

DENiM

Deliverable D2.2 Data Management Plan

Date: 30.04.2021

Version: R1.0

Dissemination Level: PU



Project Number	:	958339
Project Title	:	Digital intelligence for collaborative Energy Management in Manufacturing – DENiM
Deliverable Dissemination Level	:	PU

Deliverable Number	:	D2.2
Title of Deliverable	:	Data Management Plan
Nature of Deliverable	:	Report
Internal Document Number	:	D2.2
Contractual Delivery Date	:	30 April 2021
Actual Delivery Date	:	30 April 2021
Work Package	:	WP2
Author(s)	:	Jean HERVEG (UNamur), A. McGibney (MTU)
Total number of pages (including cover)	:	22

Executive Summary

Deliverable 2.2 provides guidelines and support for the optimal exploitation of the research data during and after the DENiM project. It fixes the General Data Management Policy and reminds the focus of the project on the ethical and legal requirements related to the activities to be carried out by the partners. The document then describes the procedures applicable to the specific activities identified in the project and concerning namely:

- The DENiM Project Portal security & privacy;
- The identification and recruitment procedure for human participants at the pilot sites;
- The informed consent to participate in the DENiM pilot activities;
- The organisation specific ethics approval;
- The protection of personal data at DENiM pilot sites;
- The DENiM stakeholder boards & Forum;
- The Exploitation and IPR aspects.

This document may be reviewed or updated if and where necessary.

Keyword list

Data Governance, Data Management Policy, Ethical and Legal Requirements, Data Protection, Research Participants, Informed Consent, Pilot Sites, Stakeholders, Forum, Dissemination and IPR

Document History

Date	Revision	Comment	Author/Editor	Affiliation
29.03.21	V0.1	Draft	J. HERVEG	UNamur
30.03.21	V0.1	Draft	J. HERVEG	UNamur
10.04.21	V0.2	Revision by IDENER	C. Leyva	IDENER
15.04.21	V0.3	Internal Review & Revision	A. McGibney	MTU
16.04.21	V0.4	Finalization of the draft	J. HERVEG	UNamur
19.01.21	V0.5	Finalization of the draft	J. HERVEG	UNamur
20.04.21	V0.6	Minor corrections and layout modifications	J. Kortelainen	VTT
22.04.21	V0.7	Finalization of the Deliverable	J. HERVEG	UNamur
28.04.21	V1.0	Approved by STM, minor formatting	J. Kortelainen	VTT
29.04.21	R1.0	Released for submission	A. McGibney	MTU

Table of Contents

1	Introduction.....	5
1.1	Objectives of the Data Management Plan	5
1.2	Scope of the Data Management Plan	5
2	General Data Management Policy.....	7
2.1	Project Data Management Process.....	7
2.2	Data Set Categories	11
2.2.1	Project Documentation and Scientific Results	11
2.2.2	Baseline Data.....	11
2.2.3	Pilot Site Use Case Data.....	12
2.2.4	DENiM System Data.....	12
3	Open Data Access Policy.....	13
4	Ethical and Legal Requirements	14
5	Identification and Recruitment Procedure for Human Participants at the Pilot Sites.....	15
6	Organisation Specific Ethics Approval	16
7	DENiM Stakeholder Boards & Forum	17
8	Exploitation and IPR	18
8.1	IPR and Innovation Management.....	18
8.2	Results Exploitation	18
9	Review of the Data Management Plan.....	19
	Annex 1: Template of the Data Management Form to be Fulfilled by the Partners	20

Glossary

CETS	Council of Europe Treaty Series
DMP	Data Management Plan
DPO	Data protection officers
EDPB	European Data Protection Board
EEAB	External Expert Advisory Board
EELAB	External Ethical and Legal Advisory Board
ELM	Ethical and Legal Manager
ETS	European Treaty Series
FAIR	Findable, Accessible, Interoperable and Reusable
GDPR	General Data Protection Regulation
GDPR	General Data Protection Regulation
IoT	Internet of Things
IPR	Intellectual Property Rights
PEB	Project Executive Board
POPD	Protection of personal data
SWOT	Strengths, Weaknesses, Opportunities and Threats

1 Introduction

The overarching objective of the DENiM project is the development of an interoperable digital intelligence platform to enable a collaborative approach to industrial energy management. DENiM aims at providing an integrated toolchain to provision advanced digital services including secure edge connectivity leveraging IoT, data analytics, digital twin, energy modelling and automation culminating in the delivery of continuous energy impact assessment, together with energy control and optimisation across existing production facilities, processes and machines.

