify which data will be made openly available? If some data is kept closed provide rationale for doing so • Specify how the data will be made available	• Currently the plan is to provide metadata describing interoperable resources openly available. Datasets related to interoperability performance logs will be made openly available in agreement with data owners. • Through REST APIs, other options will be investigated.

	• Specify what methods or software tools are needed to access the data? Is documentation about the software needed to access the data included? Is it possible to include the relevant software (e.g. in open source code)? • Specify where the data and associated metadata, documentation and code are deposited • Specify how access will be provided in case there are any restrictions	• Web service capable of accessing REST APIs with JWT authorization mechanism. Other software tools might also be required for additional access channels. • On InterConnect cloud resources and on platforms operated by project partners providing interoperable resources. Other possibilities for hosting data (i.e. open repositories and marketplaces) will be investigated. • Restricted access will be specified and documented if required.
2.3. Making data interoperable	• Assess the interoperability of your data. Specify what data and metadata vocabularies, standards or methodologies you will follow to facilitate interoperability. • Specify whether you will be using standard vocabulary for all data types present in your data set, to allow inter-disciplinary interoperability? If not, will you provide mapping to more commonly used ontologies?	• SAREF ontology will be followed, other options will be investigated.
2.4. Increase data re-use (through clarifying licences)	• Specify how the data will be licenced to permit the widest reuse possible • Specify when the data will be made available for re-use. If applicable, specify why and for what period a data embargo is needed • Specify whether the data produced and/or used in the project is useable by third parties, in particular after the end of the project? If the re-use of some data is restricted, explain why • Describe data quality assurance processes	• Open licenses like Apache 2.0 and GPLVx will be investigated among others. • Possibilities for data reusage and optional embargos will be specified later in the project. • The plan is to make metadata bout interoperable resources and services available to third parties during and after the project. Availability of performance log datasets will be decided during the WP5 execution. • Data quality assurance process will follow best practices for IoT and smart grid systems. Specifics ill be documented in WP2-5 and WP7. • The length of time for reusability of data will be specified during the WP5 execution.

	• Specify the length of time for which the data will remain re-usable	
3. Allocation of resources	• Estimate the costs for making your data FAIR. Describe how you intend to cover these costs • Clearly identify responsibilities for data management in your project • Describe costs and potential value of long-term preservation	• Costs will be assessed during the WP5 and WP7 execution. • Ethics and data protection committee will be responsible for data management. WP5 partners also have representatives in this committee. • Long term preservation costs and values will be assessed later on in the project.
4. Data security	• Address data recovery as well as secure storage and transfer of sensitive data	• WP5 generated datasets will be stored on multiple locations with daily backups. Regarding transfer, secure APIs will be utilized. Specific security measures will be specified during WP5 execution.
5. Ethical aspects	• To be covered in the context of the ethics review, ethics section of DoA and ethics deliverables. Include references and related technical aspects if not covered by the former	• Ethics aspects of WP5 generated data covered in DoA.
6. Other	• Refer to other national/funder/sectorial/departmental procedures for data management that you are using (if any)	• No additional, specific procedures identified as necessary at the moment.

7. TH!NK E

DMP component	Issues to be addressed	Explanation
1. Data summary	• State the purpose of the data collection/generation	Th!nk E is responsible for a Belgium pilot on the site of Leuven Noord. Many sensors will be placed around the site to control and monitor several devices and buildings. The platform for gathering the data will be governed by I.Leco who will make the data accessible to other parties involved in the pilot project.

	• Explain the relation to the objectives of the project • Specify the types and formats of data generated/collected • Specify if existing data is being re-used (if any) • Specify the origin of the data • State the expected size of the data (if known) • Outline the data utility: to whom will it be useful	Energy and thermal metering data will be collected every second. This data includes voltage, current, power, temperature, humidity and much more. The exact number of sensors is unknown at the current time. The data will be used to measure the progress towards the KPI's of the project and to make smart coordinated decisions between different devices on the pilot site.
2. FAIR Data 2.1. Making data findable, including provisions for metadata	• Outline the discoverability of data (metadata provision) • Outline the identifiability of data and refer to standard identification mechanism. Do you make use of persistent and unique identifiers such as Digital Object Identifiers? • Outline naming conventions used • Outline the approach towards search keyword • Outline the approach for clear versioning • Specify standards for metadata creation (if any). If there are no standards in your discipline describe what type of metadata will be created and how	All measuring points will receive a unique identifier within the pilot. A measuring point combined with the timestamp can uniquely identify each piece of data. Naming conventions and metadata are to be determined.
2.2 Making data openly accessible	• Specify which data will be made openly available? If some data is kept closed provide rationale for doing so	The platform for gathering the data will be governed by I.Leco who will make the data accessible to other parties involved in the pilot project. Because there are several stakeholders that are deploying innovative technologies (construction companies, device manufacturers, DSO, …) each stakeholder needs access to the data to control their innovative technology.

	• Specify how the data will be made available • Specify what methods or software tools are needed to access the data? Is documentation about the software needed to access the data included? Is it possible to include the relevant software (e.g. in open source code)? • Specify where the data and associated metadata, documentation and code are deposited • Specify how access will be provided in case there are any restrictions	The data will only be shared with stakeholders in the pilot. Access to the data will be managed through the i.Leco data management platform. More information about the I.Leco platform is to be gathered.
2.3. Making data interoperable	• Assess the interoperability of your data. Specify what data and metadata vocabularies, standards or methodologies you will follow to facilitate interoperability. • Specify whether you will be using standard vocabulary for all data types present in your data set, to allow inter-disciplinary interoperability? If not, will you provide mapping to more commonly used ontologies?	There is a high need for interoperable data because different stakeholders with different backgrounds require access to the data. Naming conventions and metadata need to be determined to address this issue of interoperability.
2.4. Increase data re-use (through clarifying licences)	• Specify how the data will be licenced to permit the widest reuse possible • Specify when the data will be made available for re-use. If applicable, specify why and for what period a data embargo is needed • Specify whether the data produced and/or used in the project is useable by third parties,	To be determined

	in particular after the end of the project? If the re-use of some data is restricted, explain why • Describe data quality assurance processes • Specify the length of time for which the data will remain re-usable	
3. Allocation of resources	• Estimate the costs for making your data FAIR. Describe how you intend to cover these costs • Clearly identify responsibilities for data management in your project • Describe costs and potential value of long-term preservation	I.Leco is responsible for data management in the pilot. The cost for maintaining the platform needs to be determined.
4. Data security	• Address data recovery as well as secure storage and transfer of sensitive data	To be determined with the i.Leco platform
5. Ethical aspects	• To be covered in the context of the ethics review, ethics section of DoA and ethics deliverables. Include references and related technical aspects if not covered by the former	To be determined with the i.Leco platform
6. Other	• Refer to other national/funder/sectorial/departmental procedures for data management that you are using (if any)	

8. FUNDING BOX

DMP component	Issues to be addressed	Explanation

1. Data summary	• State the purpose of the data collection/generation • Explain the relation to the objectives of the project • Specify the types and formats of data generated/collected • Specify if existing data is being re-used (if any) • Specify the origin of the data • State the expected size of the data (if known) • Outline the data utility: to whom will it be useful	**Purpose**: Through “WP 8 Fostering Innovation Through Bottom-up Projects” we will collect data of European SMEs and Startups, through an online form within the FBOX Platform which will be used during the project´s Open Calls. **Objectives**: The information gathered will serve to evaluate and fund the most promising projects in the Energy and Home domains. Therefore, it is necessary to collect, store and process the online forms that will be submitted by project applicants. **Format**: The data sets to be collected during the Open Calls in order to facilitate good analysis of proposals include (non-exhaustive list): Country; Organization name; Project name; Address; Number of team members; Funds requested; Verticals Targeted; Solution type; Name of coordinator and name of the team members; Abstract; Brief description; Company years of experience, etc. All these data sets will be represented in a mapping of submitted proposals. The selected proposals are a subgroup of the submitted proposals and are identified with the field. It is expected to generate a relevant deal-flow of applications through the INTERCONNECT open calls along the project which will contribute to create five main data sets: 1) Applicants that start an application but don't submit a proposal; 2) Submitted proposals; 3) Evaluated proposals; 4) Winner Startups; 5) Follow up metrics **Re-use:** Data will be collected throughout the project, but no datasets of previously collected personal data will be re-used or merged for the purpose of the project. Likewise, sharing data with non-EU members not being part of the consortium isn’t foreseen. **Origin**:

		The information will be captured through online forms and will be recorded and stored in FBOX Cloud infrastructure as an object database. The information will be accessible through an online Dashboard application and it will be downloadable in csv and xls formats. Only authorised users will be allowed to access the data sets via authentication. **Size**: The project doesn't expect to store a huge amount of data, since the data generated by the Project will be stored in excel, word and pdf format. **Data Utility**: The consent for data preservation and sharing will be awarded through explicit consent of the applicants through the online forms. The data will be exploited by project partners and external evaluators for three main purposes: 1) evaluation of proposals; 2) impact assessment; 3) research. The individual registers will be only accessible for evaluation purpose to be done by accredited and authorised evaluators. Each evaluator will be granted with a limited access to a restricted number of registers from the data set. The evaluators will be requested to sign, before giving them access to the data, an 'Experts Evaluators Code of Conduct', an 'External Evaluation Fundamentals' and a 'Declaration of confidentiality and no conflict of interest'. The access will be online for a limited period of time, using a secure mode via authentication.
2. FAIR Data 2.1. Making data findable, including provisions for metadata	• Outline the discoverability of data (metadata provision) • Outline the identifiability of data and refer to standard identification mechanism. Do you make use of persistent and unique identifiers such as Digital Object Identifiers? • Outline naming conventions used	**Discoverability**: In order to be able to use the data generated by the project it is essential to integrate data from the participants in the open calls and the activities undertaken by project partners data should: • Be assigned to a globally unique and persistent identifier; • contain enough metadata to fully interpret the data, and; • be indexed in a searchable source. By applying these principles data become retrievable and include their authentication and authorisation details. **Identifiability**:

	• Outline the approach towards search keyword • Outline the approach for clear versioning • Specify standards for metadata creation (if any). If there are no standards in your discipline describe what type of metadata will be created and how	All documents associated to one particular project will be identified with a unique and persistent number that will be given at the time of the submission process. Examples: - 001ApplicationForm - 001FinancialIdentification - 001Demo - 001Ethics - 001EvaluationReport - 001FinalMonitoring As per the documents related to project activities and/or deliverables, the tasks or deliverables number will be used to identify the document followed by a brief title of the activity or deliverable. **Naming convention**: The recommendations to name documents of the project and facilitate its retriable are as follows : • Choose easily readable identifier names (short and meaningful); • Use capital letter to delimit words instead of spaces or underscores; • Do not use acronyms that are not widely accepted; • Do not use abbreviations or contractions; • Avoid Language-specific or non-alphanumeric characters; • Add a two-digit numeric suffix to identify new versions of one document. • Dates should be included back to front and include the four-digit years: YYYYMMDD **Search keyword**: 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. The information submitted by the applicants to the open calls will use keywords related to the topics covered by INTERCONNECT.

		The keywords used to easily identify documents related to a specific project will be the ones used throughout the submission process, where applicant will have to select the characteristics of their projects selecting descriptors from a dropdown menu. An excel spreadsheet with all information about the projects will be done in order to identify projects submitted for example under one specific challenge or on a TRL 8. Excel will be an efficient tool to filter projects by its characteristics. The “export” functionality of FundingBox platform allows such a listing.
2.2 Making data openly accessible	• Specify which data will be made openly available? If some data is kept closed provide rationale for doing so • Specify how the data will be made available • Specify what methods or software tools are needed to access the data? Is documentation about the software needed to access the data included? Is it possible to include the relevant software (e.g. in open source code)? • Specify where the data and associated metadata, documentation and code are deposited • Specify how access will be provided in case there are any restrictions	**Data openly available:** The full data set of anonymised data will be also available for third parties that would request access to the information for research purposes. Furthermore, the anonymised datasets will be exploited through the creation of maps and charts that will be updated at the end of the selection process of each Open Call. The maps and charts generated will be publicly shown as part of the dissemination activities of the project. **How made available:** The availability of project data will depend on the purpose and the use that third parties are going to make and the added value of sharing such data. Moreover, the Dashboard application of the FBOX platform will also be used to share data. **Methods or tools:** No specific software tools will be needed to access the data, since anonymised data sets will be saved and stored in word, pdf or excel to facilitate its exploitation and guarantee their long-term accessibility. **Deposited:** Throught the INTERCONNECT open calls we will collect data of European SMEs, through an online form within FBOX Platform which will be used during the project. Data will be deposited and secured in the FBOX platform. **Restrictions**: The FBOX platforms allows to create users with different access levels. Access can be granted online for a limited period of time, to a specific information and using a secure mode via authentication.

2.3. Making data interoperable	• Assess the interoperability of your data. Specify what data and metadata vocabularies, standards or methodologies you will follow to facilitate interoperability. • Specify whether you will be using standard vocabulary for all data types present in your data set, to allow inter-disciplinary interoperability? If not, will you provide mapping to more commonly used ontologies?	The vocabulary used in the project Open Calls is a very standard and common language within the business creation culture. Vocabulary won't represent any barrier for data interoperability and re-use.
2.4. Increase data re-use (through clarifying licences)	• Specify how the data will be licenced to permit the widest reuse possible • Specify when the data will be made available for re-use. If applicable, specify why and for what period a data embargo is needed • Specify whether the data produced and/or used in the project is useable by third parties, in particular after the end of the project? If the re-use of some data is restricted, explain why • Describe data quality assurance processes • Specify the length of time for which the data will remain re-usable	**Licenced**: Information related to the winning SMEs/startups, such as the name of the entity, will be published for dissemination purposes only after having obtained the beneficiaries' consent. **Available for re-use:** Data related to the open calls will be made accessible once the final list of beneficiaries is published after each round. Other results such as the performance indicators of the projects will be released in agreement with the participating SMEs when the programme comes to its end and will be available 4 years after the end of the project. **Third parties:** It is foreseen that external evaluators are granted with access to a restricted number of registers from the data set during the evaluation phase and programme. The evaluators will be requested to sign, before giving them access to the data, an 'Experts Evaluators Code of Conduct', an 'External Evaluation Fundamentals' and a 'Declaration of confidentiality and no conflict of interest'. The access will be online for a limited period of time, using a secure mode via authentication. After the end of the project, results of the open calls will be available 4 years in a downloadable archive from the FBOX website. **Quality**:

		Personal data processing will be done following the EU, national and international laws taking into account the "data quality" principles listed below : • Data processing is adequate, relevant and non-excessive; • Accurate and kept up to date; • Processed fairly and lawfully; • Processed in line with data subjects' rights; • Processed in a secure manner; • Kept for no longer that necessary and for the sole purpose of the project
3. Allocation of resources	• Estimate the costs for making your data FAIR. Describe how you intend to cover these costs • Clearly identify responsibilities for data management in your project • Describe costs and potential value of long-term preservation	**Costs**: No extra costs, apart from those linked to the maintenance of the FBOX platform, are expected for making data FAIR. **Open Call data management**: Concerning the data of applicants and beneficiaries, FBOX will be responsible of managing the data stored in its platform (https://fundingbox.com/).
4. Data security	• Address data recovery as well as secure storage and transfer of sensitive data	The FBOX platform applies technological and organizational measures to secure processing of personal data against publishing to unauthorised persons, processing in violation of the law and change, loss, damage or destruction. - Information security: SSL (Secure Socket Layer) certificates are applied. In order to ensure the appropriate level of security, the password for the account will exist on the platform only in a coded form. Registration on and logging in to the platform proceeds in a secure https connection. Use of password to access data sets: the FBOX platform offers 4 different access levels/roles (administrators, developers, evaluators and invitees) to secure access to data by unauthorised users. Communication between the User's device and the servers will be encoded using the SSL protocol.

