InCUBE
sustainable building innovations

WP10 – D10.4

Data Management Plan (DMP) (v1)

Main authors:

KENT

HORIZON-CL5-2021-D4-01
EUROPEAN COMMISSION

European Climate, Infrastructure and Environment Executive Agency
Grant agreement no. 101069610

This project is funded by the European Union's 'Horizon Europe Research & Innovation programme' under grant agreement No 101069610. This publication reflects the authors' view only and the European Commission is not responsible for any use that may be made of the information it contains.

Project contractual details

Project title	An INClUsive toolBox for accElerating and smartening deep renovation
Project acronym	InCUBE
Grant agreement no.	101069610
Project duration	48 months (01/07/2022 – 30/06/2026)

Document details

Deliverable no.	10.4
Dissemination level	PU = Public
Work package	WP10
Task	T10.4
Due date	M6 (31/12/2022)
Actual submission date	M6 (29/12/2022)
Lead beneficiary	2 (KENT)
Contributing beneficiary/ies	1 (CERTH)

Authors

Full Name	Beneficiary	Contact Information
Levent Gürgen	KENT	levent@kentyou.com
Bertrand Copigneaux	KENT	b.copigneaux@kentyou.com
Stylianos Zikos	CERTH	szikos@iti.gr
Komninos Angelakoglou	CERTH	angelakoglou@certh.gr

Reviewers

Full Name	Beneficiary	Contact Information
Sara Barbieri	LAMA	sara.barbieri@agenzialama.eu
Philo Tamis	NEC	p.tamis@newenergycoalition.org

History of changes

Version	Date	Beneficiary	Changes
0.1	05/12/2022	KENT	Initial draft
0.2	12/12/2022	KENT, CERTH	Added content about the data management framework
0.5	16/12/2022	KENT, CERTH	Added content on ethics management
0.9	20/12/2022	KENT, CERTH	Added information on datasets and conclusions
1.0	28/12/2022	KENT	Final version addressing the comments from partners, ready for submission

Executive Summary

This document presents the first version of InCUBE Data Management Plan (DMP), as well as the ethics requirements and management in the project lifetime. It also encapsulates information about open access to research data. In particular, the DMP provides details on the data the project will generate (.i.e. content, type, format), which standards and methodologies will be used for data collection and management, how it will be exploited and how they will be made findable, accessible, interoperable and reusable. The general principles are presented, including data handling and open access policy. Furthermore, data management processes during and after the end of the project are described, such as data collection, storage, retention and destruction. Regarding the datasets, a dataset identification template was created and sent to partners responsible for the development of specific components or data collection from participants, in order to collect information about anticipated produced datasets.

The InCUBE project will collect and analyse data in three pilot sites in Italy, Netherlands, and Spain, in order to develop and evaluate innovative solutions for use in building renovations. It shall be noted that during the execution of the project's activities, ethical concerns may be raised with regard to the privacy and security of data collection and processing. These issues will be addressed according to the ethics management methodology that has been developed and presented in the document, and according to the EU and national legislation and directives of the countries where the data collection will take place.

The DMP is intended to be a living document. As the tasks and pilot activities progress, the datasets will be elaborated and the related information will be updated and enriched in the next version of the DMP (D10.12), which will be delivered on M24. The final version of the DMP (D10.13) will be delivered at the end of the project.

Table of contents

List of figures

List of tables

List of Acronyms and Abbreviations

Term	Description
AI	Artificial Intelligence
BIM	Building Information Modelling
DMP	Data Management Plan
DPO	Data Protection Officer
EC	European Commission
EU	European Union
FAIR	Findable Accessible Interoperable Reusable
GA	Grant Agreement
GDPR	General Data Protection Regulation
HTTP(S)	Hypertext Transfer Protocol (Secure)
IT	Information Technology
ML	Machine Learning
MQTT	MQ Telemetry Transport
NDA	Non-Disclosure Agreement
R&I	Research and Innovation
RES	Renewable Energy Sources
SSL	Secure Sockets Layer
TLS	Transport Layer Security
WP	Work Package

1 Introduction

1.1 Aim of the deliverable

This deliverable presents the detailed Data Management Plan (DMP) as well as the ethics management framework that will be followed within the InCUBE project. The Data Management Plan that is presented in this deliverable provides details on the data the project will generate (i.e., content, type, format, volume), which standards and methodologies will be used for data collection and management, whether and how it will be exploited, and how they will be made findable, accessible, interoperable, and reusable (FAIR). InCUBE involves carrying out data collection, including personal data and metadata, in the context of the piloting and monitoring phase and setting up the digital building logbook. The Data Management Plan is intended to be a living document, and therefore updated versions will be delivered throughout the project's duration following the InCUBE progress presenting updated information.

1.2 Dependencies with other tasks

This deliverable is the initial outcome of T10.4 - Ethics and Data Management that is part of WP10. The information that is provided in this document can be used as input for the work packages that are related to solutions' development activities. Additionally, the DMP can be used as a reference for the exploitation activities that will be performed within T9.4 - Exploitation activities, IPR management and post-project sustainability. Lastly, the topics presented on ethics management and procedures to be followed in the pilots in compliance with data protection legislation shall be taken into account where recruitment and involvement of end users is envisaged, such as in tasks within WP1, WP6 and WP7.

1.3 Structure of the deliverable

The document is structured as follows:

- Section 2 describes the data management framework that will be followed within the InCUBE project.
- Section 3 provides examples of data that will be created within the project and presents their main properties.
- Section 4 provides details on relevant legislation (both EU and national) related to data protection that shall be considered.
- Section 5 presents the InCUBE ethics management methodology that has been specified.
- Section 6 summarizes the main conclusions of this version of the document and highlights the next steps.
- Accompanied content and template documents are provided at the end of the document as Annexes.

2 InCUBE Data Management Framework

This section describes the InCUBE data management framework, which defines the format of the datasets and handles issues related to data, such as data handling and sharing, data protection, data collection & storage, and data retention & destruction.

2.1 General principles

2.1.1 Data availability and handling

With regard to the availability of data, three different categories have been defined as presented in Table 1.