1.1 Objectives of the Data Management Plan

The goal of the Data Management Plan [in short “the DMP”] is to ensure firstly that all relevant data management policies are adhered to and also to ensure reliable data can be extracted in a reliable and consistent manner to be used for the DENiM project development. The DMP will also provide guidance and support to ensure the optimal exploitation of the research data during and after the DENiM project.

The DMP is centred around the lifecycle of the research data and will inform project partners how to describe and document the following aspects during the completion of their tasks:

- ❖ The research data (e.g. data content, data sets, data categories and data characteristics (including data sets size and metadata));
- ❖ The origin of the research data (the way data have been collected, created or generated);
- ❖ The standards, formats and methodologies applied to the research data;
- ❖ The ethical and legal issues regarding the research data;
- ❖ The way to store and archive the research data (data curation and data preservation);
- ❖ The data access and data sharing policies inside the consortium and with respect to requests from external entities (data availability and data exploitation) (including data access for review and scrutiny and their re-use (data utility criteria)).

The DMP has been developed in accordance to the H2020 Programme Guidelines on FAIR Data Management principles (version 3.0 – 26 July 2016)¹. The Guidelines’ template has been used to capture this information as described above and is presented in Annex 1 of this deliverable. The template is a key component to the project data management procedure and indicates the minimum requirements to collect, store, analysed, and publish data in a consistent way according to the FAIR principles.

1.2 Scope of the Data Management Plan

The DMP is viewed as a living document, as such it will be reviewed regularly aligned with the project work plan and updated if and where necessary throughout the project lifecycle. All project partners will be informed of any changes made to this document and procedures. Common standards, data strictures, folder structure and identifiers will be agreed within the Project Executive Board (PEB) meetings and informed by the external Ethical and Legal Advisory Board (EELAB), and made available via the internal communication processes (e.g. meeting minutes) and during the meeting of the subsequent General Assembly (GA).

¹ https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf



D2.2: Data Management Plan

This deliverable is supported by the information captured in the context of the following deliverables:

- **Deliverable 10.1 Humans: H – Requirement No. 1** presents the procedures and requirements that will be used to identify/recruit research participants for the DENiM pilot site scenarios and the informed consent procedure that will be used to support the participation of humans
- **Deliverable 10.2 Protection of Personal Data: POPD – Requirement No. 2** presents the protection of personal data principles that the DENiM consortium will adhere to in order to safeguard the rights and freedoms of the research participants (see *infra*, Section 4. Specific Procedures).

As such the DMP will reference, where appropriate to these specific deliverables link as they map to the overall project data management procedures.

The deliverable is organised as follows. Section 2 describes the General Data Management Policy. Section 3 details the Open Data Access Policy. Section 4 concerns the Ethical and Legal Requirements. Section 5 refers to the process for recruiting human participants at pilot sites and the informed consent required to participate to the DENiM activities at the pilot sites. Section 6 concerns the requirements regarding getting the prior approval from ethical bodies. Section 7 focuses on the DENiM Stakeholder Boards and Forum. Section 8 covers the aspects relating to the exploitation of the research results and to intellectual property rights (IPR). Annex 1 contains a template of data management form that should be fulfilled by the partners.



2 General Data Management Policy

Project research data will be collected and processed throughout the DENiM project in full accordance with the ethical rules and standards of the HORIZON 2020 Programme.

The partners will comply with both the ethical principles and the relevant national, European and international legal instruments. At the European level, the latter refers namely to:

- ❖ The European Convention on Human Rights (and especially the requirements that can be deduced from the case law of the European Court of Human Rights on article 8 (right to respect for private life));
- ❖ The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe, CETS No. 108, 1981) (including its latest protocol);
- ❖ The Charter of Fundamental Rights of the European Union (especially articles 7 & 8 on the right to respect for private life and to data protection) and the requirements that can be deduced from the case law of the European Court of Justice;
- ❖ The General Data Protection Regulation (GDPR);
- ❖ The Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (and the Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications));
- ❖ The Commission Regulation n° 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications;
- ❖ The Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union;
- ❖ The Regulation 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union;
- ❖ The Directive 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (to be transposed before 17 July 2021).