		- Options for reading data: the platform offers the possibility to make data available in a read-only or downloadable format, hindering the access to information by unauthorised users. Once an Open Call finishes information is archived, so it's no longer publicly accessible, only administrators will have access to the historic data in a read-only mode. - Back-up policy: complete and redundant back-ups are done every hour. Moreover, every time a modification is done an older version is saved. - Accidental deletion or modifications: in case of a catastrophic event that implies the partial or complete deletion of the data sets, the data from the most recent back up will be automatically restored (back-up won't be older than 60 minutes). In case of accidental deletion or modification only the most recent document will be restored, so in case of accidental changes or deletion data can be easily recovered. - Deletion or modification of data by users: only administrators have the rights to delete or modify the information included in the datasets. Under exceptional circumstances administrators can be given the permission to delete applications (utilities offered by the FBOX platform) but the user responsible of its creation will be notified before doing so. - Deletion of data by participants in open calls: users having started the application process can withdraw any time using the FBOX platform before the deadline for submission. - Terms and conditions: the FBOX platform have specific terms of use and conditions that have to be accepted by all users of the platform. o FundingBox terms of service: https://fundingbox.com/about/terms o FundingBox platform privacy policy https://fundingbox.com/about/privacy
5. Ethical aspects	• To be covered in the context of the ethics review, ethics section of DoA and ethics deliverables. Include references and related technical aspects if not covered by the former	
6. Other	• Refer to other national/funder/sectorial/departmental procedures for data management that you are using (if any)	

9. WINGS

DMP component	Issues to be addressed	Explanation
1. Data summary	• State the purpose of the data collection/generation	• Data needed for analytics and prediction with respect to energy consumption in houses.
	• Explain the relation to the objectives of the project	• Provided solutions for data analytics and prediction are complementing the Greek pilot for “showcase the satisfaction of energy users needs with cost-effective solutions, allowing different market agents to create their value, and simultaneously maintain high levels of cybersecurity and data privacy.”
	• Specify the types and formats of data generated/collected	• Data format is JSON.
	• Specify if existing data is being re-used (if any)	• N/A
	• Specify the origin of the data	• Data coming from partners of Greek pilot and own data
	• State the expected size of the data (if known)	• Order of GB (specific number not available yet)
	• Outline the data utility: to whom will it be useful	• Energy providers, end users
2. FAIR Data 2.1. Making data findable, including provisions for metadata	• Outline the discoverability of data (metadata provision)	• Data will be protected and not discoverable through public search
	• Outline the identifiability of data and refer to standard identification mechanism. Do you make use of persistent and unique identifiers such as Digital Object Identifiers?	• Following project’s guideline
	• Outline naming conventions used	• Following project’s guideline
	• Outline the approach towards search keyword	• Following project’s guideline
	• Outline the approach for clear versioning	• Following project’s guideline • Following project’s guideline

	• Specify standards for metadata creation (if any). If there are no standards in your discipline describe what type of metadata will be created and how	
2.2 Making data openly accessible	• Specify which data will be made openly available? If some data is kept closed provide rationale for doing so • Specify how the data will be made available • Specify what methods or software tools are needed to access the data? Is documentation about the software needed to access the data included? Is it possible to include the relevant software (e.g. in open source code)? • Specify where the data and associated metadata, documentation and code are deposited • Specify how access will be provided in case there are any restrictions	• Mainly closed data for security reasons • If needed, available upon request through secure connection • RDBMS mainly • In partner's server • Secure API
2.3. Making data interoperable	• Assess the interoperability of your data. Specify what data and metadata vocabularies, standards or methodologies you will follow to facilitate interoperability. • Specify whether you will be using standard vocabulary for all data types present in your data set, to allow inter-disciplinary interoperability? If not, will you provide mapping to more commonly used ontologies?	• Try to have a common format with other partners in the Greek pilot and the project • Yes, according to project's guideline

2.4. Increase data re-use (through clarifying licences)	• Specify how the data will be licenced to permit the widest reuse possible • Specify when the data will be made available for re-use. If applicable, specify why and for what period a data embargo is needed • Specify whether the data produced and/or used in the project is useable by third parties, in particular after the end of the project? If the re-use of some data is restricted, explain why • Describe data quality assurance processes • Specify the length of time for which the data will remain re-usable	• Following project's guideline • Following project's guideline • No, mainly for security reasons • Well-known processes will be followed including: Data profiling to discover inconsistencies and other anomalies in the data, as well as performing data cleansing activitiesto improve the data quality. • Following project's guideline
3. Allocation of resources	• Estimate the costs for making your data FAIR. Describe how you intend to cover these costs • Clearly identify responsibilities for data management in your project • Describe costs and potential value of long-term preservation	• Cost depends on the amount of available data. To be defined at a later stage • Company's data protection officer is appointed. Best practices for data handling are followed. • Cost depends on the amount of available data. To be defined at a later stage
4. Data security	• Address data recovery as well as secure storage and transfer of sensitive data	• Yes, these aspects are taken into account
5. Ethical aspects	• To be covered in the context of the ethics review, ethics section of DoA and ethics deliverables. Include references and related technical aspects if not covered by the former	• N/A

6. Other	• Refer to other national/funder/sectorial/departmental procedures for data management that you are using (if any)	• N/A

10. SONAE

DMP component	Issues to be addressed	Explanation
1. Data summary	1. State the purpose of the data collection/generation 2. Explain the relation to the objectives of the project 3. Specify the types and formats of data generated/collected 4. Specify if existing data is being re-used (if any) 5. Specify the origin of the data 6. State the expected size of the data (if known)	1. Data collection is necessary in order to monitor energy consumption / generation and key operational information of the systems/buildings under analysis. Additional data (metadata) shall also be considered to properly characterize the monitored variables (owner, device location, source, time step, integration time, variable type, metric, etc…). 2. Such data will be collected and processed in order to enable actuation over the systems/buildings under appreciation, a necessary step to enable the ultimate target of the project pilot, provide demand side flexibility to the grid operator. 3. The data regards mostly time series on energy consumption and generation (energy, power, voltage, current, etc…), while systems operational information regard device temperature, set points, status, etc…, forecasted time-series on energy price, PV generation and load profiles shall also be generated / provided. Existing data series can be re-used to train the models / run analytics. 4. Existing data is being re-used in the context of analytics and reporting. 5. Most of the data will be generated at smart meters, data loggers, consumption / generation devices and/or associated platforms. 6. The size of the data sets is still under analysis. 7. This data might be useful to SonaeMC as energy consumers / producers (Refrigeration, HVAC, Lighting, EV chargers, PV generation) in order to allow real time monitoring as well as improvement of energy

	7. Outline the data utility: to whom will it be useful	management methodologies. It will also be useful to Elergone, as flexibility aggregator, in order to allow a better understanding of the flexibility and optimization of methodologies.
2. FAIR Data 2.1. Making data findable, including provisions for metadata	1. Outline the discoverability of data (metadata provision) 2. Outline the identifiability of data and refer to standard identification mechanism. Do you make use of persistent and unique identifiers such as Digital Object Identifiers? 3. Outline naming conventions used 4. Outline the approach towards search keyword 5. Outline the approach for clear versioning 6. Specify standards for metadata creation (if any). If there are no standards in your discipline describe what type of metadata will be created and how	1. Metadata such as owner, device location, source, time step, integration time, variable type, metric, etc…) shall be gathered thus improving discoverability. Elfos@Marisa 2. No, we do not make use of DOI. 3. Naming conventions are defined for main energy usage and generation devices as well as its location: • Store identification: *store – location* where *store* is the store name and location is the *location*; • Energy consumption / generation vector: ➢ C.FRIO+: Cold central (positive temperatures – refrigerators) ➢ C.FRIO-: Cold central (negative temperatures – freezers) ➢ AVAC: HVAC system ➢ ILUM: Lighting ➢ SOSG: Emergency generator ➢ STRG: Storage ➢ UPAC: Self-consumption renewable generation ➢ UPP: Small renewable generation 4. After the selection of a specific client it is possible to search by *Store identification* key words. A broader approach can be considered where key words consider not only the *Store identification* but also, for example, *Energy consumption / generation vector, region, client name, etc…* 5. No versioning approach was developed until now. 6. No standards for metadata creation were adopted. Metadata created aims to properly characterize the data sets, main attributes regard data origin, ownership, and technical details (owner, access, author, device id, source, variable type, component, time step, integration time, metric, etc…). Part of the metadata is automatically generated, other metadata needs to be filled in manually by the user.
2.2 Making data openly accessible	1. Specify which data will be made openly available? If some data is kept closed provide rationale for doing so 2. Specify how the data will be made available	1. Data regarding **corporate users**, such as Commercial designation, buildings location, area, annual energy consumption, type of consumption / generation devices installed (cold networks, lighting, storage, PV generation, etc…), achieved energy efficiency can be disclosed. All the other data shall remain confidential as it is either related to third parties and/or potentially discloses competitive advantages. For the

	3. Specify what methods or software tools are needed to access the data? Is documentation about the software needed to access the data included? Is it possible to include the relevant software (e.g. in open source code)? 4. Specify where the data and associated metadata, documentation and code are deposited 5. Specify how access will be provided in case there are any restrictions	accomplishment of the pilot tasks, namely the *Energy Efficiency as a service @ commercial buildings* use case, any information shared with partners cannot be disclosed to third parties. Data regarding **non-corporate end-users**, for example the one related to Electric Vehicle users, shall remain confidential, as private users information cannot be disclosed. For the accomplishment of the pilot tasks, namely the *Convenient EV charging* use case, the strictly necessary information shall be shared with partners as long as anonymity is ensured. 2. Data might be made available via different protocols (MODBUS, RS485, …), API's or via FTP folder. 3. No specific software is foreseen needed to access the data. 4. All data and associated metadata is deposited in Elergone repository. 5. Access scheme were not defined yet. Worst case scenario an access via FTP will be created.
2.3. Making data interoperable	1. Assess the interoperability of your data. Specify what data and metadata vocabularies, standards or methodologies you will follow to facilitate interoperability. 2. Specify whether you will be using standard vocabulary for all data types present in your data set, to allow inter-disciplinary interoperability? If not, will you provide mapping to more commonly used ontologies?	1. Interoperability is very limited. The diversity of technological solutions is immense. It is expected that the developments to be achieved during the project in the field of interoperability become of great help not only improving the monitoring ability to as well as control over the diverse systems. 2. Still not defined.
2.4. Increase data re-use (through clarifying licences)	1. Specify how the data will be licenced to permit the widest reuse possible 2. Specify when the data will be made available for re-use. If applicable, specify why and for what period a data embargo is needed	1. Data re-use will be limited to our organization due to the data privacy issue already mentioned. 2. Data shall be useful to re-use in order to run analytics (within the scope of auditing, consultancy), train models and support additional developments. 3. Data is not useable by third parties due to the privacy issues already mentioned. 4. Data quality is verified in different way, adapted to specific data set in consideration, from simple criteria regarding expected range to statistical identification of outliers, correlation of historic data between variables, etc…

	3. Specify whether the data produced and/or used in the project is useable by third parties, in particular after the end of the project? If the re-use of some data is restricted, explain why 4. Describe data quality assurance processes 5. Specify the length of time for which the data will remain re-usable	5. Variable
3. Allocation of resources	1. Estimate the costs for making your data FAIR. Describe how you intend to cover these costs 2. Clearly identify responsibilities for data management in your project 3. Describe costs and potential value of long-term preservation	1. Still unclear which data set will be made FAIR, if any. Costs can only be defined after the definition of the target data sets. The associated costs are eligible within the scope of InterConnect project. 2. Elergone + SonaeMC 3.
4. Data security	1. Address data recovery as well as secure storage and transfer of sensitive data	1. Data is stored in a RAID5 repository with daily backups. Offline backups are done on a monthly basis – still under discussion.
5. Ethical aspects	2. To be covered in the context of the ethics review, ethics section of DoA and ethics deliverables. Include references and related technical aspects if not covered by the former	1. -
6. Other	3. Refer to other national/funder/sectorial/departmental procedures for data management that you are using (if any)	1. GDPR

11. FRAUNHOFER IEE

Partner not involved in data collection activities.

12. ICITY

DMP component	Issues to be addressed	Explanation
1. Data summary	•State the purpose of the data collection/generation	To be able to identify , monitor and report on indoor climate and energy usage. The ability to identify , monitor and control smart appliances and HVAC in apartments/ smart homes. The ability to identify , monitor and control centralised Building Management systems in the smart building.
	•Explain the relation to the objectives of the project	Goal to collect and use data (based on prior consent/approval of individual persons) with the aim to optimize energy consumption/cost and or to improve comfort/convenience (this includes safety/health).

	•Specify the types and formats of data generated /collected	Therefore at this moment it is planned amongst others to collect data from:
		- Smart meter
		- Indoor (climate) sensors
		- Status and (set) preferences of
		  - appliances
		  - smart devices (light, lock, gateway)
		  - building management systems

	•Specify the origin of the data	Data directly gathered from the Single sensor device, multi- sensor devices, wearables for the usage in the smart home , and smart building . Sensors and data embedded in the smartphone or tablet device of the user. Data directly gathered from edge and fog gateways. A more specific tentative list of data fields (to be defined in which room(s): - Co2 level - Temperature (current, set point ,targeted) - Humidity level [%] - Motion detected [Y/N] - Appliances setup/preferences [P, E, State] - Energy consumption of devices [W, Kwh] - …. To be explored/defined (depending on scope) - Smart energy meter of central district heating [T, flow/GJ] - PV panels [kwh] - Battery (building and /or district and/or elevator [kwh,..] - EV charging stations [state, E, occupancy]

		Static data of the user such as Profile Information, Reported Outcomes and reports. These data will be shared after anonymisation. Although the format and synchronization of these data have still to be decided, we are considering the possibility of having specific ontologies in order to normalize data formats and make them interoperable among the different modules of WP2, 4 and 5. Regarding the re-use of the data in this WP, we plan to make them as open as possible. Because of this, as the project reaches maturity and we have more certainty about the data, we will define some measures to ensure that IPR and data privacy is taken into consideration by design as well as which data is feasible to be made open without prejudice to the foregoing.
	•Specify if existing data is being re-used (if any) •State the expected size of the data (if known) •Outline the data utility: to whom will it be useful	The uncertainty about this data makes it difficult to determine the expected size of this data as well as to define to whom it will be useful.

2. FAIR Data 2.1. Making data findable, including provisions for metadata	•Outline the discoverability of data (metadata provision) •Outline the identifiability of data and refer to standard identification mechanisms. Do you make use of persistent and unique identifiers such as Digital Object Identifiers? •Outline naming conventions used	It is envisioned that any data that is moved (from producer to consumer and in between) data will be SAREFized, thus adding metadata attributes to each data artifact. All data will be formatted in the NGSI-LD JSON Data formats. In case we decide to publish the anonymized dataset for analysis, data will be provided files, containing the extracted features (CSV) or preferred in API's . However, due to the uncertainty about the data to be shared in this module, there is not yet a final decision about how we plan to make these data findable. For sure, we will use a standard format for metadata and naming as is already described. Further metadata might be added at the end of the project in line with these metadata conventions. It is envisioned that data will be discoverable via indexed via these SAREFized attributes/ structures in API's, databases , data stores and in the Data marketplace. All data is identifiable by unique GUID identifiers It is envisioned that data will be using SAREF naming conventions

	•Outline the approach towards search keyword	It is envisioned that data wil keywords will be recognised by contains operators, based on text searches.
	•Outline the approach for clear versioning	It is envisioned that data versions to be denoted as <MAJOR::MINOR::DATE> ● Minor releases will be indicated by existing data fields updates. ● Major releases denoted a structure change to the model, data object etc. ● followed by a date of the release
	Specify standards for metadata creation (if any). If there are no standards in your discipline describe what type of metadata will be created and how	None at this moment/. Not sure at this moment , still to be discussed
2.2 Making data openly accessible	•Specify which data will be made openly available? If some data is kept closed provide rationale for doing so	All personal identifiable data will be removed , anonymised Smart Building information relating to Energy demand, energy requests and overall health indicators.
	•Specify how the data will be made available	Data will be made available via the API and or Data Marketplace , part of the WP7 implementation based on the WP 5 deliverables. The Marketplace has all details relating the the usage, test values, user api keys and developer /data scientist information needed to subscribe/ingest data via the API's .

	•Specify what methods or software tools are needed to access the data? Is documentation about the software needed to access the data included? Is it possible to include the relevant software (e.g. in open source code)?	Software able to ingest JSON API's - Postman , cURL , etc.
	•Specify where the data and associated metadata, documentation and code are deposited	The Marketplace has all details relating the the usage, test values, user api keys and developer /data scientist information needed to subscribe/ingest data via the API's .
	•Specify how access will be provided in case there are any restrictions	Not sure at this moment , still to be discussed
2.3. Making data interoperable	•Assess the interoperability of your data. Specify what data and metadata vocabularies, standards or	The interoperability of data will be made possible thanks to the use of ontologies that will ensure that data is converted to common formats that enable interoperability both among the different modules in this WP and the scientific community when making them open. SAREF model as per the WP 2 definitions .

	methodologies you will follow to facilitate interoperability. •Specify whether you will be using standard vocabulary for all data types present in your data set, to allow inter-disciplinary interoperability? If not, will you provide mapping to more commonly used ontologies?	Following the ideas described along the project, since the initial stage of the project, there is still some uncertainty on the specific data to be handled. Datasets will be made open as long as they serve as support to scientific publications in the project and also under anonymized basis, considering that neither I PR or data privacy of users from which this data was originated are at risk.
2.4. Increase data re-use (through clarifying licences)	•Specify how the data will be licenced to permit the widest reuse possible •Specify when the data will be made available for re-use. If applicable, specify why and for what period a data embargo is needed •Specify whether the data produced and/or used in the project is useable by third parties, in particular	As already mentioned, whenever possible, the datasets will be licensed under an Open Access license. Once we decide which data in this WP is reused we will establish quality assurance measures to ensure that all datasets in this WP are cleared of bad records, with clear naming conventions, and with appropriate meta- data conventions applied as well as the responsible for this. During the Pilot rollout period - WP7

	after the end of the project? If the re-use of some data is restricted, explain why	Not sure at this moment , still to be discussed
	•Describe data quality assurance processes	Not sure at this moment , still to be discussed
	•Specify the length of time for which the data will remain re-usable	Not sure at this moment , still to be discussed
3. Allocation of resources	•Estimate the costs for making your data FAIR. Describe how you intend to cover these costs	TBD
	•Clearly identify responsibilities for data management in your project	Not sure at this moment , still to be discussed
	•Describe costs and potential value of long-term preservation	
4. Data security	•Address data recovery as well as secure storage and transfer of sensitive data	This is not applicable for data related to dissemination - containing only the cumulative, anonymized data representation.