Table 1 – Categories of data in respect to availability

Data availability categories	Description
Confidential	This category refers to data that are retained by individual partner (data owner) of the project
Consortium	This category refers to data that are available only to the members of the project and the EU Commission services, and are subject to Non-Disclosure Agreement
Open Data	This category refers to data that are publicly shared for re-use and exploitation

Within the InCUBE project, datasets can be subdivided as follows with regard to their availability:

- Generated datasets at pilot sites that are used for individual partner purposes (Confidential)
- Generated datasets at pilot sites that are shared between the Consortium partners (Consortium)
- Generated datasets at pilot sites that are shared to the public (Open Data)
- Research findings and outcomes that shall be publicly disseminated (Open Data)

Data handling activities will be performed by the data controllers and the date processors, in compliance with the General Data Protection Regulation (more details about GDPR are provided in the ethics management section of this document). Data controllers are responsible for specifying the purposes and means of the processing of personal data. On the other hand, data processors process the personal data on behalf of the data controller. In the context of InCUBE project, the pilot responsible partners and the Data Protection Officers (DPOs) will act as the data controllers, while the technical partners who will use the data as input to software/hardware solutions and analyse the data will have the role of data processors. Regarding the datasets that will be shared among the Consortium partners ('Consortium' availability category) during the execution of relevant tasks,

NDAs are foreseen to be signed among the involved data processors and data controllers prior to sharing of the data. Data handling in InCUBE project is illustrated in Figure 1.

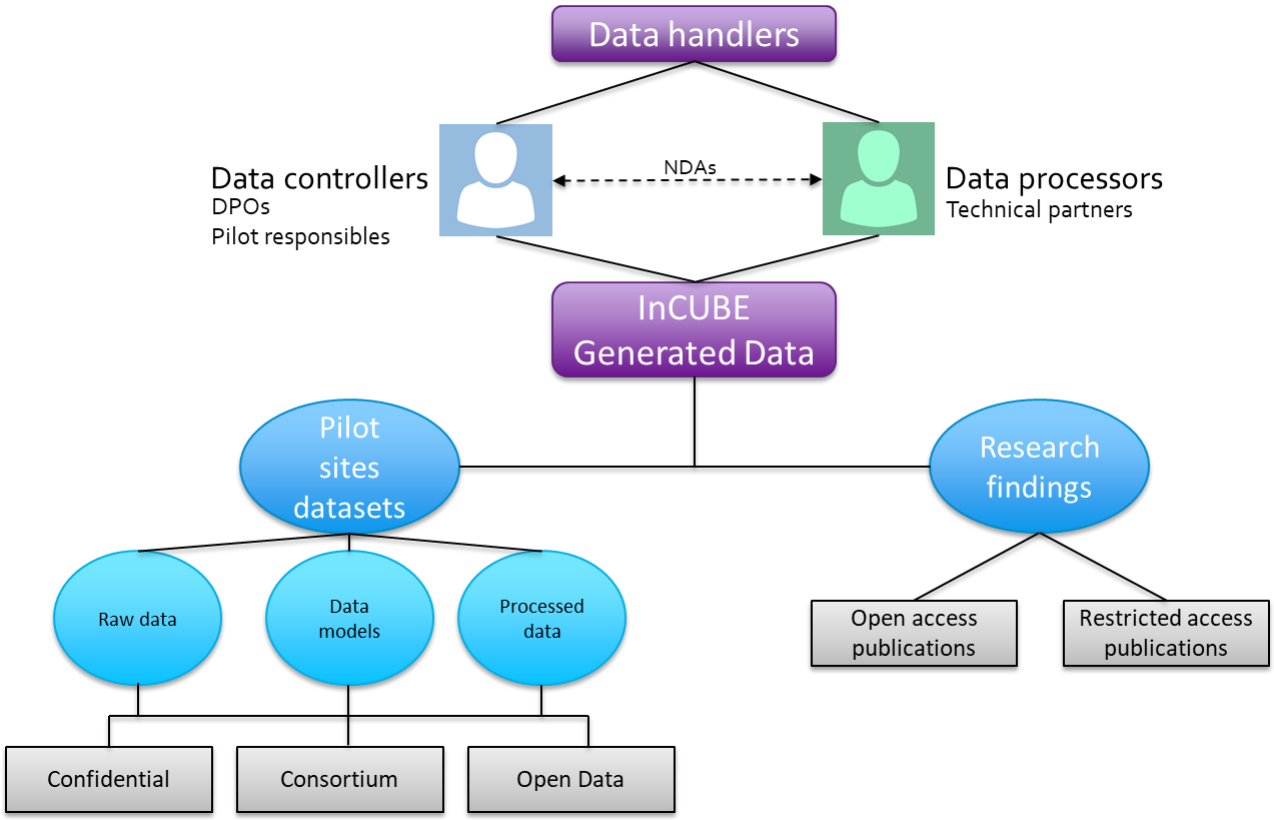

Figure 1 – InCUBE data handling

2.1.2 Open access to scientific publications

Open access is defined as online access to research outputs provided free of charge to the end-users. Research outputs include peer-reviewed scientific publications related to the results derived from scientific research and experiments, as well as research data which can be data underlying publications, curated data and/or raw data.

The two main options for open access that will be considered are the following:

'Green' open access (or self-archiving): The author, or a representative, archives (deposits) the published article or the final peer-reviewed manuscript in an online repository, such as zenodo.org, before, at the same time as, or after publication. Some publishers request that open access be granted only after an embargo period has elapsed.

'Gold' open access: An article is immediately published in open access mode. The payment of publication costs is shifted away from subscribing readers if this option is chosen.

The usual business model is based on one-off payments by authors. These costs, often referred to as article processing charges are usually borne by the researcher's university or research institute

or the agency funding the research. In other cases, the costs of open access publishing are covered by subsidies or other funding models.

2.1.3 Open access to research data (FAIR data)

Open Access to research data refers to the right to access and reuse digital research data under the terms and conditions set out in the GA. Examples of data that are available in digital form include measurements, results of experiments, calculated statistics, survey results, interview recordings, and images. Users can normally access, query, exploit, reproduce and disseminate openly accessible research data free of charge. The various data dissemination an exploitation options are summarized as a flowchart diagram in Figure 2.