More specifically, the DENiM project will comply with the specific national legislations applicable to the activities of the project, and the work carried out at each of the four Pilot sites. It will also comply with any organisational or institutional rules and procedures that are in place where the project activities will be conducted.

Partners will document these specific national legislations and organisational or institutional rules and procedures.

2.1 Project Data Management Process

DENiM will follow a data management lifecycle as shown in Figure 1. The fulcrum of this process will be Data Protection Officers (DPO) identified at each of the pilot sites and the EELAB as they will provide continuous monitoring of the process utilised throughout the project. They will provide advice and approval on mechanisms used to collect, protect, store and retain data as set out by the project team to ensure they are in line with the national, organisational and institutional guidelines in addition to

those described above. In addition, the EELAB including the project WP2 leader (data protection advisor) will continually monitor any associated legal and ethical issues for the data being collected by the project.

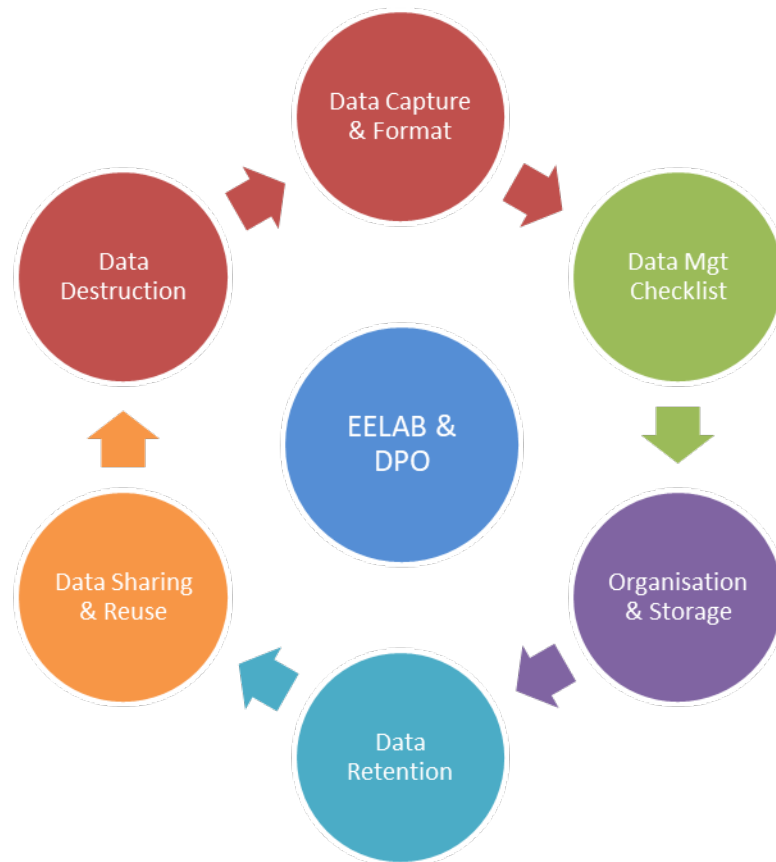


Figure 1: DENiM Data Management Lifecycle

A data management checklist will be used by the project as a verification point to ensure the data to be collected is assessed and approved by the DPO and EELAB. This ensures that a clear mechanism for capturing, storing, retention and monitoring is put in place before actual data collection occurs. Figure 2 presents the workflow used by the DENiM project.