5. Ethical aspects	•To be covered in the context of the ethics review, ethics section of DoA and ethics deliverables. Include references and related technical aspects if not covered by the former	All participants in the consortium have agreed with posting their pictures online for dissemina¬ tion items and project updates, still to be discussed
6. Other	•Refer to other national/funder/sectorial/departmental procedures for data management that you are using (if any)	No other procedures need to be put in place for project management data.

13. PLANET

DMP component	Issues to be addressed	Explanation
1. Data summary	• State the purpose of the data collection/generation • Explain the relation to the objectives of the project	• Monitoring and management of connected whitegoods • report on energy usage in apartments and social dwelling • seamless integration with BEMS and HEMS • Data collection and management at the Italian pilot site (based on prior consent/approval of enrolled persons) will lead to optimize energy consumption/cost and or to improve comfort/convenience and will support the achievement of the following project's specific objectives: ○ Increase end-user acceptance of IoT and energy services In smart home and building environment (SO3); ○ Deployment, operation and evaluation of user-driven human centric pilots (SO4) ○ Establishment and support of sustainable interoperable IoT and energy ecosystems, leveraging open standards and commercially viable or economically sustainable use cases (SO5).

	• Specify the types and formats of data generated/collected	• Monitoring of electricity loads, at dwelling and residential level
		  ○ Energy consumption per single connected appliance (whitegood)
		  ○ Aggregated loads and consumption (POD / smart meter /gateways)
		  ○ Surveys and questionnaires
		  ○ BEMS /HEMS

	• Specify if existing data is being re-used (if any)	• Not foreseen at the time being.

	• Specify the origin of the data	• Data is intended to have multiple origins:
		  ○ External Actor – Aggregator
		  ▪ Energy set points (Kw)
		  ○ External Actor – End-users
		  ▪ Sensitive data (Profile information, location, energy consumption [Kwh], appliances setup, preferences)
		  ○ Devices/appliances: POD, smart meters [Kwh, V], connected appliances, whitegoods
		
		Data format and sampling frequency is not yet decided. Normalization and interoperability of data sources needs further discussion and agreement at project level.

		• External stakeholders (End users, Aggregator) to validate the site‘s business case • Internal stakeholders to validate the project’s objectives
	• State the expected size of the data (if known)	• Not known

	• Outline the data utility: to whom will it be useful	• End-users (tenants/house owners); Energy Managers; Building manager. Aggregator.
2. FAIR Data 2.1. Making data findable, including provisions for metadata	• Outline the discoverability of data (metadata provision) • Outline the identifiability of data and refer to standard identification mechanism. Do you make use of persistent and unique identifiers such as Digital Object Identifiers? • Outline naming conventions used • Outline the approach towards search keyword • Outline the approach for clear versioning • Specify standards for metadata creation (if any). If there are no standards in your discipline describe what type of metadata will be created and how	• Metadata will be provided for key interoperable resources (as part of WP2 activities) and made available and discoverable through REST APIs and web dashboards developed within the project • data will be SAREFized, thus adding metadata attributes. • Under evaluation, data may be provided together with its extracted features (csv) • Applied ontology will guide specification of search parameters • Versioning of datasets will be provided based on standard approaches. • Metadata will be specified in line with SAREF ontology, other possibilities will be explored as well (standards and best practices for IoT and smart grid).
2.2 Making data openly accessible	• Specify which data will be made openly available? If some data is kept closed provide rationale for doing so • Specify how the data will be made available • Specify what methods or software tools are needed to access the data? Is documentation about the software needed to access the data included? Is it possible to include the relevant software (e.g. in open source code)?	• Aggregated energy related data and appliance interoperability metadata will be possibly let available. • Data will be made available through REST APIs, other options will be investigated. • Web/app services capable of accessing REST APIs with authorization mechanism.

	• Specify where the data and associated metadata, documentation and code are deposited • Specify how access will be provided in case there are any restrictions	• Cloud based DWH and on platforms operated by project partners providing interoperable resources. Other possibilities for hosting data (i.e. open repositories and marketplaces) will be investigated. • Restricted access will be specified and documented if required following the rules of GA and GDPR.
2.3. Making data interoperable	• Assess the interoperability of your data. Specify what data and metadata vocabularies, standards or methodologies you will follow to facilitate interoperability. • Specify whether you will be using standard vocabulary for all data types present in your data set, to allow inter-disciplinary interoperability? If not, will you provide mapping to more commonly used ontologies?	• SAREF ontology will be followed, other options will be investigated. • During the Pilot rollout period [M24 on]
2.4. Increase data re-use (through clarifying licences)	• Specify how the data will be licenced to permit the widest reuse possible • Specify when the data will be made available for re-use. If applicable, specify why and for what period a data embargo is needed • Specify whether the data produced and/or used in the project is useable by third parties, in particular after the end of the project? If the re-use of some data is restricted, explain why • Describe data quality assurance processes	• Data will be licenced following Open access principles (only for EU countries). Data shared will be anonymised or pseudonymized • Informed Consent Forms will be requested for Piloting Execution [M24]. A written declaration: data controller (the Party collecting the data), Project goals, data collection, retention, processing and communication of data to third parties (including other consortium Partners) must therefore be acquired. Prior to any reuse of data, a Data Protection Impact Assessments (DPIA) must be carried Appropriate Data Processing Agreements shall be prepared and celebrated by each Party that is a data controller with data processors, either Parties to this Consortium or third parties, dealing with personal data collected for the purposes of the Project.

	• Specify the length of time for which the data will remain re-usable	Dissemination and exploitation activities related to the Project shall use anonymised data Data will eventually remain re-usable for research purposes for 5 years after the project's end.
3. Allocation of resources	• Estimate the costs for making your data FAIR. Describe how you intend to cover these costs • Clearly identify responsibilities for data management in your project • Describe costs and potential value of long-term preservation	• Not defined yet • DPO will be identified, if needed, for Piloting activities • Cost for Data storage keeping and security issues have not been estimated.
4. Data security	• Address data recovery as well as secure storage and transfer of sensitive data	• Not defined yet
5. Ethical aspects	• To be covered in the context of the ethics review, ethics section of DoA and ethics deliverables. Include references and related technical aspects if not covered by the former	• n/a
6. Other	• Refer to other national/funder/sectorial/departmental procedures for data management that you are using (if any)	• Data collection and management will follow: DECRETO LEGISLATIVO 10 agosto 2018, n. 101 "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679" and decreto legislativo 196 del 2003 "Codice in materia di protezione dei dati personali".

14. GRIDNET

DMP component	Issues to be addressed	Explanation
1. Data summary	• State the purpose of the data collection/generation	The purpose of the data collection is to provide IoT-assisted energy management services and enable demand side flexibility.

	• Explain the relation to the objectives of the project • Specify the types and formats of data generated/collected • Specify if existing data is being re-used (if any) • Specify the origin of the data • State the expected size of the data (if known) • Outline the data utility: to whom will it be useful	Data is related to WP7 activities and mainly in Greek Pilot objectives, which are the implementation of advanced demand response scenarios in residential setups. Energy consumption data is collected along with temperature/humidity indoor and outdoor, human presence and door contact sensors' data. The collected data is serialized in JSON format. Historical data before the beginning of the project will be available for data analytics if necessary. Data is generated by smart meters installed in homes along with a sensor kit installed, which in some cases it may include smart plugs for some white appliances. Data is not expected to go over 10GBs for the first year of the project. Data will be useful to the home owners and Greek Pilot stakeholders that will use it to either provide incentives for DSF engagement or to create prediction services. Later on the data will be useful to some of the bottom-up projects that will be selected in WP8.
2. FAIR Data 2.1. Making data findable, including provisions for metadata	• Outline the discoverability of data (metadata provision) • Outline the identifiability of data and refer to standard identification mechanism. Do you make use of persistent and unique identifiers such as Digital Object Identifiers? • Outline naming conventions used • Outline the approach towards search keyword • Outline the approach for clear versioning • Specify standards for metadata creation (if any). If there are no standards in your discipline describe what type of metadata will be created and how	A specific API endpoint is provided which serves as an inventory and lists the available data types and their characteristics. No standard identification mechanism is used. We avoid using naming conventions to store metadata, we prefer to provide those as key:value in JSON formats. No search keyword will be provided, the consumer of the data would explicitly request data with the guidance of documentation and inventory service. Specific endpoint of the API will provide its current version. No metadata creation is planned for the moment. If the need arises, we will try to reuse SAREF from WP3 if applicable.
2.2 Making data openly accessible	• Specify which data will be made openly available? If some data is kept closed provide rationale for doing so	Data will be open to Interconnect stakeholders including Greek Pilot stakeholders, marketplace and bottom-up projects. Data is a collection of energy and sensor measurements that correspond to individuals. Even though data is anonymized, there is always danger of exporting the user's identity through analytics. For this reason data will not be publicly accessible.

	• Specify how the data will be made available • Specify what methods or software tools are needed to access the data? Is documentation about the software needed to access the data included? Is it possible to include the relevant software (e.g. in open source code)? • Specify where the data and associated metadata, documentation and code are deposited • Specify how access will be provided in case there are any restrictions	Data will be made available through well defined REST endpoints with adequate documentation and access rights. Any software/service capable of using REST endpoints with JSON format could access the data. Data is stored in our server along with the API and backend code. Documentation will be available over email and in the project repository. Predefined credentials will be shared to the relevant stakeholders that need access to the data.
2.3. Making data interoperable	• Assess the interoperability of your data. Specify what data and metadata vocabularies, standards or methodologies you will follow to facilitate interoperability. • Specify whether you will be using standard vocabulary for all data types present in your data set, to allow inter-disciplinary interoperability? If not, will you provide mapping to more commonly used ontologies?	We will follow WP3 recommendations on how to make our platform and data SAREF-compliant, thus interoperable with the interconnect ecosystem. We plan to map all our data types to the proposed SAREF ontology by WP3.
2.4. Increase data re-use (through clarifying licences)	• Specify how the data will be licenced to permit the widest reuse possible • Specify when the data will be made available for re-use. If applicable, specify why and for what period a data embargo is needed • Specify whether the data produced and/or used in the project is useable by third parties,	We haven't' investigated yet, which data license will be the most suitable for our case. As mentioned above, no plan for open public access is planned for the moment. Data will be usable by third parties after the end of the project. assuming a pre-agreement is made on how and for what purpose the data will be used. Data relevant to the user's identity is not exposed and usable at any point of the project and beyond, due to GDPR compliance reasons. Haven't defined yet any. It will remain re-usable for the amount of time that is defined in the GrantAggreement (3 years if the amendment was agreed).

	in particular after the end of the project? If the re-use of some data is restricted, explain why • Describe data quality assurance processes • Specify the length of time for which the data will remain re-usable	
3. Allocation of resources	• Estimate the costs for making your data FAIR. Describe how you intend to cover these costs • Clearly identify responsibilities for data management in your project • Describe costs and potential value of long-term preservation	Most of the costs and allocation of resources will be made in WP3 efforts, which will allow us to make our data FAIR by adopting the SAREF ontology.
4. Data security	• Address data recovery as well as secure storage and transfer of sensitive data	Storage of data is made in our server where all the security measures like firewall and security updates take place. Data recovery is made available to consumers only through a dedicated and predefined set of credentials and is encrypted over SSL.
5. Ethical aspects	• To be covered in the context of the ethics review, ethics section of DoA and ethics deliverables. Include references and related technical aspects if not covered by the former	GDPR guidelines are followed whenever necessary. For example only anonymized data are made accessible to data consumers.
6. Other	• Refer to other national/funder/sectorial/departmental procedures for data management that you are using (if any)	None

15. YNCREA

DMP component	Issues to be addressed	Explanation
1. Data summary	• State the purpose of the data collection/generation • Explain the relation to the objectives of the Project	**The purpose of the data collection/generation:** In InterConnect, Yncrea will collaborate with TPM , & the company that operate the place of the French pilot (Simielec, Bouygues Immobilier, the city hall, Enedis =DSO, from aggregators, Dalkia = manage hot water in Font Pré , Heliopolis condominium from the Levant's island). **The relation to the objectives of the project (*objectives should be listed centrally in this doc)*:** WP1 Task 1.1 – Human-centric services and business models definition Subtask 1.1.1 Design of energy services: WP7 Task 7.7 – Demand flexibility for supporting the grid in normal and emergency operation situations, an end-users focused approach: French uptake Subtask 7.7.1 – Setup and integration of tools and hardware: Subtask 7.7.2 – Management and demonstration of the use cases and services: • Optimal activation of available local flexibilities: preventive (day-ahead) or emergency (intraday) scenarios, using interoperable ICT solutions with two different architectures: flexibility function architecture (SGAM) and existing smart meters communications' infrastructure. • Energy and non-energy services: novel services related to the adoption of DSF by end-users and smart grids actors. Potential **Specify the types of data generated/collected ; the format will be defined later.**

	• Specify the types and formats of data generated/collected	• Caloriemeter, smartmeter Linky, Watermeter. • Smartshutter, know if door are open or not, indoor temperature of the different rooms. • PV & smartparking + ombrière solaire. Within the city hall infracstructre & measure in real time the electricity production. • Monitoring of electricity, cooling, heating and Domestic Hot Water consumption at residential property and Building Heating Network level • Comfort profiles of occupants • User and stakeholder needs and requirements • Surveys and questionnaires (the type data Will be detailed later in the Project) • Metadata on interoperability
	• Specify if existing data is being re-used (if any)	**Specify if existing data is being re-used (if any):** We do not use any data from prior activities.
	• Specify the origin of the data	**Specify the origin of the data:** • Connected flat (Font pré), different Smart meters, caloriemeter, Linky, hot water Smart meter) • DSO • Aggregators • Device level (appliances, heat pumps, inverters,…) • Building Energy Management Systems(BEMS) • HEMs (Home Energy Management System) • Electric heat pump. • Sensors at residential level for shutter, heating, lighting, DOCIS (Data over cable service interface specification) (Font Pré demo). • Residents (collected through surveys) • Additional third parties services (predictive data, weather data,…)

	• State the expected size of the data (if known) • Outline the data utility: to whom will it be useful	**The expected size of the data (if known):** • To be defined. TBD • Size of the storage of the platform TBD. **Outline the data utility: to whom will it be useful:** • Site stakeholders to validate the site's business case • Project stakeholders to validate the project's objectives
2. FAIR Data 2.1. Making data findable, including provisions for metadata	• Outline the discoverability of data (metadata provision) • Outline the identifiability of data and refer to standard identification mechanism. Do you make use of persistent and unique identifiers such as Digital Object Identifiers? • Outline naming conventions used	To be defined. (wait output from WP1 & WP2) As far as FAIR data management is concerned, the guidelines of the Go Fair initiative will be considered and applied where possible. At this stage (April 2020) a fully detailed plan is not yet available. For now, we refer to https://www.go-fair.org/fair-principles

	• Outline the approach towards search keyword • Outline the approach for clear versioning • Specify standards for metadata creation (if any). If there are no standards in your discipline describe what type of metadata will be created and how	
2.2 Making data openly accessible	• Specify which data will be made openly available? If some data is kept closed provide rationale for doing so • Specify how the data will be made available • Specify what methods or software tools are needed to access the data? Is documentation about the software needed to access the data included? Is it possible to include the relevant software (e.g. in open source code)? • Specify where the data and associated metadata, documentation and code are deposited	• To be discussed and decided. Personal data will not be made available in an open fashion in accordance with GDPR as well as any national legislation that applies. The use of data in France Will required a PIA (Privacy Impact Assessment). • Type of data : o TDB o Data that will be made available will be accessible through API's & via monitoring application interface. • TBD • Where the data and associated metadata, documentation and code are deposited will also be considered at a later stage.

	• Specify how access will be provided in case there are any restrictions	• Access in case there are any restrictions to data will be dealt with on a case-by-case basis on request and the links Will be securized & the data Will be encrypted.
2.3. Making data interoperable	• Assess the interoperability of your data. Specify what data and metadata vocabularies, standards or methodologies you will follow to facilitate interoperability. • Specify whether you will be using standard vocabulary for all data types present in your data set, to allow inter-disciplinary interoperability? If not, will you provide mapping to more commonly used ontologies?	Wait WP2 output To be defined.
2.4. Increase data re-use (through clarifying licences)	• Specify how the data will be licensed to permit the widest reuse possible • Specify when the data will be made available for re-use. If applicable, specify why and for what period a data embargo is needed • Specify whether the data produced and/or used in the project is usable by third parties, in particular after the end of the project? If the re-use of some data is restricted, explain why • Describe data quality assurance processes • Specify the length of time for which the data will remain re-usable	Mostly, we will deliver open-source on specific code embedding intelligent work, but we will be able to change the type of license. To be discussed and decided. To be discussed and decided.

		To be discussed and decided. To be discussed and decided.
3. Allocation of resources	• Estimate the costs for making your data FAIR. Describe how you intend to cover these costs • Clearly identify responsibilities for data management in your project • Describe costs and potential value of long-term preservation	• Costs will be disclosed within Wp2 to Wp5 and Wp7; • Data protection will be handled by the entities DPO's, and via the Ethics and Data Protection Committee within the consortium; WP7 Data management will be the shared responsibility of the original data owners, pilot leads, WP7 partners and task leads and the Ethics and Data Protection Committee of InterConnect. Costs will be assessed during WP7 execution. The repartition of the cost will be defined later.
4. Data security	• Address data recovery as well as secure storage and transfer of sensitive data	**WP7** Data used by the different applications from the French pilot would be encrypted for critical data. All data are stored in a distributed way, all data are distributed on several nodes in order to be highly available. All the nodes of the infrastructure will be a daily back-up.