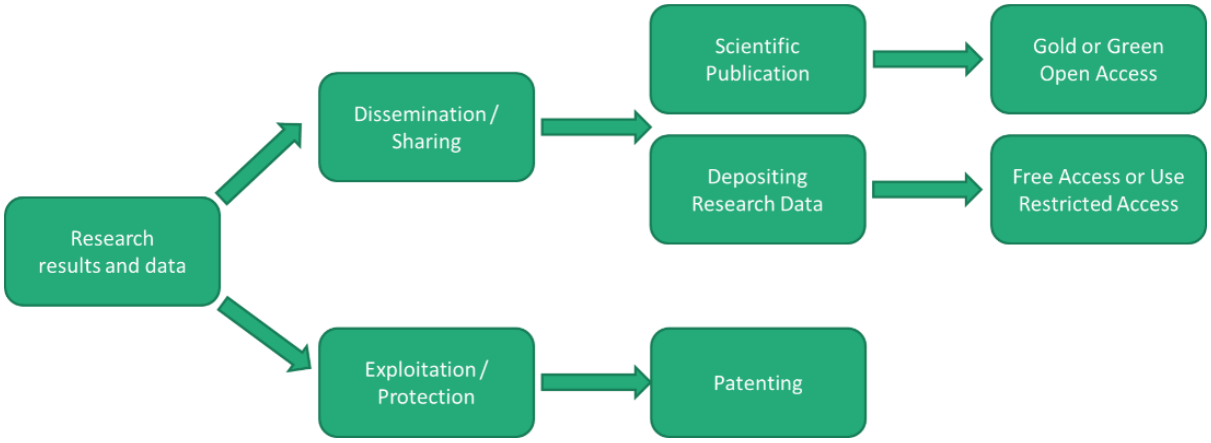

Figure 2 – Options for the dissemination and exploitation of data

There are four main aspects of open data that are summarized in the acronym **FAIR**[1]:

- **Findable**: Data has a unique, persistent ID, located in a searchable resource, and documented with meaningful metadata.
- **Accessible**: Data are readily and freely retrievable using common methods and protocols, metadata are accessible even if the data are not.
- **Interoperable**: Data are presented in broadly recognized standard formats, vocabularies, and languages.
- **Re-useable**: Data has clear licenses, and accurate meaningful metadata conform to relevant community standards and identifying its content and provenance.

InCUBE will follow thoroughly all the required actions in order to be aligned with the Open Science practices as they are also defined in Horizon Europe guidelines. In particular, InCUBE will address the following:

- Early and open sharing of research

[1] REGULATION (EU) 2021/695 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32021R0695

- Research output management and measures to ensure reproducibility of research outputs: InCUBE will cover the three main research processes that reproducibility is based on (reproduction, replication, and re-use)
- Open access to research outputs and participation in open peer-review: the publications of the project will be published in Open Access Journals and Open Access Repositories
- Involvement of relevant knowledge actors including citizens, civil society and end users in the co-creation of R&I agendas and contents, within WP1 And WP7

2.2 Data collection and storage

Data managed during the project will be processed only under the following preconditions: (i) When the data subject has given her/his consent; (ii) When the processing is necessary for the performance of or the entering into a contract; (iii) When processing is necessary for compliance with a legal obligation; (iv) When processing is necessary in order to protect the vital interests of the data subject.

It is important to note that personal data managed within InCUBE will be anonymized and stored in a form which does not permit identification of users. The InCUBE strategy is to minimize the use of personal data as much as possible and use of anonymized data.

Moreover, any data from the pilot use cases that will have been identified as confidential will be discarded after the implementation of the project (more details are provided in the next section). However, the public / open access models and created datasets will remain open.

2.3 Data retention and destruction

Collected data until the end of the project that will not be characterised as Open Data will be deleted after the project is finished. Regarding data destruction, it shall be permanent and irreversible by using methods such as full disk overwriting and re-formatting, considering that hard disk drives will be utilised for storing the data. All existing backups of the data shall be deleted as well.

In all cases, the data retention of personal data will be governed by the following principles: (i) Protective measures against infiltration will be provided, (ii) Physical protection of core parts of the systems and access control measures will be provided, (iii) Logging of InCUBE systems and appropriate auditing of the peripheral components will be available.

2.4 Data sharing

The partners of InCUBE project will use various means for the exploitation and dissemination of the produced data, as for example:

- Use in future research activities.
- Development / marketing a product or process.
- Creation of a service.

Activities for both commercial and scientific exploitations of the results are planned to be performed.

For the datasets that will be available for use only among the Consortium members, mechanisms for authentication and authorization will be applied (e.g. use of private links, password-protected archives) in order to restrict access and make sure that only approved/relevant users can retrieve the data. Commonly, the datasets will be provided in the form of files (e.g. csv). Additionally, certain data about the developed solutions and technologies will be available through the InCUBE one-stop-shop renovation marketplace to be developed within T8.4.

The Zenodo online open repository is planned to be used in order to host the open datasets of InCUBE, facilitating re-use and exploitation. A dedicated InCUBE community will be created on Zenodo.

2.5 Data protection and security

Confidentiality is protected by various measures which ensure that personal data neither fall into the hands of third parties nor can be viewed by them. Such measures are the anonymisation of personal data, enabled password protection and storage on encrypted servers.

In order to protect the collected data and control unauthorised access to the InCUBE Data Lake and repositories, only authenticated personnel will have access to use case-specific data collected. Additionally, the use of secure protocols such as SSL/TLS will help to protect privacy. For implementing secure data exchange among InCUBE components, the security configuration options of the common industry protocols that are foreseen to be used (I.e. MQTT and HTTP(s)), will be enabled.

Regarding the topic of data interoperability, which is highly important, an interoperability framework for building systems, products and operations, will be developed within T3.1 of InCUBE.

2.6 Format of Datasets

Each dataset that will be created within InCUBE project will be described by the following properties that have been included in the dataset identification template that is presented in Table 2. The dataset identification template was formed by considering the guidelines and requirements of EC on data management in Horizon Europe and includes the following main sections: “Data Identification”, “Related WPs and Tasks”, “Partners Responsibilities”, “Metadata, Pre-processing, Sharing and Expected Size”, and “Exploitation”.