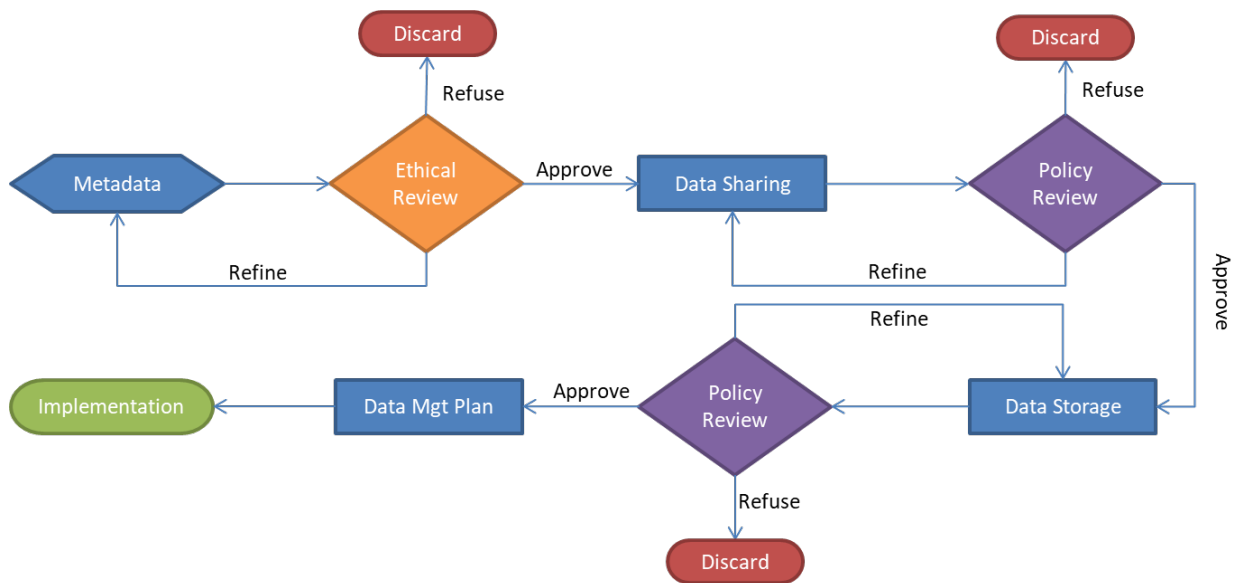


Figure 2: Data Management Checklist

The workflow begins by the data set owner defining a metadata description of the data that will be captured, created or used by the project. It is also important to record this detail to help the project and subsequent users understand why and how the data was created. The minimal information required as input to the first checkpoint is described below and captured as part of the DMP template provided in Annex 1:

What is the nature of the data?	e.g. Business data, personal data, data types
Purpose for collection?	e.g. Baseline, research, validation
How will data be created (captured)?	e.g. interview data, questionnaires, imaging, experimental measurements etc. what is the data source, how often
Data Owner?	Who owns the data
What data formats will be used?	e.g. File formats such as excel, word, open source etc. Consider choice of data formats such as: will the data formats meet certain specifications including international or national standards, widely used, is it accepted as best practice in this discipline
Will existing data be used?	If so what is the relationship to the existing data?
How will metadata be captured, created and managed?	How will descriptive information regarding the type of data being collected be managed?
Data Curator?	Who will manage the data after it is collected
Consent Required?	Is consent required to collect the data, if so from whom and how will it be sought.
Will there be special hardware or software requirements for this data?	Are there any IT related requirements to capture this data that need to be considered?

Based on the data captured above, this form will be reviewed by the project Ethical and Legal Manager (ELM) in conjunction with the EELAB and the appropriate DPOs to assess the impact collecting this data set may have on the ethical or legal considerations of the DENiM project. At this point the project will

be instructed by the ELM to either refine the metadata specifications to include additional information, refuse the data as not adhering to the ethical requirements of the project (as set out in ethical deliverables) or alternatively approve the data set to the next stage of the workflow. Approval at this point indicates that no sensitive personal information is recorded or appropriate mechanisms are put in place to be in line with ethical and legal constraints.

The next step is for the project to provide a specification for how the project will allow access to the data or share it if appropriate. The following questions are provided as input guidelines which will be intern reviewed by the DPO in terms of national/institutional policy:

Who will be interested in the data?	Internal partners of the project, research community, project stakeholders?
Are there any reasons why data cannot be shared?	Are there any restrictions on the use of the data?
How and when will data be shared?	What platform will be used to share data, e.g. public website, intranet, file sharing?
Are there potential restrictions, for example, charging for access?	Can the data be used freely or are there constraints on providing access for other uses?
Will there be right-of-first-use for the data collector, creator?	Will data be available after a period of time to others once used for its main purpose?

The final check point of the workflow provides important consideration of mechanisms used for the storage and management of the data. This is an important aspect to consider for the security and preservation of the data. This will also include a plan for the long-term preservation of the data. It is important to ensure that regulatory requirements are met for the long-term storage and access to the data. The following provides required input:

File naming convention	Consistency is important across all data sites
Storage	Where and what media? Who will be responsible?
Estimated size of data	How much storage space is required?
Back-up	How regularly will it be done? Who will be responsible?
Security – How will data confidentiality be guaranteed	e.g. data encryption, password controlled access etc.
How will the data be shared during the project?	Who will have access to the data and for which purpose, how will it be used?
How long will the data be kept?	Is the data only kept for a short period, for the life time of the project or beyond the project? What is the deletion process, automated, manual and who is the responsible party for deletion?
Where will I store the data?	e.g. archive, data repository, data centre, physical location of data store, country etc.
Who will manage the long term data?	Who will ensure data is kept for the required time, perhaps even beyond the lifetime of the project?
What is needed to prepare the data for preservation or data sharing?	What plan will be put in place to review quality of the data being collected and maintenance of the same
What is the data retention period and the access rights	Does the data owner authorise sharing of data on long term?