5. Ethical aspects	• To be covered in the context of the ethics review, ethics section of DoA and ethics deliverables. Include references and related technical aspects if not covered by the former	Will be covered in the context of the ethics review, the ethics section of the DoA and ethics deliverables.
6. Other	• Refer to other national/funder/sectoral/departmental procedures for data management that you are using (if any)	Peer review of the architecture with experts. (Be compliant with AAA* & CIA** concepts) Penetration test on the global solution. For the experts, be compliant with ISO 27701. * AAA (Authentification, Autorisation,Accountability) **CIA (Confidentiality Integrity Availability) Cybersecurity begins from the requirements' writing until the integration. Concern all the stages of a deliverable project from its specification to its exploitation. From the functional requirements, cybersecurity is present and applied to the architecture. In the 12 sectors of vital importance, the energy sector occupies an important part. We need to make sure that the pilots we are going to deploy on a large scale are secure & resilient. ***OVI (Organe Vitals Infrastructure) Single Point of Failure Be compliant with the forensic method. (Forensic, when there is an attack, ability to analyze what has happened. Back up the machine, scan it, locate it in the network. Know if returned by back door, root kit ... tracking. Malware analysis, data infiltration análysis, network forensic). Treat this as a moving target.

16. AUEB

DMP component	Issues to be addressed	Explanation
1. Data summary	• State the purpose of the data collection/generation • Explain the relation to the objectives of the project • Specify the types and formats of data generated/collected • Specify if existing data is being re-used (if any) • Specify the origin of the data • State the expected size of the data (if known) • Outline the data utility: to whom will it be useful	• The purpose of the data collection is to enhance the **features of the mobile application that AUEB is going to develop**, by incorporating energy and non-energy data provided by HERON, GRIDNET and COSMOTE. • The data collected are directly related with the project objectives of "Large-scale pilots leading to market driven deployments" and "User centric energy and non-energy services", since they are utilized by AUEB's mobile app for the Greek pilot. This app is going to be used by the customers of HERON, GRIDNET and COSMOTE. • The data collected are going to be stored in **JSON object format using MongoDB**. • The origin of the data is the **databases of HERON, GRIDNET and COSMOTE** • The data will be useful for the **Greek pilot mobile application and therefore for the customers of HERON, GRIDNET and COSMOTE**. • The storage capacity of the storage platform will be in the order of 10 TB.
2. FAIR Data 2.1. Making data findable, including provisions for metadata	• Outline the discoverability of data (metadata provision) • Outline the identifiability of data and refer to standard identification mechanism. Do you make use of persistent and unique identifiers such as Digital Object Identifiers? • Outline naming conventions used • Outline the approach towards search keyword • Outline the approach for clear versioning	• The database we are going to use (MongoDB) attaches a unique id to each object stored as an identification mechanism by default. • Metadata are going to be generated and stored regarding various metrics like statistics related to the original data, user characteristics like energy efficiency type (either manually inserted through the mobile application by the user or automatically generated from the original user data).

	• Specify standards for metadata creation (if any). If there are no standards in your discipline describe what type of metadata will be created and how	
2.2 Making data openly accessible	• Specify which data will be made openly available? If some data is kept closed provide rationale for doing so • Specify how the data will be made available • Specify what methods or software tools are needed to access the data? Is documentation about the software needed to access the data included? Is it possible to include the relevant software (e.g. in open source code)? • Specify where the data and associated metadata, documentation and code are deposited • Specify how access will be provided in case there are any restrictions	• **All the data are going to be private**, since they are used only for the purpose of the mobile application for the Greek pilot.
2.3. Making data interoperable	• Assess the interoperability of your data. Specify what data and metadata vocabularies, standards or methodologies you will follow to facilitate interoperability. • Specify whether you will be using standard vocabulary for all data types present in your data set, to allow inter-disciplinary interoperability? If not, will you provide mapping to more commonly used ontologies?	N/A

2.4. Increase data re-use (through clarifying licences)	• Specify how the data will be licenced to permit the widest reuse possible • Specify when the data will be made available for re-use. If applicable, specify why and for what period a data embargo is needed • Specify whether the data produced and/or used in the project is useable by third parties, in particular after the end of the project? If the re-use of some data is restricted, explain why • Describe data quality assurance processes • Specify the length of time for which the data will remain re-usable	• The data will only be consumed by the Greek pilot mobile application so there is **no need to consider data re-use.**
3. Allocation of resources	• Estimate the costs for making your data FAIR. Describe how you intend to cover these costs • Clearly identify responsibilities for data management in your project • Describe costs and potential value of long-term preservation	N/A
4. Data security	• Address data recovery as well as secure storage and transfer of sensitive data	Data transfer between AUEB's backend, AUEB's mobile application and provider's backend is going to be conducted using HTTPS.
5. Ethical aspects	• To be covered in the context of the ethics review, ethics section of DoA and ethics deliverables. Include references and related technical aspects if not covered by the former	The data stored in AUEB's database will be in anomymized and in format compliant with GDPR regulations and will not be shared with any other party. Mobile app users will give their informed consent about data storage and processing for the purpose of user profiling, recommendation and other purposes that aim at improving user experience with the app.
6. Other	• Refer to other national/funder/sectorial/departmental procedures for data management that you are using (if any)	N/A

17. ELEKTROLJUBLJANA

DMP component	Issues to be addressed	Explanation
1. Data summary	• State the purpose of the data collection/generation • Explain the relation to the objectives of the project	The scope of WP4, where the engagement of Elektro Ljubljana is foreseen: ✓ Design and implementation of the Standard DSO Interface, which is an API interface that defines the communication standards to connect the DSO to the several market platforms of the evolving energy sector (in T4.1) ✓ Ensure interoperability between InterConnect Reference Architecture and DSO legacy systems, particularly SCADA/ DMS (in T4.2) ✓ Specification and implementation of a DSO flexibility market enabling new standardized flexibility services provided by aggregators, energy communities and microgrids for distribution grids (in T4.3) ✓ Implementation of distributed control architectures for the operation of MV and LV distribution grids, particularly involving energy communities and microgrids participating in P2P markets (in T4.4)
	• Specify the types and formats of data generated/collected • Specify if existing data is being re-used (if any) • Specify the origin of the data • State the expected size of the data (if known) • Outline the data utility: to whom will it be useful	Elektro Ljubljana should provide the detailed specifications of his Grid Operation and management tool. The type and the format of the data iec61970cim17v16,_iec61968 cim13v10,_iec62325 cim03v14 will be in details specified later, during the work on the WP and particular task. The origin of the data: extracted from the Elektro Ljubljana's repository. Size: approx.. 3GB. the data will be useful to the connected third parties' platforms.
2. FAIR Data 2.1. Making data findable, including provisions for metadata	• Outline the discoverability of data (metadata provision) • Outline the identifiability of data and refer to standard identification mechanism. Do you	• CIM format is written as a standard XML file, and the Metadata in relation with established services can be found in the data. APIs would allow its discovery due to the interoperability of the format. • cim:IdentifiedObject.

	make use of persistent and unique identifiers such as Digital Object Identifiers? • Outline naming conventions used • Outline the approach towards search keyword • Outline the approach for clear versioning • Specify standards for metadata creation (if any). If there are no standards in your discipline describe what type of metadata will be created and how	• Not possible to particularize at this stage.
2.2 Making data openly accessible	• Specify which data will be made openly available? If some data is kept closed provide rationale for doing so • Specify how the data will be made available • Specify what methods or software tools are needed to access the data? Is documentation about the software needed to access the data included? Is it possible to include the relevant software (e.g. in open source code)? • Specify where the data and associated metadata, documentation and code are deposited • Specify how access will be provided in case there are any restrictions	• most data will be kept closed, to authorized entities. On request based on elaborated requirement? • RTU, smart meters, other ICT interfaces, the concept of the data exchange will be point to point.
2.3. Making data interoperable	• Assess the interoperability of your data. Specify what data and metadata vocabularies, standards or methodologies you will follow to facilitate interoperability.	• Following the development using the project. Data from the AMI infrastructure, topology and elements properties are written in parallel from a repository to a standard CIM format.

	• Specify whether you will be using standard vocabulary for all data types present in your data set, to allow inter-disciplinary interoperability? If not, will you provide mapping to more commonly used ontologies?	• Yes.
2.4. Increase data re-use (through clarifying licences)	• Specify how the data will be licenced to permit the widest reuse possible • Specify when the data will be made available for re-use. If applicable, specify why and for what period a data embargo is needed • Specify whether the data produced and/or used in the project is useable by third parties, in particular after the end of the project? If the re-use of some data is restricted, explain why • Describe data quality assurance processes • Specify the length of time for which the data will remain re-usable	• In accordance to GA, from our perspective we do not seen any special conditions for reusage. • we cannot answer this now, but no embargo on the data is foreseen. • past data e.g. from the meters, operation status of the grid might be used even after the end of the project but would not have any value.
3. Allocation of resources	• Estimate the costs for making your data FAIR. Describe how you intend to cover these costs • Clearly identify responsibilities for data management in your project • Describe costs and potential value of long-term preservation	
4. Data security	• Address data recovery as well as secure storage and transfer of sensitive data	• The concept of the integration must ensure the secure manner for handling with the sensitive data. CIM is extracted i.e. written as an output from a repository, where all the relevant data and attributes of elements, topology and metering is stored and it is been backed-up. Data recovery is not an issue.
5. Ethical aspects	• To be covered in the context of the ethics review, ethics section of DoA and ethics	

	deliverables. Include references and related technical aspects if not covered by the former	
6. Other	• Refer to other national/funder/sectorial/departmental procedures for data management that you are using (if any)	• data from the meters cannot be send to any unauthorized person/entity. The owners of the data from the meters are the grid users. The system specification will not be exposed to third parties.

18. THERMOVAULT

DMP component	Issues to be addressed	Explanation
1. Data summary	• State the purpose of the data collection/generation • Explain the relation to the objectives of the project • Specify the types and formats of data generated/collected • Specify if existing data is being re-used (if any) • Specify the origin of the data • State the expected size of the data (if known) • Outline the data utility: to whom will it be useful	• The purpose of the data collection: model, control, and enable interoperability of flexible energy devices • Relation to objectives: Objectives of WPs 3 and 7 • Types and formats of data collected: Thermal data regarding water and space heaters, ambient temperature, electric vehicles and batteries. Formats are not specified yet • Existing data is being re-used: not specified yet • Specify the origin of the data: Belgian ThermoVault pilot • The expected size of the data: Not specified yet • Outline the data utility: Not specified yet
2. FAIR Data 2.1. Making data findable, including	• Outline the discoverability of data (metadata provision)	Data will be shared in the project platform using the standard decided by the consortium

provisions for metadata	• Outline the identifiability of data and refer to standard identification mechanism. Do you make use of persistent and unique identifiers such as Digital Object Identifiers? • Outline naming conventions used • Outline the approach towards search keyword • Outline the approach for clear versioning • Specify standards for metadata creation (if any). If there are no standards in your discipline describe what type of metadata will be created and how	
2.2 Making data openly accessible	• Specify which data will be made openly available? If some data is kept closed provide rationale for doing so • Specify how the data will be made available • Specify what methods or software tools are needed to access the data? Is documentation about the software needed to access the data included? Is it possible to include the relevant software (e.g. in open source code)? • Specify where the data and associated metadata, documentation and code are deposited • Specify how access will be provided in case there are any restrictions	Data that will be shared is not yet specified
2.3. Making data interoperable	• Assess the interoperability of your data. Specify what data and metadata vocabularies,	Data format will follow SAREF ontology and the recommendations from the consortium in terms of architecture, formats and data models.

	standards or methodologies you will follow to facilitate interoperability. • Specify whether you will be using standard vocabulary for all data types present in your data set, to allow inter-disciplinary interoperability? If not, will you provide mapping to more commonly used ontologies?	
2.4. Increase data re-use (through clarifying licences)	• Specify how the data will be licenced to permit the widest reuse possible • Specify when the data will be made available for re-use. If applicable, specify why and for what period a data embargo is needed • Specify whether the data produced and/or used in the project is useable by third parties, in particular after the end of the project? If the re-use of some data is restricted, explain why • Describe data quality assurance processes • Specify the length of time for which the data will remain re-usable	Not specified yet
3. Allocation of resources	• Estimate the costs for making your data FAIR. Describe how you intend to cover these costs • Clearly identify responsibilities for data management in your project • Describe costs and potential value of long-term preservation	Not specified yet
4. Data security	• Address data recovery as well as secure storage and transfer of sensitive data	Not specified yet

5. Ethical aspects	• To be covered in the context of the ethics review, ethics section of DoA and ethics deliverables. Include references and related technical aspects if not covered by the former	GDPR is included in all data-related processes with the corresponding anonymisation and protection
6. Other	• Refer to other national/funder/sectorial/departmental procedures for data management that you are using (if any)	

19. TRIALOG

DMP component	Issues to be addressed	Explanation
1. Data summary	• State the purpose of the data collection/generation • Explain the relation to the objectives of the project • Specify the types and formats of data generated/collected • Specify if existing data is being re-used (if any) • Specify the origin of the data • State the expected size of the data (if known) • Outline the data utility: to whom will it be useful	Technical data will be collected by the T-EMS module in order to calculate the charging profile. This data will cover the EV user's need (power need and departure time) and the EV's characteristics (max power, level of its batteries, charging capabilities…) and will only be stored during the charging session. In addition, statistical data may be computed based on the collected data.

2. FAIR Data 2.1. Making data findable, including provisions for metadata	• Outline the discoverability of data (metadata provision) • Outline the identifiability of data and refer to standard identification mechanism. Do you make use of persistent and unique identifiers such as Digital Object Identifiers? • Outline naming conventions used • Outline the approach towards search keyword • Outline the approach for clear versioning • Specify standards for metadata creation (if any). If there are no standards in your discipline describe what type of metadata will be created and how	At this stage of the project, it is not foreseen a need to make the collected data available (so this data will remain inside the T-EMS module). It may reconsidered in the future in case a need is identified.
2.2 Making data openly accessible	• Specify which data will be made openly available? If some data is kept closed provide rationale for doing so • Specify how the data will be made available • Specify what methods or software tools are needed to access the data? Is documentation about the software needed to access the data included? Is it possible to include the relevant software (e.g. in open source code)? • Specify where the data and associated metadata, documentation and code are deposited • Specify how access will be provided in case there are any restrictions	

2.3. Making data interoperable	• Assess the interoperability of your data. Specify what data and metadata vocabularies, standards or methodologies you will follow to facilitate interoperability. • Specify whether you will be using standard vocabulary for all data types present in your data set, to allow inter-disciplinary interoperability? If not, will you provide mapping to more commonly used ontologies?	
2.4. Increase data re-use (through clarifying licences)	• Specify how the data will be licenced to permit the widest reuse possible • Specify when the data will be made available for re-use. If applicable, specify why and for what period a data embargo is needed • Specify whether the data produced and/or used in the project is useable by third parties, in particular after the end of the project? If the re-use of some data is restricted, explain why • Describe data quality assurance processes • Specify the length of time for which the data will remain re-usable	
3. Allocation of resources	• Estimate the costs for making your data FAIR. Describe how you intend to cover these costs • Clearly identify responsibilities for data management in your project • Describe costs and potential value of long-term preservation	

4. Data security	• Address data recovery as well as secure storage and transfer of sensitive data	
5. Ethical aspects	• To be covered in the context of the ethics review, ethics section of DoA and ethics deliverables. Include references and related technical aspects if not covered by the former	
6. Other	• Refer to other national/funder/sectorial/departmental procedures for data management that you are using (if any)	

20. SGTA

DMP component	Issues to be addressed	Explanation
1. Data summary	• State the purpose of the data collection/generation • Explain the relation to the objectives of the project • Specify the types and formats of data generated/collected • Specify if existing data is being re-used (if any) • Specify the origin of the data • State the expected size of the data (if known)	• Data will be collected in buildings both commercial and domestic. • Data will mainly consist in energy values and other that can help characterize and predict energy consumption and production such as climatic values (temperature, humidity,..), business type (office, retail,..), physical building data (areas,…)

	• Outline the data utility: to whom will it be useful	
2. FAIR Data 2.1. Making data findable, including provisions for metadata	• Outline the discoverability of data (metadata provision) • Outline the identifiability of data and refer to standard identification mechanism. Do you make use of persistent and unique identifiers such as Digital Object Identifiers? • Outline naming conventions used • Outline the approach towards search keyword • Outline the approach for clear versioning • Specify standards for metadata creation (if any). If there are no standards in your discipline describe what type of metadata will be created and how	• Consortium shall decide a standard to be used
2.2 Making data openly accessible	• Specify which data will be made openly available? If some data is kept closed provide rationale for doing so • Specify how the data will be made available • Specify what methods or software tools are needed to access the data? Is documentation about the software needed to access the data included? Is it possible to include the relevant software (e.g. in open source code)? • Specify where the data and associated metadata, documentation and code are deposited	• At this stage of the project this is still not specified

	• Specify how access will be provided in case there are any restrictions	
2.3. Making data interoperable	• Assess the interoperability of your data. Specify what data and metadata vocabularies, standards or methodologies you will follow to facilitate interoperability. • Specify whether you will be using standard vocabulary for all data types present in your data set, to allow inter-disciplinary interoperability? If not, will you provide mapping to more commonly used ontologies?	• SAREF ontology will probably be used
2.4. Increase data re-use (through clarifying licences)	• Specify how the data will be licenced to permit the widest reuse possible • Specify when the data will be made available for re-use. If applicable, specify why and for what period a data embargo is needed • Specify whether the data produced and/or used in the project is useable by third parties, in particular after the end of the project? If the re-use of some data is restricted, explain why • Describe data quality assurance processes • Specify the length of time for which the data will remain re-usable	• Still undefined as far as we know
3. Allocation of resources	• Estimate the costs for making your data FAIR. Describe how you intend to cover these costs • Clearly identify responsibilities for data management in your project	• At this stage, without requirements definitions, its not possible to estimate costs

	• Describe costs and potential value of long-term preservation	
4. Data security	• Address data recovery as well as secure storage and transfer of sensitive data	• Project guidelines will be strictly followed on pilot implementation.
5. Ethical aspects	• To be covered in the context of the ethics review, ethics section of DoA and ethics deliverables. Include references and related technical aspects if not covered by the former	• GDPR and other best practices shall be followed in order to assure the fulfilment of legal and ethical issues
6. Other	• Refer to other national/funder/sectorial/departmental procedures for data management that you are using (if any)	

21. SEP

DMP component	Issues to be addressed	Explanation
1. Data summary	1 State the purpose of the data collection/generation 2 Explain the relation to the objectives of the project 3 Specify the types and formats of data generated/collected 4 Specify if existing data is being re-used (if any) 5 Specify the origin of the data 6 State the expected size of the data (if known)	1. We intend to collect energy data (active energy produced, currents, others), environment (temperature, humidity, CO2), equipment status (hours of operation), other data framed with project requirements. Additional data such as site name, geographical location, area, others info should be considered. Data collected locally will be transformed into building performance indicators (KPI's) or processed according to project needs. 2. The data collected are mainly from commercial buildings, such as energy consumption, temperatures, humidity, equipment status, others to be defined. The data can be shared locally with the facility manager and other stakeholders, alone or correlated. The data can be provided in real time or historical. The way the data will be collected and shared will be according to the project definitions and reference architectures.