Table 2 – Dataset identification template

<DS-XX-Title>	
Data Identification	
Dataset name	<Short name/outline of the dataset>
Dataset description	<Explain why and how data are collected and describe the content. Also, mention the related datasets (used as input), if any.> Related datasets:
Origin of the data (e.g. device, evaluation surveys)	<Mention how the dataset will be collected>
Related InCUBE component(s)	<Mention the related InCUBE component>
Relation to the InCUBE objectives	<Mention the related InCUBE objectives>
Related WPs and Tasks	
WPs	<The data will be collected within activities of WPX>
Tasks	<The data will be collected within activities of tasks TX>
Partners Responsibilities	
Partner(s) responsible for the data collection	<Partner short name>
Partner(s) responsible for the data storage	<Partner short name>
Partner(s) responsible for the data analysis	<Partner short name>
Metadata, Pre-processing, Sharing and Expected Size	
Metadata and documentation	<Provide information about the discoverability of the dataset and if a documentation will be available>
External data used	<Mention the external data/database sources in case the dataset includes data from sources outside of InCUBE project>
Data pre-processing steps	<Mention any pre-processing done to the dataset: E.g. anonymization, data interpolation, outlier cleaning etc.>
Sharing	<Public / Consortium / Confidential>

Licence type (e.g. Public Domain, Attribution, Non-commercial, No Derivatives, or other)	<Mention the type of licence>
Expected volume of data	<Mention the expected size of data e.g. in Megabytes>
Format of data	<Mention the format of data, e.g. JSON, csv etc.>
Storage location (URI)	<Mention where dataset is stored: e.g. public URL address, SVN path>
Exploitation	
Data utility (to whom will it be useful)	<Explain shortly the purpose of the data collection>

3 Description of Datasets

Various types of data will be collected within the InCUBE project, such as automatically collected data from energy and environmental sensors, data related to buildings' information, data related to renovation processes/works from the pilot sites, data generated from InCUBE components after processing, and data that will be collected directly from end users and stakeholders through surveys, interviews and workshops.

A preliminary list of datasets, which has been formulated based on the foreseen activities and the offered solutions within the project is shown in Table 3.

Table 3 – Preliminary Datasets List

Dataset	Relevant Task(s)
Stakeholder and user requirements list	T1.2
Pilot sites surveys	T1.3, T7.5
Training material (multimedia content) for upskilling workforce	T4.3, T6.4
Social-oriented data	T6.1, T6.3
Energy consumption data and forecasting	T2.3, T5.1
Energy generation data from RES and forecasting	T2.2, T5.1
Environmental data from sensors	T3.4, T4.4
Layout, topology and equipment data in buildings through Building Information Modelling files and 3D scans	T3.2
Energy performance certificates analysis data per building	T4.4
Smart readiness indicator analysis data per building	T4.4
Hardware equipment and construction material properties	T2.1, T2.3
Renovation plan/processes and sub-processes characteristics	T4.2, T5.2

It shall be noted that the availability of each dataset will depend on the scope of the data and its use, therefore not all datasets will be available as Open Data. In any case, the goal of the Consortium will be to make publicly available and accessible as much data as possible. In addition, special focus will be given on the documentation and inclusion of metadata in order to describe each dataset adequately. As far as the format is concerned, widespread open formats will be preferred to facilitate processing.

In the next versions of the data management plan, detailed information on the format and properties of the aforementioned data will be provided, based on the InCUBE dataset identification template.

4 Legislation

Special focus will be given to ethical, social, and data protection considerations within the InCUBE project. InCUBE partners are aware of the fact that privacy and data protection concerns could be anticipated with regard to the activities especially in WP1, WP6 and WP7. InCUBE employs data gathering as part of its pilot trials in order to evaluate how effective the envisaged solution is, and specific individuals are expected to participate in the pilot execution activities. All processing of personal data will be conducted in accordance with the provisions of: a) the GDPR (Regulation (EU) 2016/679)[2], b) the Universal Declaration of Human Rights and the Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data, and c) the national laws relevant to the country where the data collection is taking place (i.e. Italy, Netherlands, and Spain).

4.1 EU Legislation

All activities related to data management within InCUBE will be performed in full compliance with the following EU legislation and directives:

- The Universal Declaration of Human Rights and the Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data
- General Data Protection Regulation & Directive 2002/58/EC of the European parliament regarding issues with privacy and protection of personal data and the free movement of such data

The General Data Protection Regulation (GDPR) is a privacy and security law which was drafted and passed by the EU and imposes obligations onto organizations anywhere, as long as they target or collect data related to people in the EU.

Article 4 of the GDPR presents the list of the definitions that are used for the purposes of the regulation. Indicatively, 'personal data' are defined as *"any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;"*

A data 'controller' is defined as follows: *"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*

[2] General Data Protection Regulation, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG

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;"

A data 'processor' is defined as follows: *"processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;"*

A GDPR checklist[3] for data controllers is provided in ANNEX I. The checklist includes statements and actions that can help a data controller to limit exposure to regulatory penalties.

In Article 5.1-2 of the GDPR, seven protection and accountability principles related to processing of personal data are explained. These principles must be considered before and during the data processing phase:

- Lawfulness, fairness and transparency - Processing must be lawful, fair, and transparent to the data subject.
- Purpose limitation - Data must be processed for the legitimate purposes specified explicitly to the data subject when they were collected.
- Data minimization - Only as much data as absolutely necessary for the purposes specified should be collected and processed.
- Accuracy - Personal data must be kept accurate and up to date, where necessary. Every reasonable step must be taken to make sure that inaccurate personal data, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Storage limitation - Personally identifying data may be stored only for as long as necessary for the specified purpose. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1).
- Integrity and confidentiality - Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g. by using encryption).
- Accountability - The data controller is responsible for being able to demonstrate GDPR compliance with all of these principles.

Article 9 of the GDPR refers the following about processing of special categories of personal data: *"Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."*

[3] https://gdpr.eu/checklist/

InCUBE will not collect the aforementioned special categories of personal data (formerly known as 'sensitive data').

4.2 National Legislation

This section provides information about the legislation related to data protection, and the data protection authorities, within the three countries that are directly involved in the piloting activities (Italy, Netherlands, and Spain).

4.2.1 Italy

Legislative Decree 196/2003 (Codice in materia di protezione dei dati personali or the "Code"), has defined the core of privacy in Italy for more than two decades. In Italy the GDPR is implemented by the Code. Following the introduction of the GDPR, the Code has undergone a considerable modification by Legislative Decree 101/18. The adaptation decree repealed most of the previous provisions and integrated the national legislation with the new Regulation.

The Italian data protection authority[4] (Garante per la protezione dei dati personali) is an independent authority, which was established in 1997, and set up to protect fundamental rights and freedoms in connection with the processing of personal data, and to ensure that individuals' dignity is respected. The tasks of the authority are laid down in the GDPR 2016/679 as well as in the Personal Data Protection Code (legislative decree No. 196/2003) and in other national and EU regulatory instruments. The authority is committed to ensure that, in all sectors, data are processed as required by the law, and the rights of individuals are respected whenever personal data are processed.

4.2.2 Netherlands

The processing of personal data in the Netherlands is mainly governed by the GDPR and the Dutch GDPR Implementation Act[5]. An unofficial English version of the latter is available[6].