What related information will be deposited with the data?	Any additional data, e.g. file specification
Who will be responsible for metadata creation and documentation?	Who is the data curator?
Which metadata standards will you use?	Are there any meta data standards that can be used?

Assuming each checkpoint is passed successfully this will result in a data set specific plan that will be implemented by the project team. The subsequent steps of the data management lifecycle as outlined in Figure 1, i.e. organisation & storage, data retention, data sharing and data destruction refers specifically to the implementation of the data management plan as output of the data management checklist.

2.2 Data Set Categories

Data collected by the project will be stored on the project management site, and only accessible by project consortium members. All data will be prepared in suitable formats accordingly and if necessary, in liaison with EU Data Support Service for archiving. The DMP defines a clear management strategy for managing the project data. All partners are responsible for the implementation of this with the project coordinator will have overall responsibility for the data (in accordance with the DENiM legal, ethical and data management framework WP2) and will ensure that all other named managers are adhering to the data management plan (D2.2). From a work package perspective each WP lead has the responsibility for checking, storing and submitting data for archiving. All data will be kept on the local hard drive of the collector, sent to WP data manager to be archived on their PCs and backed up on department network drives. Research staff undertaking the data collection will be responsible for formatting data in accordance with established standards and supplying the relevant meta-data. An initial review of the data types collected was undertaken, the following classes of data sets have been identified and will be collected during the lifetime of the DENiM project.

2.2.1 Project Documentation and Scientific Results

This includes public relation material, project deliverables, management reports, technical reports and documentation that are generated by or on behalf of the project consortium. Project documents will be managed in accordance with the project management procedures as set out in D1.1 Project Guidelines and Quality Assurance Plan Report. Project partners are encouraged to publish research and development results obtained from the project in usual scientific forms. However, a Party shall not publish Foreground or Background of another Party, even if such Foreground or Background is amalgamated with the Party's Foreground, without other Party's prior written approval according to the Consortium Agreement (CA). As described in D10.1, the DENiM project platform is based on Microsoft Teams and this is built on the Microsoft 365 and Office 365 hyper-scale, enterprise-grade cloud platform, which delivers advanced security and compliance capabilities. The data in Teams resides in the geographic region associated with MTU's Microsoft 365 and Office 365 account, which is hosted in the EU. Please refer to D10.1 section 3.2 regarding the policy and security processes of the project repository.

2.2.2 Baseline Data

The validation of the DENiM platform will be based on baseline data collected at each pilot site. For each pilot, the available historical performance, usage, and process monitoring data is collected and serve for initial baseline performance assessment, the innovation within the project and the evaluation of the



D2.2: Data Management Plan

DENiM impact in terms of energy savings and cost reduction. During the collection of data consent for archiving will be requested to making the data available to other researchers in the longer term. The data required for the baseline will be captured through two mechanisms, firstly via surveys and document templates completed at each site and via historical data extracted from energy performance sensors (e.g. electricity meters) located in the relevant industrial sites. The baseline data includes:

- a) Static non-private sensitive business data such as process schematics, maps, management systems, interfaces and access.
- b) Time series energy data which may be processed later to equate baseline performance metrics.
- c) Meta-data, origin of the baseline data, where and when the data is collected.
- d) All data will be collected in accordance to standard based auditing methodologies.

2.2.3 Pilot Site Use Case Data

Data related to industrial processes, production planning, products, energy consumption, environmental impacts, usage patterns and demos. This data will be used by partners to support the development of DENiM specific models, tools and services. Confidential data, as dictated by data owner, will be kept restricted and not published unless permission is granted, in writing, by the owner. The process for protection of personal data that may be collected at DENiM pilot sites is captured in D10.2.

2.2.4 DENiM System Data

These data include time series and system data generated from the DENiM platform, including real time data streams from manufacturing systems, modelling output, data processed (e.g. energy performance metrics), key performance indicators, fault pattern analysis, scheduling and production patterns, weather predictions, local controller performance.