	7 Outline the data utility: to whom will it be useful	3. The data is recorded in time series such us electrical measurements (active power, reactive power, voltage, current, etc...), building operating information (temperature, humidity, CO2, others) and equipment operating information (operating hours, status, alarm, others). Time series on performance indicators, energy price, load profiles should also be generated/supplied. Existing data series can be reused to compare periods in order to evaluate the performance of the building. 4. We can reuse data to compare periods to evaluate the performance of the building. This data is generated and stored locally. 5. Local equipment such as meters, HVAC, electrical panels, other equipment that allows integration and data communication. 6. We cannot estimate the expected data size but the local controller, which is part of the proposed digital platform, has the capacity to store 4GB of information. The proposed digital platform has an unlimited capacity and depends on the available disk space 7. The **DSO and the end user (Facility Manager, Maintenance, Operators, other's related with Building)**
2. FAIR Data 2.1. Making data findable, including provisions for metadata	1 Outline the discoverability of data (metadata provision) 2 Outline the identifiability of data and refer to standard identification mechanism. Do you make use of persistent and unique identifiers such as Digital Object Identifiers? 3 Outline naming conventions used 4 Outline the approach towards search keyword 5 Outline the approach for clear versioning 6 Specify standards for metadata creation (if any). If there are no standards in your discipline describe what type of metadata will be created and how	1. Not applicable on digital platform proposed by SEP. 2. It is not applied. 3. The names and conventions can be edited/added to the SEP digital platform. 4. It is possible to search for an object using a property such as name, tag, descriptions, others depending on the type of object. 5. Is not available. 6. Our platform is developed following the standard of "project Haystack" and "Brick".

2.2 Making data openly accessible	1 Specify which data will be made openly available? If some data is kept closed provide rationale for doing so 2 Specify how the data will be made available 3 Specify what methods or software tools are needed to access the data? Is documentation about the software needed to access the data included? Is it possible to include the relevant software (e.g. in open source code)? 4 Specify where the data and associated metadata, documentation and code are deposited 5 Specify how access will be provided in case there are any restrictions	1. All data acquired and further processed is available for the interconnect digital platform. 2. The data is available through standard protocols. 3. Through Webservices (Rest, Soap) or standard protocols such as Modbus, Bacnet, LonWorks, KNX. 4. In the interconnect document repository. 5. We can make the data available through a local web interface or send by SMTP. However, we are waiting for more project definitions.
2.3. Making data interoperable	1 Assess the interoperability of your data. Specify what data and metadata vocabularies, standards or methodologies you will follow to facilitate interoperability. 2 Specify whether you will be using standard vocabulary for all data types present in your data set, to allow inter-disciplinary interoperability? If not, will you provide mapping to more commonly used ontologies?	1. We will apply the **SAREF ontology**, but we still must validate its full application. 2. We will implement the WP5 definitions.
2.4. Increase data re-use (through clarifying licences)	1 Specify how the data will be licenced to permit the widest reuse possible 2 Specify when the data will be made available for re-use. If applicable, specify why and for what period a data embargo is needed	1. Data ownership will belong the site or Building/Site owner. The servers (physical controllers; PC or Virtual Machine) have a licence schema based in the size of site control architecture. 2. There are no time limitation of access to data.

	3 Specify whether the data produced and/or used in the project is useable by third parties, in particular after the end of the project? If the re-use of some data is restricted, explain why 4 Describe data quality assurance processes 5 Specify the length of time for which the data will remain re-usable	3. The data will be available after the site engineering is finish. But when project is finish it belongs to Building/site owner. Data usage by third parties must be requested to Building Owner. 4. The data quality is under responsibility of the entity in charge of exploration. 5. No time limit.
.3. Allocation of resources	1 Estimate the costs for making your data FAIR. Describe how you intend to cover these costs 2 Clearly identify responsibilities for data management in your project 3 Describe costs and potential value of long-term preservation	1. The digital platform proposed by SEP provides a wide range of standard communication protocols. If during the project it is necessary to develop some communication protocol to share data, we have to evaluate the implementation and development. The costs will be estimated according to the development time. 2. WP leaders. 3. Data storage space is limited to the space available on the controller and/or digital platform installed on a PC or Virtual Machine. The controller's memory does not allow expansion. The memory of the digital platform can be increased but it is necessary to modify the characteristics of the PC or VM (for example number of disks).
4. Data security	1 Address data recovery as well as secure storage and transfer of sensitive data	1. Secure data transmission is only possible through API's. The data is stored in the local controller or in the BMS digital platform. It is necessary to define the architecture to implement
5. Ethical aspects	1 To be covered in the context of the ethics review, ethics section of DoA and ethics deliverables. Include references and related technical aspects if not covered by the former	1. According to DoA
6. Other	1 Refer to other national/funder/sectorial/departmental procedures for data management that you are using (if any)	1. Nothing more to add. During the progress of the project we will add other procedures

22. VUB

DMP component	Issues to be addressed	Explanation

1. Data summary	• State the purpose of the data collection/generation
	• Explain the relation to the objectives of the project
	• Specify the types and formats of data generated/collected
	• Specify if existing data is being re-used (if any)
	• Specify the origin of the data
	• State the expected size of the data (if known)
	• Outline the data utility: to whom will it be useful
		1
		• Purpose: Data is generated by pilot sites: Brussels University Hospital Micro-Grid Energy Management System (EMS data) and Green Energy Park, smart multi-energy living lab (to be implemented).
		• Project Objectives:
		  ○ Integrate over 30 energy and non-energy services (mobility) and evaluate the added value for the stakeholders' integration of SAREF compliant household appliances and uni- & bi-directional chargers.
		  ○ Implement and demonstrate future business model for P2P trading and V2G
		• Types and formats: smart meter and appliance gateway readings in SNMP, Modbus/IP, BACNet/IP, … collected in SQL databases (structured data), query results can be exported as CSV or other desired formats.
		• Existing data: historical BMS data
		• Origin: University Hospital BMS and multi-energy living lab monitoring
		• Size: BMS data is now ca. 8 GB/week
		• Utility:
		  ○ Evaluate energy management systems at building & neighbourhood level as well as interacting with the grid
		  ○ Evaluate P2P services and standardized interface with the distribution network

2. FAIR Data 2.1. Making data findable, including	• Outline the discoverability of data (metadata provision) • Outline the identifiability of data and refer to standard identification mechanism. Do you	2 2.1 • Discoverability: source of data will be identifiable as part of the structured approach of data capturing

provisions for metadata	make use of persistent and unique identifiers such as Digital Object Identifiers? • Outline naming conventions used • Outline the approach towards search keyword • Outline the approach for clear versioning • Specify standards for metadata creation (if any). If there are no standards in your discipline describe what type of metadata will be created and how	• Identification mechanism, naming convention, keywords, versioning, metadata: TBC
2.2 Making data openly accessible	• Specify which data will be made openly available? If some data is kept closed provide rationale for doing so • Specify how the data will be made available • Specify what methods or software tools are needed to access the data? Is documentation about the software needed to access the data included? Is it possible to include the relevant software (e.g. in open source code)? • Specify where the data and associated metadata, documentation and code are deposited • Specify how access will be provided in case there are any restrictions	2.2 • Openly available: yes, all available and necessary data is shared • Data is made available through (S)FTP shares on our servers, API interfaces (TBD) or if necessary direct access to the SQL databases • Access method: remote mount of share, through API (documentation will be provided once API's are developed) • Deposit: all the data, metadata and documentation will reside on pilot's servers, located in Brussels • Access provision: authentication credentials for mounting of SFTP share will be provided to partners through safe mechanism
2.3. Making data interoperable	• Assess the interoperability of your data. Specify what data and metadata vocabularies, standards or methodologies you will follow to facilitate interoperability.	2.3 • Interoperability: TBD, we will follow all necessary guidelines given regarding vocabularies, standards and methodologies • Vocabulary: SAREF compliant where possible

	• Specify whether you will be using standard vocabulary for all data types present in your data set, to allow inter-disciplinary interoperability? If not, will you provide mapping to more commonly used ontologies?	
2.4. Increase data re-use (through clarifying licences)	• Specify how the data will be licenced to permit the widest reuse possible • Specify when the data will be made available for re-use. If applicable, specify why and for what period a data embargo is needed • Specify whether the data produced and/or used in the project is useable by third parties, in particular after the end of the project? If the re-use of some data is restricted, explain why • Describe data quality assurance processes • Specify the length of time for which the data will remain re-usable	2.4 • Licensing: no data licensing is applicable (TBC), ownership of data stays with pilot. • Available for re-use: no data-embargo • Third party: no restrictions in place (TBC) • Quality Assurance: University Hospital EMS data is externally monitored; system functioning support is under external contract. • Length of Time: no limitations
3. Allocation of resources	• Estimate the costs for making your data FAIR. Describe how you intend to cover these costs • Clearly identify responsibilities for data management in your project • Describe costs and potential value of long-term preservation	3 • Costs will be covered by project budget, where applicable, to be further discussed and decided • Responsibility: responsibility for (new) data availability lies with pilot site operators (Brussels Health Campus, Green Energy Park VZW), project data management and provisioning is responsibility of VUB under the guidance of VUB Data Protection Officer (DPO) • Long term preservation: estimation is ca. 8GB/week = ca. 400GB/year; commercial backup offer is 0.2 euro/GB per month, so ca. 1.000 euro/year
4. Data security	• Address data recovery as well as secure storage and transfer of sensitive data	4 • Recovery from back-up in remote datacenter, secure storage on on-prem servers, secure data transfer through SFTP

5. Ethical aspects	• To be covered in the context of the ethics review, ethics section of DoA and ethics deliverables. Include references and related technical aspects if not covered by the former	5 • Covered by ethics review, ethics sections and ethics deliverables
6. Other	• Refer to other national/funder/sectorial/departmental procedures for data management that you are using (if any)	6 • N/A

23. IMEC

DMP component	Issues to be addressed	Explanation
1. Data summary	• State the purpose of the data collection/generation • Explain the relation to the objectives of the project • Specify the types and formats of data generated/collected • Specify if existing data is being re-used (if any) • Specify the origin of the data • State the expected size of the data (if known) • Outline the data utility: to whom will it be useful	**WP6** • Processing of data from the different pilot sites and test facilities to calculate KPIs in an automated and non-automated way. • The calculation of the KPIs allows to monitor and evaluate the deployed use cases and services in the different pilots. • Data will be collected in different formats depending on the specific monitored solution, test facility and pilot implementation. • A subset of the data collected by the different pilot sites will be reused to calculate the selected KPIs. • The data comes from pilot and test facility monitoring systems, survey results from pilot participants, inputs from pilot leads. • Size not known at the moment. • Calculation of the selected KPIs allows to perform pilot specific and cross-pilot evaluations of the designed reference architecture and the newly developed services, use cases, APIs and digital platforms within the project.

		WP7 • Data will be generated and processed in the different pilot sites in order to test the interoperability of the energy communities use case. • The data will be used to demonstrate and validate new energy management functionalities and business models • Data will be generated and collected in different formats depending on the specific monitoring solution, test facility, pilot implementation and grid API • No existing data is available for reusing • Data comes from pilot and test facility monitoring systems, entities involved in the use case and inputs from pilot leads. • Size not known at the moment. • Data will be used to perform pilot specific and cross-pilot evaluations of the designed reference architecture and the newly developed services, use cases, APIs and digital platforms within the project.
2. FAIR Data 2.1. Making data findable, including provisions for metadata	• Outline the discoverability of data (metadata provision) • Outline the identifiability of data and refer to standard identification mechanism. Do you make use of persistent and unique identifiers such as Digital Object Identifiers? • Outline naming conventions used • Outline the approach towards search keyword • Outline the approach for clear versioning • Specify standards for metadata creation (if any). If there are no standards in your discipline describe what type of metadata will be created and how	**WP6** • When calculating the KPIs, appropriate metadata will be provided (e.g. kpi description, date of calculation, calculation frequency, method of calculation (automatic or manual), calculation period, responsible partner, original data provider, foreseen date for next calculation, etc.) • The most appropriate approach for the kpi identification will be investigated • Naming conventions will be in line with SAREF ontology. • The used SAREF ontology will define how search parameters are specified. • Versioning of the calculated KPIs will be based on standard approaches. • Metadata will be specified in line with the SAREF ontology. Other approaches will be investigated as well (e.g. NGSI). **WP7** • Data will be made available • We will further investigate the best approach for uniquely identify our datasets • Naming conventions will be in line with SAREF ontology. • Collected data will use the SAREF ontology to define keywords.

		• Data versioning will be based on standard approaches followed by other pilot sites. • Metadata will be specified in line with the SAREF ontology. Other approaches will be investigated as well (e.g. NGSI).
2.2 Making data openly accessible	• Specify which data will be made openly available? If some data is kept closed provide rationale for doing so • Specify how the data will be made available • Specify what methods or software tools are needed to access the data? Is documentation about the software needed to access the data included? Is it possible to include the relevant software (e.g. in open source code)? • Specify where the data and associated metadata, documentation and code are deposited • Specify how access will be provided in case there are any restrictions	**WP6** • Access rights to the calculated KPIs will be defined together with the pilot leads and will be based on IP sensitiveness. • The calculated APIs will be made available through REST APIs. • A wide range of tools and software libraries exist to access REST APIs. A well-known tool for testing is Postman (https://www.postman.com). • The data and metadata will be hosted on InterConnect cloud resources of platforms of responsible partners. • Restricted access will be defined together with the pilot leads and original data owners. **WP7** • We will make data publicly available only if it is anonymized or aggregated. Privately kept data will only occur under use case requirements that will be further defined together with the pilot leads and will be based on IP sensitiveness. • Data will be made available through REST APIs. • Any REST API application (standard or custom-made) will be able to access through the given URL. • The data and metadata will be hosted on InterConnect cloud resources of platforms of responsible partners. • Restricted access will be defined together with the pilot leads and original data owners.
2.3. Making data interoperable	• Assess the interoperability of your data. Specify what data and metadata vocabularies, standards or methodologies you will follow to facilitate interoperability. • Specify whether you will be using standard vocabulary for all data types present in your	**WP6** • Data and metadata will be specified in line with the SAREF ontology. **WP7** • Data and metadata will be specified in line with the SAREF ontology. • Vocabulary will also be used in line with the SAREF ontology.

	data set, to allow inter-disciplinary interoperability? If not, will you provide mapping to more commonly used ontologies?	
2.4. Increase data re-use (through clarifying licences)	• Specify how the data will be licenced to permit the widest reuse possible • Specify when the data will be made available for re-use. If applicable, specify why and for what period a data embargo is needed • Specify whether the data produced and/or used in the project is useable by third parties, in particular after the end of the project? If the re-use of some data is restricted, explain why • Describe data quality assurance processes • Specify the length of time for which the data will remain re-usable	**WP6** • The calculated KPIs are meant to be used within the InterConnect project. If during the project it turns out that it is useful to make some of these KPIs publicly available, open licenses (like Apache 2.0, GPL, …) will be investigated. • The details of how data will be made available (if re-use is found to be applicable) will be specified during the project. • The calculated KPIs are primarily intended for use within the InterConnect project. If it turns out that data could be made available to third parties, data access will be defined together will all concerned partners. • Common best practices will be followed to assure data quality. • Reusability of the data and associated time period will become clear during the project. **WP7** • Data is meant to be used within the InterConnect project. Again, if after the project data needs to be kept publicly available, open licenses will be investigated. • The details of how data will be made available (if re-use is found to be applicable) will be specified during the project. • Collected and generated data are primarily intended for use within the InterConnect project. If it turns out that data could be made available to third parties, data access will be defined together will all concerned partners. • Common best practices will be followed to assure data quality. • Re-usability of the data and associated time period will become clear during the project. •
3. Allocation of resources	• Estimate the costs for making your data FAIR. Describe how you intend to cover these costs	**WP6** • Costs will be assessed during WP6 execution.