The Dutch Data Protection Authority (Autoriteit Persoonsgegevens) has been appointed by law as the supervisory data protection authority in Netherlands. It supervises compliance with the GDPR and the Implementation Act. The Authority has the statutory duty to assess whether persons and organizations, including government organisations, comply with the Dutch Personal Data Protection Act. The Authority also supervises compliance with the Police Data Act, the Municipal Personal Records Database Act and all other statutory regulations concerning the processing of personal data. The Authority often refers to the guidelines released by the European Data Protection Board,

[4] https://www.garanteprivacy.it/web/garante-privacy-en
[5] https://wetten.overheid.nl/BWBR0040940/2021-07-01
[6] https://www.dataguidance.com/sites/default/files/dutch_general_general_data_protection_regulation_implemention_act.pdf

but also publishes guidelines, Q&A's and explanations on various topics under the GDPR and the Act. The Dutch Data Protection Authority can be reached online at this address[7].

4.2.3 Spain

Protection of individuals with regard to the processing of personal data is a fundamental right protected by Article 18.4 of the Spanish Constitution. A document of consolidated Spanish legislation on data protection, personal security and digital rights (Law 3/2018) can be found online[8].

The supervisory data protection authority of Spain can be reached at https://www.aepd.es/es, where practical information on data protection rights and obligations are provided along with answers to common questions.

[7] https://autoriteitpersoonsgegevens.nl/en
[8] https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf

5 InCUBE Ethics Management

InCUBE Consortium will ensure that all necessary measures will be applied to protect the privacy of the involved data subjects. This section presents the measures that will be applied by the Consortium towards complying with the EU and national legislation that was outlined in the previous section.

5.1 Ethics Monitoring

InCUBE has appointed two roles in the Project Management Plan (D10.1) to ensure compliance of its activities with European regulations and standards: The role of Quality and Risk Manager (Ferran Pérez from ITEC) and the role of Ethics and Data Manager (Bertrand Copigneaux from KENT). They will be involved during all research activities to ensure all privacy and data protection issues are solved responsibly.

The InCUBE Ethics and Data Manager will cover the following areas:

- Planning the data protection processes;
- Establish the data protection measures;
- Monitor the data protection compliance;
- Design, prepare and communicate rules and guidelines for data security for the InCUBE Consortium.

The InCUBE Quality and Risk Manager will elaborate transparent information regarding ethics procedures to users and stakeholders, and supervise and monitor the implementation of set procedures & serve as the first point of contact for all ethics related issues during the course of the project (for example, organize meetings to solve issues).

The two aforementioned members will be assisted by external experts or the commission, of needed. Moreover, in order to ensure that each pilot site will comply with its national legislation, one person from each site will be nominated as responsible for monitoring of the project's guidelines.

5.2 Ethical Policy

InCUBE will follow and fulfil all national legal and ethical requirements and guidelines of the countries where the research activities are performed. Collection of any data related to humans will be strictly kept confidential at any time, which will also be in full compliance with the principles and guidelines of "Ethics for Researchers" to facilitate research excellence (that was introduced by the EC Governance and Ethics Unit in 2007). In particular:

- detailed information will be provided to all end-users upon requesting their consent to any data collection and processing activity. All end-users will participate voluntarily and will receive detailed oral (and if needed written) information.
- data will be processed using data scrambling and abstraction techniques where possible in a way that will not affect the final outcome of the project.

The following material and advice will be provided in native language in order to facilitate understanding and communication:

- A simplified written general description of the project and its goals
- The project's time plan, including progress aspects and relevant testing and evaluation plans
- Advice on unrestricted disclaimer rights on their agreement

The members of the project responsible for ethics monitoring will evaluate all research activities in order to guarantee that there will be no unjustified risk for the end users related to the breach of their privacy and all ethical and legal requirements are respected. In case authorisations are required from national bodies, those shall be considered as project-related documents. Copies of such authorisations shall be submitted to the EC prior to the application of the relevant activities.
For the issues that are related to Artificial Intelligence (AI), Ethics Guidelines for Trustworthy Artificial Intelligence (AI) prepared by the High-Level Expert Group on Artificial Intelligence (AI HLEG) set up by the European Commission in 2018, as part of the AI strategy, will govern the implementation of AI/ML tools and algorithms in InCUBE. The Assessment list for trustworthy artificial intelligence (ALTAI) for self-assessment released in 2020 will guide the developers and deployers of AI in InCUBE for all AI-based algorithms/tools/systems implemented.

5.3 Ethical Risks

The IT framework of InCUBE will consider privacy and (cyber)security as key topics. The goal is to develop InCUBE in full compliance with the GDPR and security standards. Privacy and security risks of the project will be identified in order to mitigate them and reduce the risk of causing harm to individuals through the misuse of their personal information. Details on risk management approach to be followed are provided in D10.3 - "Quality & Risk Assessment Plan".

5.4 Pilot Ethical Methodology

5.4.1 Ethical requirements

InCUBE has identified the following steps to be followed when performing an activity that involves data collection from end-users.

1. Provide detailed consent forms for the participation of end users.
2. Provide information about the data management process (e.g., collection, storage, protection, retention, handling and destruction), according to national and EU legislation.
3. Provide Non-Disclosure Agreements to be signed among Consortium members if needed, to ensure proper information exchange within InCUBE activities.
4. Acquire confirmation by the Data Protection Officer and/or obtain authorization or notification by the corresponding National Data Protection Authority.
5. Provide reasonable justification for collecting and processing personal data.
6. Prior to the deployment of the solution at the pilot sites, all involved end-users must agree and sign informed consents.
7. Prior to final integration and piloting, all necessary NDAs (ANNEX II) will have been signed by the involved parties.
8. All personal data will be held private and will be anonymised as soon as possible during data processing.

5.4.2 Ethics management methodology

For all demonstrator cases, in order to ensure that all proper procedures will be followed for collecting and handling data, the process depicted in Figure 3 will be followed. The methodology defines four phases for supporting the pilots' activities from the ethical and legislation aspects, namely the Planning, Ethics Management Principles, Data Management Plan, and Pilot Demonstration Activities. Each phase is associated with specific activities.

Main points are listed below:

- Detailed informed consent forms including all required project information must be prepared for the pilot participants and owners. Native language shall be used where required.
- Permission from the national data protection authorities should be taken for each of the pilots prior to the deployment of InCUBE software and equipment.
- NDAs shall be signed between InCUBE pilot responsible partners and building owners for the data collection and use, in cases where the buildings are not owned by Consortium members.