3 Open Data Access Policy

Publication of scientific papers is encouraged by the DENiM consortium following the publication approval process as described above. ‘Open access’ publications are encouraged. To comply with ‘open access’ requirement, the beneficiaries will ensure that their publications can be read online, downloaded and printed. This will be implemented depositing publications into a repository (online archive) with open access. Enforcing ‘open access policy’, publications fees for ‘green access’ and ‘gold access’ publications will be part of the project budget. Additionally, the project website will contain an overview and archive of all published information: scientific articles, publications, press releases, conference papers, etc. The project consortium will make sure that all publications related to the project are made available in Open Access publications or via an online repository. Further details on the procedure for the dissemination of project results is captured in the Consortium Agreement.

Datasets where possible will be made openly available. Where the release of data sets collected from the project is considered to be (i) commercially non-sensitive; (ii) not leading to violations of personal privacy; (iii) not violating any ethics or privacy approval obtained for experimentation; and (iv) of scientific interest to verify or extend project output; then, the consortium will make the data sets publicly available by identifying suitable national or international repositories where the data may be placed.

There are several existing tools that will support the implementation of the DMP including for example, the **Metadata Standards Directory** provided by the Research Data Alliance² provides a mechanism to find discipline-specific standards and associated tools. The **EUDAT B2SHARE** tool includes a license wizard that facilitates the selection of an adequate license for research data. The project will utilise research data repositories to provide access of open data; a registry of repositories is available through the R3Data portal³. Below is a list of samples of repositories that will be considered by the project to deposit both publications and research data, while also includes mechanism to link them together.

Open Research Europe	Open access publications for EU project results. https://open-research-europe.ec.europa.eu/
Zenodo	“Share and showcase multidisciplinary research results (data and publications) that are not part of the existing institutional or subject-based repositories of the research communities.” (https://zenodo.org/)
OpenAIRE	“Provide services make all research information freely available so that 3rd party providers build value added services to foster better understanding of scientific knowledge, while we scout for open and innovative scholarly communication services.” (https://www.openaire.eu/)
EU Open Data Portal	https://data.europa.eu/euodp/en/home
IEEE Data Port	https://ieee-dataport.org/
SWORD	South West Open Research Deposit (SWORD) is an institutional research data repository supported by MTU. https://sword.cit.ie/open_research/

² <https://www.rd-alliance.org/groups/metadata-standards-directory-working-group.html>

³ <https://www.re3data.org/>

4 Ethical and Legal Requirements

A number of activities that include data collection, storage and processing will take place in the context of the four pilots, all of which contribute to informing the DENiM approach, validating and assessing the technology as part of the overall evaluation of the effectiveness of the DENiM solution. As a consequence of these activities, data relating to stakeholders and participants will be collected in the context of the four pilots. As a result, ethical, privacy and data protection and confidentiality issues for volunteers regarding the collected data arise that need to be successfully handled. Furthermore, volunteers must be informed about their rights and responsibilities in relation to their participation in the studies realised in the context of the four pilots.

The DENiM project has dedicated significant resources to the analysis of the ethical and legal aspects involved in the project. It is also deeply committed to carried out its activities in full compliance with ethical and legal principles. The DENiM human participant ethics methodology will in part be informed by WP2: Ethical, Legal and Data Protection framework.

Furthermore, this WP aims at developing the legal framework, data management methodology and establishing the ethical principles to which DENiM will adhere to.

The DENiM partners will ensure that all national legal, ethical requirements and code of practice of the Member States where the research is performed are adhered to. The ethical, legal and data protection assessment is continuous (D2.1–D2.4, D2.6) and linked to the overall project workplan, and is active from the beginning of the project and will be revisited at each new project phase. This continuous assessment approach ensures that any issues relating to ethics, legality or data will be identified and resolved as early as possible and will minimise the impact on the project workplan, in particular the pilot site activities. In particular, WP2 will identify the key ethical and data protection aspects involved in the project's activities. It will issue guidelines and assistance in the implementation of the ethical and data protection requirements. Deliverable D2.3 Legal and Ethical Analysis for DENiM will describe and analyse the ethical and legal requirements for the DENiM project. WP2 will provide Guidelines and Assistance for Data Management and for the implementation of the ethical and legal constraints regarding data protection (e.g. security, confidentiality, access management, data storage and duration). UNamur will act as a data protection helpdesk for all the partners in the context of the project. The DENiM External Ethical and Legal Advisory Board will issue legal and ethical guidelines.