	• Clearly identify responsibilities for data management in your project • Describe costs and potential value of long-term preservation	• Data management will be the shared responsibility of the original data owners, pilot leads, WP6, WP7 and task leads and the Ethics and Data Protection Committee of InterConnect. • The value of long-term preservation and associated costs will be assessed during the project. **WP7** • Costs will be assessed during WP7 execution. • Data management will be the shared responsibility of the original data owners, pilot leads, WP7 partners and task leads and the Ethics and Data Protection Committee of InterConnect. • The value of long-term preservation and associated costs will be assessed during the project.
4. Data security	• Address data recovery as well as secure storage and transfer of sensitive data	**WP6** • The generated KPIs will be stored in a highly secure data platform with daily backups. For data transfer state-of-the-art secure APIs will be used. **WP7** • Generated and collected data will be stored in a highly secure data platform with daily backups. For data transfer state-of-the-art secure APIs will be used.
5. Ethical aspects	• To be covered in the context of the ethics review, ethics section of DoA and ethics deliverables. Include references and related technical aspects if not covered by the former	**WP6** • Ethics aspects are covered in the DoA. **WP7** • Ethics aspects are covered in the DoA.
6. Other	• Refer to other national/funder/sectorial/departmental procedures for data management that you are using (if any)	**WP6** • No necessary additional procedures identified at the moment **WP7** • No necessary additional procedures identified at the moment

24. DUCOOP

DMP component	Issues to be addressed	Explanation
1. Data summary	• State the purpose of the data collection/generation • Explain the relation to the objectives of the project • Specify the types and formats of data generated/collected • Specify if existing data is being re-used (if any) • Specify the origin of the data • State the expected size of the data (if known) • Outline the data utility: to whom will it be useful	Purpose of collection - Visualisation of Consumer data (heat demand (district heating & SHW), electricity consumption, water consumption data) on a household dashboard - Optimisation of district energy use - Construction of predictive models to allow optimisation of district energy use (current and future) Relation to project objectives - User experiences and demands (How they *evaluate* the tools and services that are being developed during the Interconnect project. Where their specific *needs* are to make there residential living environment more comfortable and what could *incentivise* them to participate in a smart energy system (tariff schemes, energy savings, environmental footprint, etc.) Types of data - Collective energy production (Local RES/waste heat recovery) and consumption data (EV-charging, decentralized water treatment plant, vacuum sewer system, district heating system, etc). Existing data could be used to benchmark the Ghent demo site against other districts
2. FAIR Data 2.1. Making data findable, including provisions for metadata	• Outline the discoverability of data (metadata provision) • Outline the identifiability of data and refer to standard identification mechanism. Do you make use of persistent and unique identifiers such as Digital Object Identifiers? • Outline naming conventions used • Outline the approach towards search keyword	Some generalized data might be used for scientific research or vulgarizing communications (Climate awareness/ Visualisation on energy saving measures/ optimization of Local RES) Other data will not be shared (confidential)

	• Outline the approach for clear versioning • Specify standards for metadata creation (if any). If there are no standards in your discipline describe what type of metadata will be created and how	
2.2 Making data openly accessible	• Specify which data will be made openly available? If some data is kept closed provide rationale for doing so • Specify how the data will be made available • Specify what methods or software tools are needed to access the data? Is documentation about the software needed to access the data included? Is it possible to include the relevant software (e.g. in open source code)? • Specify where the data and associated metadata, documentation and code are deposited • Specify how access will be provided in case there are any restrictions	None/ data exclusively confidential Some generalized data shared for scientific research/vulgarizing communications
2.3. Making data interoperable	• Assess the interoperability of your data. Specify what data and metadata vocabularies, standards or methodologies you will follow to facilitate interoperability. • Specify whether you will be using standard vocabulary for all data types present in your data set, to allow inter-disciplinary interoperability? If not, will you provide mapping to more commonly used ontologies?	Most data will be used confidentially and not shared with other partners/ third parties DuCoop/OpenMotics have worked on a harmonization of network architecture both at the residential level (home automation) as the industrial level (PLC monitoring of district heating, PV-installations, water treatment plant, EV charging, etc.)

2.4. Increase data re-use (through clarifying licences)	• Specify how the data will be licenced to permit the widest reuse possible • Specify when the data will be made available for re-use. If applicable, specify why and for what period a data embargo is needed • Specify whether the data produced and/or used in the project is useable by third parties, in particular after the end of the project? If the re-use of some data is restricted, explain why • Describe data quality assurance processes • Specify the length of time for which the data will remain re-usable	Most data will be used confidentially and not shared with other partners/ third parties Data from end-users (residents) can only be used with confirmation of the participant (GDPR)
3. Allocation of resources	• Estimate the costs for making your data FAIR. Describe how you intend to cover these costs • Clearly identify responsibilities for data management in your project • Describe costs and potential value of long-term preservation	No intentions to make data FAIR Responsible for compiling data in a way that makes it understandable and useable for other members of Interconnect consortium Negligible costs for long-term preservation Long-term high-frequency datasets (e.g. on second/minute base) will be reduced in resolution
4. Data security	• Address data recovery as well as secure storage and transfer of sensitive data	Protected data servers
5. Ethical aspects	• To be covered in the context of the ethics review, ethics section of DoA and ethics deliverables. Include references and related technical aspects if not covered by the former	Not applicable
6. Other	• Refer to other national/funder/sectorial/departmental procedures for data management that you are using (if any)	Internal data collection protocols of DuCoop/OpenMotics

25.3E

Did not answer or was not able to complete the information in time.

26.CORDIUM

Defined together with VITO. Please check table above.

27.VUA

DMP component	Issues to be addressed	Explanation
1. Data summary	• State the purpose of the data collection/generation • Explain the relation to the objectives of the project • Specify the types and formats of data generated/collected • Specify if existing data is being re-used (if any) • Specify the origin of the data	**The purpose of the data collection/generation:** In InterConnect, VU will collaborate with TNO and VolkerWessels (NL pilot leader) in the Dutch pilot in which data collected from a newly built residential building in Eindhoven will be used in the project for validation purposes. The validation will concern innovations and systems developed in InterConnect. VU will extend this data with existing data from external Open sources. **The relation to the objectives of the project (*objectives should be listed centrally in this doc*):** The data collected by VU in InterConnect relates to main objective 2 and 3 of the project: **Objective 2:** Demonstrate through large -scale pilots the implementation of a digital marketplace composed by different platforms and showcase the satisfaction of energy users needs with cost-effective solutions, allowing different market agents to create their value, and simultaneously

	• State the expected size of the data (if known) • Outline the data utility: to whom will it be useful	**Objective 3:** Ensure high levels of cybersecurity and data privacy. Co-creation involving citizens to design energy and non-energy services and applications that foster the active participation in new business models and grid operation, while ensuring comfortable, efficient, sustainable and healthier living environments **Specify the types and formats of data that can be generated/collected:** • Monitoring of electricity, cooling, heating and Domestic Hot Water consumption at residential property and Building Heating Network level • Indoor Temperature and presence of residents • Working conditions of heat pumps and solar systems • Comfort profiles of occupants • User and stakeholder needs and requirements • Surveys and questionnaires • Metadata on interoperability **Specify if existing data is being re-used (if any):** We plan to reuse existing Open Data sources, including Linked Open Data to enrich the raw data gathered in the pilot. **Specify the origin of the data:** • Device level (white goods, heat pumps, inverters,…) • Building Energy Management Systems • Sensors at residential level, DHN and boiler room level • Residents (collected through surveys or apps) • Additional third parties services (weather data,…) **The expected size of the data (if known):** • The dataset that VU, and the partners in the Dutch pilot will be working with is derived from approximately 100 households.

		Outline the data utility: to whom will it be useful: • Site stakeholders (residents, iCity) to validate the site‘s business case • Project stakeholders to validate the project’s objectives
2. FAIR Data 2.1. Making data findable, including provisions for metadata	• Outline the discoverability of data (metadata provision) • Outline the identifiability of data and refer to standard identification mechanism. Do you make use of persistent and unique identifiers such as Digital Object Identifiers? • Outline naming conventions used • Outline the approach towards search keyword • Outline the approach for clear versioning • Specify standards for metadata creation (if any). If there are no standards in your discipline describe what type of metadata will be created and how	The definition of metadata is one of the objectives of work package 2 and task 2.4 which is led by TNO. Any data published will be published “As Open as possible, as Closed as necessary”. We will republish datasets under Open and FAIR guidelines https://www.go-fair.org/fair-principles
2.2 Making data openly accessible	• Specify which data will be made openly available? If some data is kept closed provide rationale for doing so • Specify how the data will be made available • Specify what methods or software tools are needed to access the data? Is documentation about the software needed to access the data included? Is it possible to include the relevant software (e.g. in open source code)?	Any data published will be published “As Open as possible, as Closed as necessary”. Any data generated within the project will be published as Open Data insofar as existing licenses and institutions' ethical and legal procedures allow this. Personal data will not be made available in an open fashion in accordance with GDPR as well as any national legislation that applies. • Data that will be made available will be accessible through technical interfaces such as, but not limited to, API’s. • Methods and software tools needed to access data are to be detailed at a further stage. Documentation will be made available in due time.

	• Specify where the data and associated metadata, documentation and code are deposited • Specify how access will be provided in case there are any restrictions	• Where the data and associated metadata, documentation and code are deposited will also be considered at a later stage. • Access in case there are any restrictions to data will be dealt with on a case-by-case basis on request and after approval of relevant stakeholders.
2.3. Making data interoperable	• Assess the interoperability of your data. Specify what data and metadata vocabularies, standards or methodologies you will follow to facilitate interoperability. • Specify whether you will be using standard vocabulary for all data types present in your data set, to allow inter-disciplinary interoperability? If not, will you provide mapping to more commonly used ontologies?	Interoperability is a core principle of our data work. Interoperability and the definition of metadata vocabulary /ontology is one of the main objectives of work package 2 and task 2.4, and the pilot site managed by VolkerWessels/iCity will implement the semantic interoperability solution defined in WP2. We will use standard and Open (web) standards to publish vocabularies and metadata.
2.4. Increase data re-use (through clarifying licences)	• Specify how the data will be licensed to permit the widest reuse possible • Specify when the data will be made available for re-use. If applicable, specify why and for what period a data embargo is needed • Specify whether the data produced and/or used in the project is usable by third parties, in particular after the end of the project? If the re-use of some data is restricted, explain why • Describe data quality assurance processes • Specify the length of time for which the data will remain re-usable	Here as well, we will publish as Open as possible, as closed as necessary, in collaboration with pilot and work package partners. Details are to be discussed.
3. Allocation of resources	• Estimate the costs for making your data FAIR. Describe how you intend to cover these costs	We will be able to use facilities provided by the university, as well as National and International research infrastructures for publishing (research) data. As such, we do not expect additional costs.

	• Clearly identify responsibilities for data management in your project • Describe costs and potential value of long-term preservation	Responsibilities for data management will most probably be VolkerWessels for the pilot activities that have a direct involvement of VU and TNO.
4. Data security	• Address data recovery as well as secure storage and transfer of sensitive data	VU has extensive support for secure storage and transfer of sensitive data, including secure data archives and repositories. Here also, we connect to national research infrastructures. Where necessary, used policies can be assessed by will be assessed by the standing research ethics committee from the Department of Computer Science at VU.
5. Ethical aspects	• To be covered in the context of the ethics review, ethics section of DoA and ethics deliverables. Include references and related technical aspects if not covered by the former	Will be covered in the context of the ethics review, the ethics section of the DoA and ethics deliverables Where necessary, used policies can be assessed by will be assessed by the standing research ethics committee from the Department of Computer Science at VU.
6. Other	• Refer to other national/funder/sectoral/departmental procedures for data management that you are using (if any)	VU adheres to National principles for research data management (NWO). Where necessary, used policies can be assessed by will be assessed by the standing research ethics committee from the Department of Computer Science at VU.

28. HERON

DMP component	Issues to be addressed	Explanation
1. Data summary	• State the purpose of the data collection/generation • Explain the relation to the objectives of the project	● The purpose of the data collection is to identify HERON's customers consumption profiles and to provide IoT-assisted energy management services, based on their flexibility. ● The collected data will be used in the WP7 activities which include the large-scale demonstration and integration of the derived from the previous WP solutions.

	• Specify the types and formats of data generated/collected • Specify if existing data is being re-used (if any) • Specify the origin of the data • State the expected size of the data (if known) • Outline the data utility: to whom will it be useful	● At this point, we collect data related to active & reactive power, voltage, energy and power factor parameters. The collected data is presented in JSON format. ● There is the possibility to provide anonymized historical data for data analytics, provided that the respective users will give us their consent. ● Data are collected through the usage of accurate metering products that are installed in our users' homes. ● Unknown at this point, but a rough estimate is that they will not exceed 50GBs for the first year of the project. ● The collected data will be useful for the home owners, who will get a clear view of their consumption profiles, and to the Greek pilot partners, who will use them (in an anonymized format) for the implementation of the solutions that will be developed during the course of the project.
2. FAIR Data 2.1. Making data findable, including provisions for metadata	• Outline the discoverability of data (metadata provision) • Outline the identifiability of data and refer to standard identification mechanism. Do you make use of persistent and unique identifiers such as Digital Object Identifiers? • Outline naming conventions used • Outline the approach towards search keyword • Outline the approach for clear versioning Specify standards for metadata creation (if any). If there are no standards in your discipline describe what type of metadata will be created and how	● We will probably use a specific API endpoint for querying the requested data. ● The data will be provided in JSON format, using the "key: value" format and tags for site identification. ● No metadata creation is planned for the moment.

2.2 Making data openly accessible	• Specify which data will be made openly available? If some data is kept closed provide rationale for doing so • Specify how the data will be made available • Specify what methods or software tools are needed to access the data? Is documentation about the software needed to access the data included? Is it possible to include the relevant software (e.g. in open source code)? • Specify where the data and associated metadata, documentation and code are deposited • Specify how access will be provided in case there are any restrictions	● At this point we do not intend to make our collected data openly available due to GDPR considerations. Only Greek pilot stakeholders will have access to the anonymized data for the project activities. ● Data will be made available through well-defined REST endpoints with adequate documentation and access rights. ● The data and the associated code will be securely stored at a server that will be the property of HERON. ● Access will be provided to the Greek partners through APIs, whereas predefined credentials will be shared to the relevant stakeholders.
2.3. Making data interoperable	• Assess the interoperability of your data. Specify what data and metadata vocabularies, standards or methodologies you will follow to facilitate interoperability. • Specify whether you will be using standard vocabulary for all data types present in your data set, to allow inter-disciplinary interoperability? If not, will you provide mapping to more commonly used ontologies?	● We plan to follow the SAREF-compliant proposals and specifications of WP3 ● At this point, we intend to follow the proposed SAREF ontology in order to facilitate the interoperability with the InterConnect ecosystem.