- Pilot responsible partners should identify and introduce Data Protection Officers (DPOs) and Data Controllers for the proper execution of the Data Management Plan according to ethical requirements.

The methodology will ensure that:

- All the end-user participants are fully aware of the InCUBE objectives and the data that will be collected to fulfil them.
- It will not be possible to distribute sensitive data to external parties outside of the project.
- Access to all InCUBE partners to the data necessary for the completion of the research, will be provided, as needed.
- Data minimisation principle will be applied, meaning that only necessary data to accomplish the objectives will be collected.

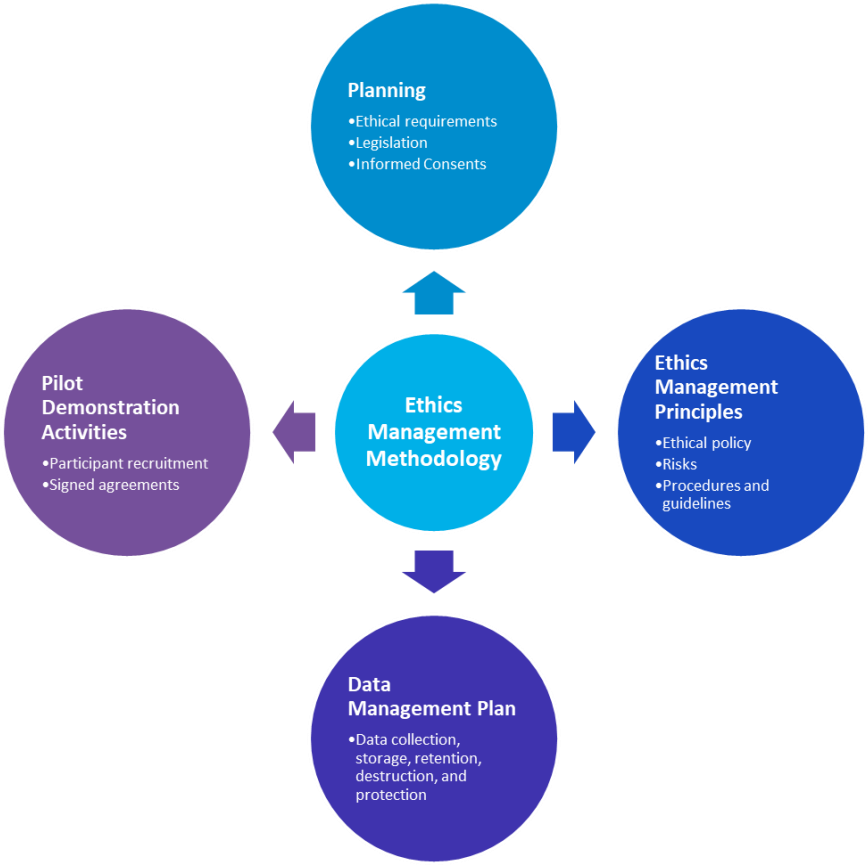

Figure 3 – Ethics Management Methodology

5.4.3 Methodology and guidelines for the delivery of Informed Consent

It is expected that some of the project activities will imply processing of personal data and therefore fall within the scope of the GDPR. Thus, informed consent procedures must be implemented for the participation of humans. InCUBE will collect and store personal data only if it is absolutely necessary

for achieving the project goals and will whenever possible process encrypted/anonymised personal data only. Research on personal data that has been collected on a legal basis will be carried out on condition that the consent of data subjects exists.

The research participants' consent will be obtained through a two-stage procedure:

- Initially the respective pilot leader will orally describe the pilot in which people will be involved and will also carefully describe the level of privacy infringement that the pilot involves. In case the person wants to exercise his/her right not to know, he/she will be excluded by the pilot.
- Secondly, after a few days, subjects will be required to read and sign an informed consent form that will explain in plain English and in local language what the experiment/pilot leader has already orally explained. Informed consent forms in English and in local language will be sent to the Research Executive Agency and included in the experimental protocol. A consent form template and an example are provided in ANNEX III and ANNEX IV respectively.

The Consortium will take the appropriate actions in order to ensure that:

1. Data cannot be collected without the explicit informed consent of people under observation; no person unable to express a free and informed consent for age-related reasons, ongoing medical and/or psychological conditions, mental incapacity, will be participate in Use case activities;
2. Data collected may not be sold or used for any different purposes from the InCUBE project;
3. Any data, which is not strictly necessary to accomplish the current study, will not be collected; data minimisation policy will be adopted at any level of the project and will be supervised by the ethical/privacy component of the project;
4. Any shadow (ancillary) personal data obtained in the course of the observation will be immediately cancelled.

6 Conclusion

This document presented the first version of the InCUBE Data Management Plan (DMP) along with the ethics management framework that will be followed in the project lifetime. Special focus has been given on information about open access to research data as it is important for proper exploitation of such data. Additionally, key points of the General Data Protection Regulation have been highlighted along with the main national legislations on data protection of Italy, the Netherlands, and Spain, where the piloting activities will take place. The DMP addresses topics and defines procedures that will facilitate the protection of user rights and the work of the Consortium, such as the open access policy, data handling and sharing, and procedures that will be followed for data collection, storage, retention and destruction.

A dataset identification template has been created by including various properties and by considering guidelines on FAIR Data Management, allowing to define datasets descriptions. Project partners are responsible for the collection and management of different types of data in the three pilot sites that are located in Italy, Netherlands, and Spain. At this phase of the project, it is difficult to specify in detail the relevant datasets that will be developed within the projects' activities. This process will be supported by the studies and the tests on the pilot sites. Further information about the anticipated datasets that will be generated within the project will be provided in the next version of the DMP, after the finalisation of the InCUBE architecture and the definition of the different use case scenarios. The DMP is a living document, and therefore updated versions will be delivered throughout the project's duration following the InCUBE progress presenting updated information.