It is highlighted that the ethical and legal analysis will have a foundation on inputs coming from all the other DENiM WPs. In addition, Deliverable 10.1 (Humans: H – Requirement No. 1) presents the procedures and requirements that will be used to identify/recruit research participants for the DENiM pilot site scenarios and the informed consent procedure that will be used to support the participation of humans and Deliverable 10.2 (Protection of Personal Data: POPD – Requirement NO. 2) presents the protection of personal data principles that the DENiM consortium will adhere to in order to safeguard the rights and freedoms of the research participants (see *infra*, Section 4. Specific Procedures).

5 Identification and Recruitment Procedure for Human Participants at the Pilot Sites

As stated *supra* in Section 3, a number of activities that include data collection, storage and processing will take place in the context of the four pilots, all of which contribute to informing the DENiM approach, validating and assessing the technology as part of the overall evaluation of the effectiveness of the DENiM solution.

As a consequence of these activities, data relating to stakeholders and participants will be collected in the context of the four pilots. As a result, privacy and data protection and confidentiality issues for volunteers regarding the collected data arise that need to be successfully handled. Furthermore, volunteers must be informed about their rights and responsibilities in relation to their participation in the studies realised in the context of the four pilots. For this purpose, special guidelines have been set and presented in Deliverable D10.1, so that the procedures and rules that need to be followed by the partners and the participants involved in these DENiM's activities are made clear and specific. The "legitimate interests" of the controller (responsible for the data processing) is the lawful basis to process personal data in the case of the DENiM pilot site activities and as part of this we include the requirement to request the consent of the employees in order to participate in the project pilot site activities. Depending on the specific manufacturing processes, the pilot site owners (employer – specifically the person/people responsible for the manufacturing process) will identify the group of people that work as part of the specific manufacturing process, and from that group individuals will be asked to participate in the pilot site activities and give their informed consent to participate to the research (for further details, please refer to D10.1 Section 4).

D10.1 Section 5 describes the process of informed consent used by the project and provides a template of Informed Consent Form to be submitted to the research participants at the pilot sites.

6 Organisation Specific Ethics Approval

As outlined in D10.2 Protection of Personal Data: POPD – Requirement NO. 2, Section 2, a number of organisations (that are processing personal data) will require approval by their organisation's ethics committee.

It is reinforced that prior to engaging in any activity with human participants, the relevant project beneficiaries must have secured approval from their specific ethics committees or approval body. The relevant documents and approvals must be kept on file and be submitted as a deliverable. If they are not in English, they should be submitted with an accompanying summary in English, which shows the conclusion and recommendations of the committee or authority concerned.

7 DENiM Stakeholder Boards & Forum

The mission of the External Expert Advisory Board and the DENiM Stakeholder Forum is to inform the DENiM approach, facilitate the exchange of expert opinion and provide feedback on the DENiM outcomes. In addition, these stakeholder groups will also be part of the dissemination and communication channels being defined in WP 9. D10.2 Protection of Personal Data: POPD – Requirement NO. 2 provides the guidelines regarding the use of personal data related to the individual stakeholders involved in these boards and forum will be collected.

In relation to the DENiM External Expert Advisory Board (EEAB), the DENiM External Ethical and Legal Advisory Board (EELAB) and the DENiM Stakeholder Forum limited personal data will be collected. The primary collection of personal data will be limited to the name, professional title, organisation and email address. No special categories of personal data will be collected. Personal contact data will be kept internally within the DENiM partners as part of a stakeholder database and will not be accessible to nor shared with any external organisation or individual. Members of the DENiM Stakeholder Boards can step down at any time and members of the DENiM Stakeholder Forum can unsubscribe from the DENiM Stakeholder Forum at any time through an email opt-out and unsubscribe process. If a Board member steps down or a Forum member opts-out all personal data related to this individual and coming from the primary collection of personal data will be removed from the DENiM stakeholder database. Personal data collected during the DENiM project in relation to stakeholders will be stored electronically on the DENiM project Portal and shared through the DENiM intranet with consortium partners. The data cannot be accessed or copied by nor shared with any third party. Data will be retained for the duration of the project (unless a request to opt-out is received) and the DENiM consortium is in full control of the retention requirements. The data remains in the full control of the owner, and all data generated by a partner can be deleted on request, with consideration of consortium agreement and the project exploitation and IPR requirements.