2.4. Increase data re-use (through clarifying licences)	• Specify how the data will be licenced to permit the widest reuse possible • Specify when the data will be made available for re-use. If applicable, specify why and for what period a data embargo is needed • Specify whether the data produced and/or used in the project is useable by third parties, in particular after the end of the project? If the re-use of some data is restricted, explain why • Describe data quality assurance processes • Specify the length of time for which the data will remain re-usable	● This is a vague point at the moment. We will have to consult with our legal department in order to clarify this issue. ● Currently, there is no plan for providing open access to the gathered data. At a later stage, we will probably provide datasets containing aggregated and anonymized consumer data, provided that we have our users' and legal departments' consent. ● At this point, there is no data quality process defined.
3. Allocation of resources	• Estimate the costs for making your data FAIR. Describe how you intend to cover these costs • Clearly identify responsibilities for data management in your project • Describe costs and potential value of long-term preservation	● All of the costs will be covered by the project's resources. Cost estimation will be provided on a later stage. ● Data management will be performed by HERON analysts, whereas data protection will be ensured with a close collaboration of the energy management, IT and legal departments. ● Long-term preservation costs and potential value will be discussed on a later stage.
4. Data security	• Address data recovery as well as secure storage and transfer of sensitive data	● All the collected for the project's purposes data will be stored at HERON's servers, whose security and access will follow all the strict protocols that adhere to the company's standards. SSL encryption will be used for the secure data retrieval.
5. Ethical aspects	• To be covered in the context of the ethics review, ethics section of DoA and ethics	● We will follow strict GDPR procedures. Participating in the project users will have signed an adequate consent form, whereas only anonymized and aggregated data will be probably made accessible to actors outside the Greek pilot consortium.

	deliverables. Include references and related technical aspects if not covered by the former	
6. Other	• Refer to other national/funder/sectorial/departmental procedures for data management that you are using (if any)	None

29. COSM

DMP component	Issues to be addressed	Explanation
1. Data summary	• State the purpose of the data collection/generation • Explain the relation to the objectives of the project • Specify the types and formats of data generated/collected • Specify if existing data is being re-used (if any) • Specify the origin of the data • State the expected size of the data (if known) • Outline the data utility: to whom will it be useful	● Data collection is mandatory for data analytics (e.g., forecasting services) and data visualization purposes (real-time and historical). ● In the context of the Greek Pilot, data will be collected for the implementation of demand side flexibility scenarios in residential setups, based on a SAREFised IoT-enabled architecture. ● Data Categories: ○ Energy consumption/prosumption measurements (V, A, W, Whr). ○ Environmental/Comfort-related data, such as (indoor/outdoor) temperature and humidity, wind speed, cloud cover, precipitation, etc. ○ Other data categories e.g., related to presence, door/window status, etc. ● All data is “packaged” in JSON format. ● Existing data may be re-used exclusively for the INTERCONNECT project itself (e.g., for data analytics related activities). ● Energy consumption data are gathered from z-wave/Modbus/Wi-Fi power meters @fuse-box-level (3-phase, 1-phase), relay-level and/or socket-level (smart plugs) installed at residential premises. Indoor environmental data are gathered from commercial/custom sensors (Wi-Fi, ZigBee), while outdoor

		weather data from online services. Additional data e.g. motion/presence, are gathered from indoor (ZigBee) sensors. ● Data size is not quantifiable at the moment. To be calculated. ● Data will be useful to Greek Pilot stakeholders in order to provide concrete and applicable demand side flexibility services. In this scope, they may also prove useful for data analytics and forecast services.
2. FAIR Data 2.1. Making data findable, including provisions for metadata	• Outline the discoverability of data (metadata provision) • Outline the identifiability of data and refer to standard identification mechanism. Do you make use of persistent and unique identifiers such as Digital Object Identifiers? • Outline naming conventions used • Outline the approach towards search keyword • Outline the approach for clear versioning Specify standards for metadata creation (if any). If there are no standards in your discipline describe what type of metadata will be created and how	● No metadata provisioning mechanism is designed/implemented at this stage. ● The data format (JSON) used allows for data retrieval using the key:value format and tags for explicit site/meter identification. Data shall be explicitly queried using the REST API endpoint following the guidelines provided to the relevant stakeholders; tag values are used as a persistent and unique data identifier.
2.2 Making data openly accessible	• Specify which data will be made openly available? If some data is kept closed provide rationale for doing so • Specify how the data will be made available • Specify what methods or software tools are needed to access the data? Is documentation about the software needed to access the data included? Is it possible to include the relevant software (e.g. in open source code)?	● There are no plans for the moment to make the data openly available. Taking into account local legislation and GDPR directives, energy prosumption/consumption data are considered sensitive and personal information cannot be made publicly accessible. Possibly, some datasets could be made available provided that they are anonymised. ● Data/metadata, documentation and code are securely stored at COSMOTE's R&D backend infrastructure and repositories. ● Access will be provided in the scope of the project, by means of the commonly agreed upon endpoints and via specific REST APIs that are provided by the software itself and following specific requests by the relevant parties/partners. Predefined credentials will be used for user authentication and stakeholders (limited) data access.

	• Specify where the data and associated metadata, documentation and code are deposited • Specify how access will be provided in case there are any restrictions	
2.3. Making data interoperable	• Assess the interoperability of your data. Specify what data and metadata vocabularies, standards or methodologies you will follow to facilitate interoperability. • Specify whether you will be using standard vocabulary for all data types present in your data set, to allow inter-disciplinary interoperability? If not, will you provide mapping to more commonly used ontologies?	In the scope of WP3, all data should be made SAREF-compliant and adhere to proposed ontology modelling to ensure interoperability within the Interconnect ecosystem. Standardised methods are currently being used, e.g. JSON formatted data packets, thus facilitating mapping to proposed SAREF ontology.
2.4. Increase data re-use (through clarifying licences)	• Specify how the data will be licenced to permit the widest reuse possible • Specify when the data will be made available for re-use. If applicable, specify why and for what period a data embargo is needed • Specify whether the data produced and/or used in the project is useable by third parties, in particular after the end of the project? If the re-use of some data is restricted, explain why • Describe data quality assurance processes • Specify the length of time for which the data will remain re-usable	To be discussed and decided.
3. Allocation of resources	• Estimate the costs for making your data FAIR. Describe how you intend to cover these costs	• Related costs are covered within the scope of the project. Exact allocation to be described at a later stage.

	• Clearly identify responsibilities for data management in your project • Describe costs and potential value of long-term preservation	● Data protection will be handled by the entities DPO's, and via the Ethics and Data Protection Committee within the consortium. ● Long-term data preservation value is to be discussed at a later stage.
4. Data security	• Address data recovery as well as secure storage and transfer of sensitive data	Security measures are being taken in every step of the information flow between the various components of COSMOTE's backend infrastructure and the installed (remote) equipment to ensure secure data storage, transfer and recovery. More specifically: ● Communication between the installed gateways and COSMOTE's backend infrastructure is secured through SSL/TLS certificates on top of standard username/password authentication. ● Developers' access to the gateways (remotely) is secured by means of VPN tunnels. SSH Keys authentication system is also used to maximize security and prevent all unauthorised access. ● All data exchanged between various components of the backend system (MQTT broker, influxdb, grafana, etc.) is also encrypted via SSL/TLS certificates. ● Data resilience/recovery is achieved via RAID arrays on the cloud storage infrastructure and via systematic data backup on remote FreeNAS Servers with advanced snapshot capabilities. ● A NMS system constantly monitors the network traffic for suspicious port and/or interface activities and subsequently alerts the system administrator. ● Various firewall rules are applied to the network hierarchy. ● Network Segregation is configured via VLANs. ● Personnel access to physical equipment, e.g. servers, network switches, storage arrays, etc. is also restricted and monitored.
5. Ethical aspects	• To be covered in the context of the ethics review, ethics section of DoA and ethics deliverables. Include references and related technical aspects if not covered by the former	GDPR guidelines are followed whenever applicable. Data stored and shared between interested parties are strictly anonymised and the personal information matrix is securely stored at COSMOTE's repositories.
6. Other	• Refer to other national/funder/sectorial/departmental procedures for data management that you are using (if any)	To be checked.

30. ENEDIS

DMP component	Issues to be addressed	Explanation
1. Data summary	• State the purpose of the data collection/generation • Explain the relation to the objectives of the project • Specify the types and formats of data generated/collected • Specify if existing data is being re-used (if any) • Specify the origin of the data • State the expected size of the data (if known) • Outline the data utility: to whom will it be useful	Enedis, will collect after customer consent via the Linky meter, customer's data (see list below) to allow energy supplier and energy service providers of the customer to develop new services: • The household's daily consumption in kWh • The maximum power reached during the day • Information relating to the customer's contract (contracted power) and his price • Technical information relating to the network • Production data (if the customer also produces electricity) If the customer has made a request - only in this case - Enedis also collects: • The semi-hourly consumption curve
2. FAIR Data 2.1. Making data findable, including provisions for metadata	• Outline the discoverability of data (metadata provision) • Outline the identifiability of data and refer to standard identification mechanism. Do you make use of persistent and unique identifiers such as Digital Object Identifiers? • Outline naming conventions used • Outline the approach towards search keyword	This information is described in the supplier and third-party guides and data flows files (metadata) **Data identification by their flows names :** • **R15**: counting data • **R50:** the load curves for C5 points equipped (connection point connected at LV ≤ 36 kVA) with a communicating Linky counter and which have been requested on the SGE portal. • **R151:** the daily maximum powers for C5 points equipped with a communicating Linky meter and which have been requested on the SGE portal. • F15: Billing of point C5 point routing services • C15: Description of the Measurement Reference Points (PRM) of the C5 segment managed in the new Enedis IS. **File format:** All the files contained in the R15, R50, R151, F15 and 15 streams are XML files respecting the same XSD diagram. The encoding is of type UTF-8. **Naming rules:** A stream is composed of one or more XML files (depending on the number of PRMs) grouped in a zip archive.

	• Outline the approach for clear versioning • Specify standards for metadata creation (if any). If there are no standards in your discipline describe what type of metadata will be created and how	**Each stream respect a naming rule:** • Example : R15: Enedis_R15_ <destinataire> _ <num_contrat> _ <DIR_Enedis> _ <num_seq> _ <timestamp> .zip **Name of XML files:** • Example : R15: Enedis_R15_ <destinataire> _ <num_contrat> _ <DIR_Enedis> _ <num_seq> _XXXXX_YYYYY.xml In the XML flow we find the versioning Metadata standards are XML (see XSD for data format)
2.2 Making data openly accessible	• Specify which data will be made openly available? If some data is kept closed provide rationale for doing so • Specify how the data will be made available • Specify what methods or software tools are needed to access the data? Is documentation about the software needed to access the data included? Is it possible to include the relevant software (e.g. in open source code)? • Specify where the data and associated metadata, documentation and code are deposited • Specify how access will be provided in case there are any restrictions	**Open Data** : consumption or production of electricity at different geographical and time scales, mapping of the electricity network, electric mobility and data on consumption profiles are made public. **The publication of data will comply with the RGPD regulation.** **Data accessibility:** **Remote access to smart meter's data:** The Exchange Management platform (SGE) is an historic channel of exchange between Enedis and electricity suppliers. Since 2017, it has been accessible to any legal person. It provides access to technical and measurement data for individual customers. • **Technology**: web portal, SOAP, FTP webservices • Data access : authentication certificate must be obtained (communication between STP servers) **Local access to smart meter's data:** The digital information output or "customer tele-information" (TIC) is freely accessible under the faceplate of the smart meter. Data can be collect via a modem or a radio transmitter directly connected and supplied to the smart meter. The customer could be informed in real time. This functionality can be used by domestic management solutions. With this interface to collect different kind of measurement data: current tariff period, index values, power, voltage, state of virtual contacts, various information, etc. **The technical specifications and descriptions of these interfaces are public.**
2.3. Making data interoperable	• Assess the interoperability of your data. Specify what data and metadata vocabularies,	Enedis will evaluate the interoperability of the data produced and see how the data can be adapted Enedis uses a standard data format

	standards or methodologies you will follow to facilitate interoperability. • Specify whether you will be using standard vocabulary for all data types present in your data set, to allow inter-disciplinary interoperability? If not, will you provide mapping to more commonly used ontologies?	
2.4. Increase data re-use (through clarifying licences)	• Specify how the data will be licenced to permit the widest reuse possible • Specify when the data will be made available for re-use. If applicable, specify why and for what period a data embargo is needed • Specify whether the data produced and/or used in the project is useable by third parties, in particular after the end of the project? If the re-use of some data is restricted, explain why • Describe data quality assurance processes • Specify the length of time for which the data will remain re-usable	The smart meter's data processing is governed by regulations (**Energy Code, recommendations of the CNIL**). Data are send to the electricity supplier in particular for billing purposes. Otherwise, this information cannot be transmitted to a third party **without the explicit agreement of the customer**, and even less be sold. Enedis scrupulously follows the recommendations of the National Data Protection Commission (CNIL), in particular Deliberation **n ° 2012-404 of November 15th**, and **decree n ° 2019-536 of May 29**, 2019 **Consent Duration:** No deadline except in the event the data processing change (a new consent must be requested). Keeping proof of the consent (or withdrawal) for the duration.
3. Allocation of resources	• Estimate the costs for making your data FAIR. Describe how you intend to cover these costs • Clearly identify responsibilities for data management in your project • Describe costs and potential value of long-term preservation	Enedis has different holding periods depending on the types of data (Deliberation of the CRE November 16, 2016): **In the smart meter :** • Hourly consumption (consumption recorded every hour) is stored for 5 months. • Semi-hourly consumption (consumption recorded every 30 minutes) is stored for 2 months. **In the Enedis information system:** • Monthly consumption data is stored for 60 months. • Daily consumption is stored for 36 months. • The consumption curve histories are stored over a period of 24 months.

		A data management policy is in the process of validation
4. Data security	• Address data recovery as well as secure storage and transfer of sensitive data	Data circulating through the Enedis' digital chain are **encrypted.** The system is audited by the National Information Systems Security Agency (ANSSI). The Linky system respect ANSSI recommendations and Enedis' servers are all located in France.
5. Ethical aspects	• To be covered in the context of the ethics review, ethics section of DoA and ethics deliverables. Include references and related technical aspects if not covered by the former	• Enedis respect the **RGPD** and therefore respect the **privacy** and protect the **competitive information.** • **The data holding period is described** in the customer information documents. Enedis **collects the customer's consent** before any processing of its consumption data (via Internet on its personal space, non-secure Internet page or even through its supplier or third party)
6. Other	• Refer to other national/funder/sectorial/departmental procedures for data management that you are using (if any)	NA

31. ENGIE

DMP component	Issues to be addressed	Explanation
1. Data summary	• State the purpose of the data collection/generation • Explain the relation to the objectives of the project • Specify the types and formats of data generated/collected • Specify if existing data is being re-used (if any) • Specify the origin of the data	ENGIE, as the energy supplier, aggregator and/or service provider, will collect data in order to carry out the selected use cases in the French pilot (WP7), at the residential or business level. This data will be used to perform sub services such as: - Equipment and appliance control - Flexibility management - Customer reporting - Invoicing - Maintenance

	• State the expected size of the data (if known) • Outline the data utility: to whom will it be useful	The data will be useful to: - the end-user - ENGIE (including possibly research teams) - the DSO - external partners for contract execution Data collected could cover: - Electricity consumption - Electricity production - Data on equipment technical status and customer comfort status - Data on operation of equipment, tools and platforms - Customer technical information: equipment type,… - Customer preferences - Customer contracts - External signals - KPIs to assess the performance of the use case: operational, financial, commercial,… Data generated could cover: - Equipment control signals - Customer monitoring data Data origin could be (not exhaustive): - Household equipment - Smart meters - Customer provided information - External database or services Size of data:

		The size of each piece of data is limited but the platform will receive a lot of data during the project. These data have to be stored on several servers for more security and reliability. Each server must have a high storage capacity (hundreds of Go) and could be increased during the project depending on the needs.
2. FAIR Data 2.1. Making data findable, including provisions for metadata	• Outline the discoverability of data (metadata provision) • Outline the identifiability of data and refer to standard identification mechanism. Do you make use of persistent and unique identifiers such as Digital Object Identifiers? • Outline naming conventions used • Outline the approach towards search keyword • Outline the approach for clear versioning • Specify standards for metadata creation (if any). If there are no standards in your discipline describe what type of metadata will be created and how	ENGIE will aim at processing data that can be clearly identifiable and the means to achieve this goal will be addressed later in the project.
2.2 Making data openly accessible	• Specify which data will be made openly available? If some data is kept closed provide rationale for doing so • Specify how the data will be made available • Specify what methods or software tools are needed to access the data? Is documentation about the software needed to access the data included? Is it possible to include the relevant software (e.g. in open source code)?	Some data, like **commercial data, will be kept closed**. Data that need and can be made openly available will be determined later in the project and will be shared in accordance with GDPR.

	• Specify where the data and associated metadata, documentation and code are deposited • Specify how access will be provided in case there are any restrictions	
2.3. Making data interoperable	• Assess the interoperability of your data. Specify what data and metadata vocabularies, standards or methodologies you will follow to facilitate interoperability. • Specify whether you will be using standard vocabulary for all data types present in your data set, to allow inter-disciplinary interoperability? If not, will you provide mapping to more commonly used ontologies?	Interoperability of the data will be addressed in order to test the use case(s).
2.4. Increase data re-use (through clarifying licences)	• Specify how the data will be licenced to permit the widest reuse possible • Specify when the data will be made available for re-use. If applicable, specify why and for what period a data embargo is needed • Specify whether the data produced and/or used in the project is useable by third parties, in particular after the end of the project? If the re-use of some data is restricted, explain why • Describe data quality assurance processes • Specify the length of time for which the data will remain re-usable	Data available for reuse will be determined later in the project. As an example, data like electricity consumption in an anonymized form, might be made available for reuse.
3. Allocation of resources	• Estimate the costs for making your data FAIR. Describe how you intend to cover these costs	The costs for making the data FAIR will be estimated later in the project.

	• Clearly identify responsibilities for data management in your project • Describe costs and potential value of long-term preservation	
4. Data security	• Address data recovery as well as secure storage and transfer of sensitive data	ENGIE will manage data in compliance with GDPR, including encryption of sensitive data for transfers and anonymization of personal data. ENGIE will use data securization common practices like duplication of databases, personalized and strong authentication to access data, physical access control.
5. Ethical aspects	• To be covered in the context of the ethics review, ethics section of DoA and ethics deliverables. Include references and related technical aspects if not covered by the former	In accordance with GDPR, ENGIE informs and gets consent from the customers, especially on data storage duration, data usage and data deletion options. The access to sensitive data will be limited.
6. Other	• Refer to other national/funder/sectorial/departmental procedures for data management that you are using (if any)	

32. SENSI

DMP component	Issues to be addressed	Explanation
1. Data summary	• State the purpose of the data collection/generation • Explain the relation to the objectives of the project	- Collect data from sensors, smart metering data, and other devices inside buildings. Collect user profiles. Collect building contextual information related to Building equipment (e.g., location) - Achieve interoperability amongst devices. Control equipment and unify data. Expose data through APIs. - Building devices: measurements and commands (e.g., HVAC, electric consumption, lighting, temperature, air quality). Data is formatted in JSON.