Annex I – GDPR Checklist

GDPR checklist
Lawful basis and transparency
Contact an information audit to determine what information you process and who has access to it.
Have a legal justification for your data processing activities.
Provide clear information about your data processing and legal justification in your privacy policy.
Data security
Take data protection into account at all times, from the moment you begin developing a product to each time you process data.
Encrypt, pseudonymize, or anonymize personal data wherever possible.
Create an internal security policy for your team members, and build awareness about data protection.
Know when to conduct a data protection impact assessment, and have a process in place to carry it out.
Have a process in place to notify the authorities and your data subjects in the event of a data breach.
Accountability and governance
Designate someone responsible for ensuring GDPR compliance across your organization.
Sign a data processing agreement between your organization and any third parties that process personal data on your behalf.
If your organization is outside the EU, appoint a representative within one of the EU member states.
Appoint a Data Protection Officer (if necessary)
Privacy rights
It is easy for your customers to request and receive all the information you have about them.
It is easy for your customers to request to have their personal data deleted.
It is easy for your customers to ask you to stop processing their data.
It is easy for your customers to receive copy of their personal data in a format that can be easily transferred to another company.
It is easy for your customers to object to you processing their data.
If you make decisions about people based on automated processes, you have a procedure to protect their rights.

Annex II – Non-Disclosure Agreement (NDA)

Non-Disclosure Agreement

CONFIDENTIAL DISCLOSURE AGREEMENT

THIS AGREEMENT dated DD/MM/YYYY, by and between [Name of the Data Owner] ("Discloser") and [Name of the InCUBE partner] ("Recipient").

WHEREAS, [Discloser] and [Recipient], for the purpose of establishing a cooperative relationship and pursuant to the research related to InCUBE project, anticipate that [Discloser] may disclose or deliver to [Recipient] building data and information, energy consumption information, building occupancy information, drawings, data, sketches, specifications, and other materials, both written and oral, of a secret, confidential or proprietary nature, including without limitation any and all information relating to marketing, finance, forecasts, research, prepared or filed by or behalf of by [Discloser], in any jurisdiction, and any amendments or supplements thereto (collectively, "Proprietary Information"); and

WHEREAS, [Discloser] desires to assure that the confidentiality of any Proprietary Information is maintained;

NOW, THEREFORE, in consideration of the foregoing premises, and the mutual covenants contained herein, [Discloser] and [Recipient] hereby agree as follows:

1. Under this Agreement the [Recipient] undertakes: **(i)** to hold in trust and confidence and not disclose, without the express prior written consent of the [Discloser], to any third party (including a Recipient's Affiliates) or others or use for [Recipient]'s own benefit or for the benefit of any third party or others, any Proprietary Information, in any form, which is disclosed to [Recipient] by [Discloser] at any time and **(ii)** to carry out all necessary and appropriate measures to ensure that the Proprietary Information is protected against any access by third parties or others. [Recipient] shall disclose Proprietary Information received under this Agreement to person within its organization only if such persons **(i)** have a need to know and **(ii)** are bound in writing to protect the confidentiality of such Proprietary Information under the same terms as this Agreement. This paragraph 1 shall survive and continue after any expiration or termination of this Agreement and shall bind [Recipient], its employees, agents, representatives, successors, heirs and assigns. In compliance with the European Union's General Data Protection Regulation, the [Recipient] agrees to adhere to the confidentiality expectations as outlined in the EU General Data Protection Regulations (GDPR) and require the same of any subcontractors that perform services in conjunction with this Agreement.

   In the event that the [Recipient] is required by mandatory law or regulation or by order of a court, government department or agency or recognized stock exchange to disclose any

Proprietary Information, the [Recipient] shall provide the [Discloser] with prompt notice of such requirement – to the extent that such notice is permitted by law or regulation – so that the [Discloser] may seek a protective order or other appropriate remedy or waive compliance with the provisions of this Agreement. Whether or not such protective order or other remedy is obtained, or whether the [Discloser] waives compliance with the provisions of this Agreement, a [Recipient] shall disclose only that portion of the Proprietary Information, which is legally required to be disclosed based on the advice of the [Recipient].

2. The undertakings and obligations of [Recipient] under this Agreement shall not apply to any Proprietary Information which: **(a)** is disclosed in a printed publication available to the public, or is otherwise in the public domain through no action or fault of [Recipient]; **(b)** is generally disclosed to third parties by [Discloser] without restriction on such third parties, or is approved for release by written authorization of [Discloser]; or **(c)** is shown to [Discloser] by [Recipient], within ten (10) days from disclosure, by underlying documentation to have been known by [Recipient] before receipt from [Discloser] and/or to have been developed by [Recipient] completely independent of any disclosure by [Discloser].
3. Title to all property received by [Recipient] from [Discloser], including all Proprietary Information, shall remain at all times the sole property of [Discloser], and this Agreement shall not be construed to grant to [Recipient] any patents, licenses or similar rights to such property and Proprietary Information disclosed to [Recipient] hereunder.
4. [Recipient] shall, upon request of [Discloser], return to [Discloser] all documents, drawings and other materials, including all Proprietary Information and all manifestation thereof, delivered to [Recipient], and all copies and reproductions thereof. Unless required otherwise by mandatory law, the [Recipient] shall destroy all copies of any Proprietary Information. Upon the [Discloser's] request the [Recipient] shall confirm compliance by the [Recipient] with the obligations under this paragraph 4 in writing.
5. The Proprietary Information is provided without any representation or warranty, express or implied, as to its accuracy or completeness. Each Party hereby agrees that the [Recipient] will assume full responsibility for all conclusions that the [Recipient] derives from the Proprietary Information. The [Discloser] shall have no liability with respect to the Proprietary Information, errors therein or omissions there from in any manner and on any legal ground.
6. The parties further agree to the following terms and conditions:
    a. The [Recipient] agrees to be fully responsible and liable to the [Discloser] for any actions or failures to act which result in a breach of this Agreement. Any breach by [Recipient] of any of [Recipient]'s obligations under this Agreement will result in irreparable inquiry to [Discloser] for which damages and other legal remedies will be inadequate. In seeking enforcement of any of these obligations, [Discloser] will be entitled (in addition to other remedies) to preliminary and permanent injunctive and

other equitable relief to prevent, discontinue and/or restrain the breach of this Agreement.

b. If any provision of this Agreement is invalid or unenforceable, then such provision shall be construed and limited to the extent necessary, or severed if necessary, in order to eliminate such invalidity or unenforceability, and the other provisions of this Agreement shall not be affected thereby.
c. In any dispute over whether information or matter is Proprietary Information hereunder, it shall be the burden of [Recipient] to show both that such contested information or matter is not Proprietary Information within the meaning of this Agreement, and that it does not constitute a trade secret.
d. No delay or omission by either party in exercising any rights under this Agreement will operate as a waiver of that or any other right. A waiver or consent given by either party on any one occasion is effective only in that instance and will not be construed as a bar to or waiver of any right on any other occasion.
e. This Agreement shall be binding upon and will inure to the benefit of the parties hereto and their respective successors and assigns.
f. This Agreement is governed by and will be construed in accordance with the law of {COUNTRY}, and the courts of {TOWN}, {COUNTRY} shall be the exclusive forum. (TOWN and COUNTRY is the town and the country of the Discloser respectively).
g. This Agreement is in addition to any prior written agreement between [Discloser] and [Recipient] relating to the subject matter of this agreement; in the event of any disparity or conflict between the provision of such agreements, the provision which is more protective of Proprietary Information shall prevail.