8 Exploitation and IPR

WP9 is in charge of the Dissemination and Exploitation activities in the DENiM project. It is responsible for developing the dissemination strategy, aiming to link the project with the industrial sector and other stakeholders who may be interested in the project outcomes, transfer of DENiM knowledge. It will result in the definition of a Business Model (D9.3 & D9.5) and in Best Practices for Energy Efficient Management of Manufacturing Systems (D9.6).

8.1 IPR and Innovation Management

Means for legal protection will include copyright, patents, utility models and industrial secrets. A technology watch will be carried out permanently, to quickly identify emerging potential competitor in the market and collecting the IPs that could interfere with the project and bringing to discussions any IP consideration (which are the results, who is the owner, how to exploit them, etc).

Furthermore, this WP will manage the business indicators for the identified innovation, assessing spin-off planning for spill-over opportunities and scout funding opportunities by pitching the project innovations at project-specific meetings or more general start-up/innovation events across Europe.

8.2 Results Exploitation

During the project, the Consortium will identify the most appropriate organizational and business models in order to guarantee the sustainability of the project results in the long-term. The Consortium will define a roadmap toward the commercialization of the developed solutions, including the additional development activities beyond the end of the project.

DENiM consortium will define the most effective and feasible exploitation strategy and plan considering three domains of decisions:

- (1) Definition of the project results/assets (What will be exploited?);
- (2) Decision on the exploitation policy for each asset (How are we going to exploit it?);
- (3) Decision on the market strategy (Where and in which promotion channels should we implement the exploitation policy of the specific asset?).

The task will produce the Business Plan for a joint exploitation of the DENiM platform, listing the developed business cases (starting from the use case demonstrators) and then the commercialisation strategy that will be implemented after the end of the project. Individual components exploitation will also be analysed and considered.

The crystallization of the roadmap is informed by the following analysis: Market and competitive analysis, aimed at identifying any similar solution under development or already placed in the market; SWOT analysis, defining strengths, weaknesses, opportunities, and threats involved in a DENiM business venture; Organizational and business models' alternatives for the future commercialization of DENiM outcomes; Mid-and long-term demand estimation and attractive power towards stakeholders; Main cost and revenues drivers.

9 Review of the Data Management Plan

The DMP will be reviewed and updated if and where necessary.





Annex 1: Template of the Data Management Form to be Fulfilled by the Partners⁴

HISTORY OF CHANGES		
Version	Publication date	Change
1.0	30.03.2021	<ul style="list-style-type: none"> ▪ Initial version
		<ul style="list-style-type: none"> ▪
		<ul style="list-style-type: none"> ▪
		<ul style="list-style-type: none"> ▪
DMP components		Issues to be covered
1. Data description		<ul style="list-style-type: none"> (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 are being re-used (if any) (5) Specify the origin of the data (6) State the expected size of the data (if known) (7) Outline the data utility: to whom will it be useful
2. Making data findable, including provisions for metadata		<ul style="list-style-type: none"> (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
3. Making data openly accessible		<ul style="list-style-type: none"> (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

⁴ This template is based on the H2020 templates: Data management plan v1.0 – 13.10.2016.



D2.2: Data Management Plan

	<p>(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)?</p> <p>(4) Specify where the data and associated metadata, documentation and code are deposited</p> <p>(5) Specify how access will be provided in case there are any restrictions</p>
4. Making data interoperable	<p>(1) Assess the interoperability of your data. Specify what data and metadata vocabularies, standards or methodologies you will follow to facilitate interoperability.</p> <p>(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?</p>
5. Increase data re-use (through clarifying licenses)	<p>(1) Specify how the data will be licensed to permit the widest reuse possible</p> <p>(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</p> <p>(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</p> <p>(4) Describe data quality assurance processes</p> <p>(5) Specify the length of time for which the data will remain re-usable</p>
6. Allocation of resources	<p>(1) Estimate the costs for making your data FAIR. Describe how you intend to cover these costs</p> <p>(2) Clearly identify responsibilities for data management in your project</p> <p>(3) Describe costs and potential value of long-term preservation</p>
7. Data security	<p>(1) Address data recovery as well as secure storage and transfer of sensitive data</p>
8. Ethical aspects	<p>(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</p>
9. Other	<p>(1) Refer to other national/funder/sectorial/departmental procedures for data management that you are using (if any)</p>