	• Specify the types and formats of data generated/collected • Specify if existing data is being re-used (if any) • Specify the origin of the data • State the expected size of the data (if known) • Outline the data utility: to whom will it be useful	- N/A - Pilot sites - Highly scalable for cloud-based applications. By default 2TO, but could be extended to fit pilot's needs. - Energy & non-energy applications that leverage Sensinov's APIs: own and third-party business applications. We can also expose data to academia pending on data owner's approval.
2. FAIR Data 2.1. Making data findable, including provisions for metadata	• Outline the discoverability of data (metadata provision) • Outline the identifiability of data and refer to standard identification mechanism. Do you make use of persistent and unique identifiers such as Digital Object Identifiers? • Outline naming conventions used • Outline the approach towards search keyword • Outline the approach for clear versioning • Specify standards for metadata creation (if any). If there are no standards in your discipline describe what type of metadata will be created and how	- RESTFUL API with filter criteria (based data on metadata, see last point on this section) - IETF-RFC-4122 (Universal Unique Identifier) - IETF-RFC-4122 - Unified data model common vocabulary (ontology) - Versioning is included in the API's URL - Timestamp, location (e.g., GPS coordinates, floor, room, building), id, device type, device name, tags, manufacturer/provider.
2.2 Making data openly accessible	• Specify which data will be made openly available? If some data is kept closed provide rationale for doing so • Specify how the data will be made available	- All data can be made available subject to consent by the data owner (i.e., property owner or manager). - Via APIs - Open APIs available through Swagger.

	• Specify what methods or software tools are needed to access the data? Is documentation about the software needed to access the data included? Is it possible to include the relevant software (e.g. in open source code)? • Specify where the data and associated metadata, documentation and code are deposited • Specify how access will be provided in case there are any restrictions	- Data could be hosted at a commercial cloud or on-premises. - Export to other formats (Excel, PDF, etc.)
2.3. Making data interoperable	• Assess the interoperability of your data. Specify what data and metadata vocabularies, standards or methodologies you will follow to facilitate interoperability. • Specify whether you will be using standard vocabulary for all data types present in your data set, to allow inter-disciplinary interoperability? If not, will you provide mapping to more commonly used ontologies?	- Data will be structured based on the **SAREF ontology and exposed through a SPARQL end-point**. - SAREF ontology. Other ontologies could be considered if needed.
2.4. Increase data re-use (through clarifying licences)	• Specify how the data will be licenced to permit the widest reuse possible • Specify when the data will be made available for re-use. If applicable, specify why and for what period a data embargo is needed • Specify whether the data produced and/or used in the project is useable by third parties, in particular after the end of the project? If the re-use of some data is restricted, explain why • Describe data quality assurance processes	- Data is owned by the property owner / manager (pilots), who can define the subsequent use of the data. - During the project's lifecycle. - Use by third parties is possible, subject to data owner's consent as regards subsequent use.

	• Specify the length of time for which the data will remain re-usable	- Semantic enrichment capable of detecting faulty data. Rule-based fault detection and data filtering. - Configurable, based on data owner's choices.
3. Allocation of resources	• Estimate the costs for making your data FAIR. Describe how you intend to cover these costs • Clearly identify responsibilities for data management in your project • Describe costs and potential value of long-term preservation	- FAIR compliant, no additional cost is foreseen. - Project manager - No additional cost during the project's lifecycle.
4. Data security	• Address data recovery as well as secure storage and transfer of sensitive data	- Backup and data replication.
5. Ethical aspects	• To be covered in the context of the ethics review, ethics section of DoA and ethics deliverables. Include references and related technical aspects if not covered by the former	
6. Other	• Refer to other national/funder/sectorial/departmental procedures for data management that you are using (if any)	

33. WHIRLPOOL

Did not answer or was not able to complete the information in time.

34. RSE

Partner not involved in data collection activities.

35. POLIMI

Partner not involved in data collection activities.

36. CYBERGRID

DMP component	Issues to be addressed	Explanation

1. Data summary	• State the purpose of the data collection/generation
	• Explain the relation to the objectives of the project
	• Specify the types and formats of data generated/collected
	• Specify if existing data is being re-used (if any)
	• Specify the origin of the data
	• State the expected size of the data (if known)
	• Outline the data utility: to whom will it be useful
		• The data collected will be used in the cyberGRID's cyberNOC platform for the purpose of connecting to all 7 pilots, to offer flexibility services to the balancing market
		• The data will be used to validate the tools developed within the project need to fulfil the project goals
		• Collected data will be stored internally in the cyberNOC platform in the **proprietary type and formats, such as:**
		  ○ Power
		  ○ Capacity
		  ○ Availability
		  ○ Other related to specific asset: SOC, Temperature, etc.
		• Testing data, such as energy asset simulator will be used in the preliminary validations
		• The data will be produced in the project demos
		• Expected data is 2GB/month per connected energy asset
		• Within the project, the data will be useful to the developers to stress test the develop tools and/or updated functionalities within the cyberNOC. Also, it would be useful for the demos evaluators to provide project results.

2. FAIR Data 2.1. Making data findable, including provisions for metadata	• Outline the discoverability of data (metadata provision) • Outline the identifiability of data and refer to standard identification mechanism. Do you make use of persistent and unique identifiers such as Digital Object Identifiers? • Outline naming conventions used • Outline the approach towards search keyword • Outline the approach for clear versioning • Specify standards for metadata creation (if any). If there are no standards in your discipline describe what type of metadata will be created and how	• Talking about the energy assets which will be connected to the cyberNOC platform the naming conventions are completely up to the demo leader and are not forced • Internal meta data of the information stored within the cyberNOC are proprietary and thus users can not directly access them. The cyberNOC platform comes with the set of APIs, where different formats/standards can be used. The standard used in the project still needs to be defined.
2.2 Making data openly accessible	• Specify which data will be made openly available? If some data is kept closed provide rationale for doing so • Specify how the data will be made available • Specify what methods or software tools are needed to access the data? Is documentation about the software needed to access the data included? Is it possible to include the relevant software (e.g. in open source code)? • Specify where the data and associated metadata, documentation and code are deposited • Specify how access will be provided in case there are any restrictions	• Most of the data will be closed. Only the authorised personnel can read the data – energy asset owners. • The data will be available via cyberNOC web user interface while providing credentials

2.3. Making data interoperable	• Assess the interoperability of your data. Specify what data and metadata vocabularies, standards or methodologies you will follow to facilitate interoperability. • Specify whether you will be using standard vocabulary for all data types present in your data set, to allow inter-disciplinary interoperability? If not, will you provide mapping to more commonly used ontologies?	At this point in time, it is not clear what kind of the access will be defined within the project. In general, users of the cyberNOC will be using the proprietary data models, but for the purpose of interoperability to connect to the pilots, the project standards will be developed.
2.4. Increase data re-use (through clarifying licences)	• Specify how the data will be licenced to permit the widest reuse possible • Specify when the data will be made available for re-use. If applicable, specify why and for what period a data embargo is needed • Specify whether the data produced and/or used in the project is useable by third parties, in particular after the end of the project? If the re-use of some data is restricted, explain why • Describe data quality assurance processes • Specify the length of time for which the data will remain re-usable	• The data will be available to the users of the cyberNOC platform, while following the user consent
3. Allocation of resources	• Estimate the costs for making your data FAIR. Describe how you intend to cover these costs • Clearly identify responsibilities for data management in your project • Describe costs and potential value of long-term preservation	

4. Data security	• Address data recovery as well as secure storage and transfer of sensitive data	• The data within the cyberNOC platform is backed up regularly and thus the recovery is possible from the latest backup
5. Ethical aspects	• To be covered in the context of the ethics review, ethics section of DoA and ethics deliverables. Include references and related technical aspects if not covered by the former	
6. Other	• Refer to other national/funder/sectorial/departmental procedures for data management that you are using (if any)	

37. RDGFI

DMP component	Issues to be addressed	Explanation
1. Data summary	• State the purpose of the data collection/generation • Explain the relation to the objectives of the project • Specify the types and formats of data generated/collected • Specify if existing data is being re-used (if any) • Specify the origin of the data • State the expected size of the data (if known)	• Purpose: enable modelling for interoperability, IoT & energy management components of the digital platform and marketplace and evaluating impact • Relation to objectives: related to WP 4, 5, 7 & 9 • Types & formats: energy & non-energy related appliances (with the possibility of including charging stations) data & metadata including appliance consumption, status, manufacturing & model, location and similar, as well as non-appliance relevant data such as climate & lighting data. • Existing data: limited historical data is available on some already connected smart homes, and some historical data from eMobility assets (vehicles and charging stations) • Origin: smart appliances/meters/management-systems/charging stations, manually entered, publicly available, operators & retailers

	• Outline the data utility: to whom will it be useful	• Expected size: unknown • Utility: pilot-level stakeholders to validate business cases & InterConnect partners to validate the project's objectives
2. FAIR Data 2.1. Making data findable, including provisions for metadata	• Outline the discoverability of data (metadata provision) • Outline the identifiability of data and refer to standard identification mechanism. Do you make use of persistent and unique identifiers such as Digital Object Identifiers? • Outline naming conventions used • Outline the approach towards search keyword • Outline the approach for clear versioning • Specify standards for metadata creation (if any). If there are no standards in your discipline describe what type of metadata will be created and how	• Data will be exposed through the digital platform that will be developed • Standards for identification & naming conventions will be standardized in-line with consortium references recommendations & own experience
2.2 Making data openly accessible	• Specify which data will be made openly available? If some data is kept closed provide rationale for doing so • Specify how the data will be made available • Specify what methods or software tools are needed to access the data? Is	Data that's relevant to the stakeholders' interoperability & management requirements to achieve the project objectives is yet to be specified.

	documentation about the software needed to access the data included? Is it possible to include the relevant software (e.g. in open source code)? • Specify where the data and associated metadata, documentation and code are deposited • Specify how access will be provided in case there are any restrictions	
2.3. Making data interoperable	• Assess the interoperability of your data. Specify what data and metadata vocabularies, standards or methodologies you will follow to facilitate interoperability. • Specify whether you will be using standard vocabulary for all data types present in your data set, to allow inter-disciplinary interoperability? If not, will you provide mapping to more commonly used ontologies?	SAREF ontology will be used & extended & standardized following own experience & best practices to cover novel use cases in coordination with the consortium.
2.4. Increase data re-use (through clarifying licences)	• Specify how the data will be licenced to permit the widest reuse possible • Specify when the data will be made available for re-use. If applicable, specify why and for what period a data embargo is needed	In principle, Realdolmen and its Third Parties are not expected to provide any data. Aggregated and anonymous data provided by other partners will be managed instead. An agreement with the data owners for public re-use will be analysed, with Realdolmen and its Third Parties not defining any specific embargo.

	• Specify whether the data produced and/or used in the project is useable by third parties, in particular after the end of the project? If the re-use of some data is restricted, explain why • Describe data quality assurance processes • Specify the length of time for which the data will remain re-usable	
3. Allocation of resources	• Estimate the costs for making your data FAIR. Describe how you intend to cover these costs • Clearly identify responsibilities for data management in your project • Describe costs and potential value of long-term preservation	TBD
4. Data security	• Address data recovery as well as secure storage and transfer of sensitive data	In the project, the processing of personal data will be limited to what is only strictly necessary. By ensuring that no personal data are collected or received by Realdolmen and by any of its Third Parties, the potential privacy impact of our IT solutions is limited. This principle can be achieved by ensuring: - careful selection of the personal data, in relation to the purpose of the processing - applying anonymization - use of pseudonyms. If information is collected, stored or legitimately processed by one party, then this information will be shielded from other parties. This comes down to guaranteeing confidentiality. This principle can be achieved by ensuring: - encoding, encryption - anonymization, and - the use of pseudonyms. Dividing the processing or storage of different sources of data about the same person helps to ensure that a complete profile cannot be built up about a single person. This principle can be achieved by: -

		splitting up database tables where possible - removing personal ID's from the rows in these tables, to prevent them from being linked Personal data must be processed at the highest possible level of aggregation, and with the minimum possible detail at which it is (still) usable. The presentation of information will be sufficiently generalized so that it represents a large group of people. In this way, information can only be attributed to a single individual in a very limited number of cases and privacy is better protected. The group about which the information is collected needs to be made large enough. This principle can be achieved by: - aggregation by time - other anonymization techniques.
5. Ethical aspects	• To be covered in the context of the ethics review, ethics section of DoA and ethics deliverables. Include references and related technical aspects if not covered by the former	GDPR guidelines are adopted to ensure ethical principles involving informed consent, anonymisation and controlling access to data.
6. Other	• Refer to other national/funder/sectorial/departmental procedures for data management that you are using (if any)	Realdolmen and its Third Parties will not be collecting or using any non-anonymous data, our contribution will be part of an architecture that does not interface directly with individuals, so we expect data to be encrypted and aggregated by other partners. Confidentiality is ensured and any breach will be reported.

38. EDSO

Partner not involved in data collection activities.

39. OPENMOTICS

DMP component	Issues to be addressed	Explanation
1. Data summary	• State the purpose of the data collection/generation • Explain the relation to the objectives of the project • Specify the types and formats of data generated/collected • Specify if existing data is being re-used (if any) • Specify the origin of the data • State the expected size of the data (if known) • Outline the data utility: to whom will it be useful	Purpose of data collection • Visualisation of Consumption data. • Model and control devices in the energy community to optimize and predict the energy flows on building and district level Relation to project objectives • Create a digital flow to interact with end consumers and learn what are the key initiators for them to be part of a energy community(new type of services … comfort, being incentivised … financial savings, impact on environment) • And in general objectives of WP3 and WP7 Types of data • Collective energy production(PV, waste heat recovery), consumption(EV, district heating, …) and storage(Battery, warm water) • Private energy consumption(water, heat, electricity) Existing data will most likely be used to compare against. Expected size has not been calculated yet as the amount of devices and their data format/size is yet unknown. Data origin Is from the Belgian DuCoop/OpenMotics pilot “De Nieuwe Dokken” in Ghent Data utility: Not yet specified
2. FAIR Data 2.1. Making data findable, including provisions for metadata	• Outline the discoverability of data (metadata provision) • Outline the identifiability of data and refer to standard identification mechanism. Do you make use of persistent and unique identifiers such as Digital Object Identifiers? • Outline naming conventions used	There is a generic “metric” approach through which data is identifiable. A data metric is currently defined by its name, description, type and unit and can have a custom defined set of “tags” making them findable.

	• Outline the approach towards search keyword • Outline the approach for clear versioning • Specify standards for metadata creation (if any). If there are no standards in your discipline describe what type of metadata will be created and how	
2.2 Making data openly accessible	• Specify which data will be made openly available? If some data is kept closed provide rationale for doing so • Specify how the data will be made available • Specify what methods or software tools are needed to access the data? Is documentation about the software needed to access the data included? Is it possible to include the relevant software (e.g. in open source code)? • Specify where the data and associated metadata, documentation and code are deposited • Specify how access will be provided in case there are any restrictions	Not specified yet which data will be shared, most likely only anonymized/generalized data.
2.3. Making data interoperable	• Assess the interoperability of your data. Specify what data and metadata vocabularies, standards or methodologies you will follow to facilitate interoperability. • Specify whether you will be using standard vocabulary for all data types present in your data set, to allow inter-disciplinary	Data that can be shared is available via authenticated API's. For better interoperability the current idea is to foresee mapping to SAREF ontology.

	interoperability? If not, will you provide mapping to more commonly used ontologies?	
2.4. Increase data re-use (through clarifying licences)	• Specify how the data will be licenced to permit the widest reuse possible • Specify when the data will be made available for re-use. If applicable, specify why and for what period a data embargo is needed • Specify whether the data produced and/or used in the project is useable by third parties, in particular after the end of the project? If the re-use of some data is restricted, explain why • Describe data quality assurance processes • Specify the length of time for which the data will remain re-usable	Most of the data is confidential and can not be shared with other (3rd) parties. End-user data can only be used with confirmation of the participant(GDPR)
3. Allocation of resources	• Estimate the costs for making your data FAIR. Describe how you intend to cover these costs • Clearly identify responsibilities for data management in your project • Describe costs and potential value of long-term preservation	Not specified yet.
4. Data security	• Address data recovery as well as secure storage and transfer of sensitive data	Data is subject to daily backup. Data at rest is encrypted.
5. Ethical aspects	• To be covered in the context of the ethics review, ethics section of DoA and ethics deliverables. Include references and related technical aspects if not covered by the former	All data-related process are subject to GDPR

6. Other	• Refer to other national/funder/sectorial/departmental procedures for data management that you are using (if any)	

40. KEO

Did not answer or was not able to complete the information in time.

41. ABB

Did not answer or was not able to complete the information in time.

42. UNIK

Partner not involved in data collection activities.

43. DFKI

Did not answer or was not able to complete the information in time.

44. UASD

Did not answer or was not able to complete the information in time.

45. BSH

Did not answer or was not able to complete the information in time.

46. MIELE

Did not answer or was not able to complete the information in time.

47. WIRELANE

Did not answer or was not able to complete the information in time.

48. VAILLANT

Did not answer or was not able to complete the information in time.

49. DAIKIN

Did not answer or was not able to complete the information in time.

50. KNX

Partner not involved in data collection activities.