This Agreement may not be modified, in whole or in part, except by an agreement in writing signed by [Discloser] and [Recipient].

IN WITNESS WHEREOF, the parties have executed this Agreement as of the date first above written.

[Discloser]	[RECIPIENT]
By: _____	By: _____
Signature	Signature
_____	_____
Printed Name	Printed Name
_____	_____

Annex III – Consent Form Template

Project Purpose

- A commonly understandable written description of the project and its goals even for people that are not familiar to the project scope (2-3 paragraphs)

Project Progress Schedule

- The progress schedule of the project and the related testing and evaluation procedures (1-2 paragraphs) and benefits

Disclaimer Rights

- Advice on unrestricted disclaimer rights on their agreement

Confidentiality

- A description of the applied data privacy measures

Voluntary participation

- A statement about the voluntary participation and the right to terminate the participation

Contact information

- Contact details of responsible InCUBE representative

Voluntary Participation Form

1. General Information
   - Participant basic information
   - ID (reference code) of the participant, which will be used throughout the pilot trial execution

2. Study Information
   - Details about the pilot Use Case

3. Participant's Questionnaire
   - has been fully informed on the purpose, duration, procedures of the study;
   - has been informed on the rights to deny participating or to quit from the study and about the corresponding consequences.

- has been informed on the contact person in case that I have questions and queries about the study.
- had adequate time to make my decision concerning my participation in the study.
- comprehend that he/she can quit from the study at any time without having to justify his/her decision.
- has been informed about potential effects, difficulties and dangers.
- has been informed about the sensors equipment that will be used to collect data.
- has been informed about the security of the study data and results.
- has been ensured about the confidentiality of his/her personal information. Publications of the study results do not allow the personal data recognition, due to the principle of anonymity.

4. Signed Consent to Participate

- A signed consent of the participant allowing the study responsible to examine and inspect the data collected during the study.

Annex IV – Consent Form Example

An INClUsive toolBox for accElerating and smartening deep renovation

This project has received funding from the European Horizon Europe Research and innovation programme under Grant Agreement: 101069610

Purpose of the study

This document was created on behalf of the InCUBE project (Grant Agreement N°: 101069610), funded by the European Union under Horizon Europe, with the main objective to develop and test innovative solutions to unlock the EU renovation wave.

InCUBE will develop cutting-edge standardized, lean integrated processes based on 4 key pillars of innovation: 1) Industrialization: Off-site manufactured solutions including the use of robots, so far applied only in industrial environments, offering novel services; 2) Novel self-RES power producing and storage technologies, products and environmentally friendly materials; 3) Digitalization: Dynamic Digital Twins of both products and buildings, utilizing immersive capturing techniques (e.g., Laser 3D scanners and Drones), digitally merging innovative manufacturing processes with BIMs, and 4) New market entrants, organized under novel business models, to allow for increased levels of collaboration and productivity.

The InCUBE Suite, integrates digital tools across all four pillars, enables for seamless coordination of different renovation phases while leveraging data streaming from multiple interoperable sources to accommodate tenants' comfort and render buildings active energy nodes in the synergetic energy networks paradigm of the future. The solutions will be validated in 3 large-scale demo sites in 3 countries (IT, ES, NL).

Confidentiality

Collected information are to be kept confidential and data processing will be applied on anonymised data. The procedures for data access and data processing that will be followed are in accordance with rules of the General Data Protection Regulation (GDPR). Safe data sharing is foreseen by fully enforcing and protecting user rights. For the data that will be shared only among the consortium members, authorization and authentication mechanisms will be used in order to restrict access and ensure that only the appropriate users can retrieve the data. Selected not sensitive and anonymized data may be made publicly available for scientific purpose. Special category data, e.g. personal data revealing ethnic origin, political opinions, genetic data, data concerning health, or criminal offence data, as defined in the GDPR, are not relevant to the project and are not collected.

Voluntary participation

Participation in this study is completely voluntary. There will not be any negative consequences if you decide not to participate. Please be notified that if you decide to participate, you may terminate your participation at any time and you may decide not to answer any specific question.

Contact information

In case of any questions about this project or problems you may face, feel free to contact

Contact person: _____ E-mail: _____

Address: _____

Voluntary Participation Form in the InCUBE project

1. Participant's Information

Full name	
Reference code	

2. Study Information

Country	
Infrastructure type	
Infrastructure address	
Representative of the pilot	

3. Participant's Questionnaire

I have read the InCUBE project information sheet and I have been informed about the purpose, expected duration and procedures of the study.	**Yes**	**No**
I was orally informed about the purpose, expected duration and procedures of the study by the responsible person.	**Yes**	**No**
I was informed of my right to refuse to participate or to leave the study.	**Yes**	**No**
I was notified of the contact person, in the case I have questions and queries about the study or about my personal data being collected.	**Yes**	**No**
I was given a copy of my filled in consent form.	**Yes**	**No**
I had enough time to decide on my participation in the study.	**Yes**	**No**
I understand that I can leave the study at any time, without having to justify it and to require deleting my personal data.	**Yes**	**No**
I have been informed of the recording equipment that will be installed in my environment for the purposes of data collection.	**Yes**	**No**
I was informed about the storage procedures of the study data.	**Yes**	**No**
I was informed about the personal data that will be collected, the processors and the procedures that will take place, as well as my rights according to the General Data Protection Regulation. Publication of study results does not disclose personal data. Always according to the principles of confidentiality, I allow researchers involved in the study and signing respective NDAs can utilize the information for the purpose of the study and only for this.	**Yes**	**No**
I agree to the use of the collected data also after the termination of the InCUBE project.	**Yes**	**No**

By signing this form, I am attesting that I have read and understand the information that have been provided above and I freely give my consent to participate in the study.	**Yes**	**No**

Date Reviewed & Signed:_____ **Signature:** _____