D8.3 – Data and Ethics Management Plan

COMMUNITAS

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement **No. 10196508**

D8.3 – Data and Ethics Management Plan

Dissemination Level: PU - Public
Lead Partner: EDP L
Due date: 30 of June 2023
Actual submission date: 30 of June 2023

Published in the framework of:

Bound to accelerate the roll-out of Energy Communities and empower consumers

Authors:

Filipe Neves da Silva, EDP L
Humberto Queiroz, EDP L
Cláudia Fernandes, EDP L
Maria Leonor Pereira, EDP L

Revision and history chart

Version	Date	Editors	Entity	Comment
0.1	01/06/23	Filipe Neves da Silva Humberto Queiroz Cláudia Fernandes Maria Leonor Pereira	EDP L	First version
0.2	30/06/23	Filipe Neves da Silva	EDP L	Review

Disclaimer:

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement **No. 10196508**

Table of contents

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement **No. 10196508**

List of figures:

Glossary:

Acronym	Full name
API	Application Programming Interface
CCP	COMMUNITAS Core Platform
CEP	"Clean energy for all Europeans" package
DEMP	Data and Ethics Management Plan
DPO	Data Protection Officer
EC	Energy Community
EU	European Union
GDPR	General Data Protection Regulation
IoT	Internet of Things
IP	Intellectual Property
KER	Key Exploitable Result
KO	Key Objective
KPI	Key Performance Indicator
M	Month
SSH	Social Science and Humanities
WP	Work Package

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement **No. 10196508**

1. Executive summary

The Data and Ethics Management Plan defines the processes that ensure the privacy of stakeholders and ethical data handling throughout the project. It aims to secure any data, in particular personal data, from being released or published inadvertently and promotes compliance with all legal requirements for data protection, as well as with ethical guidelines. By providing the Data and Ethics Management Plan, the consortium expects that all parties will implement secure and ethical practices in the processes that involve the collection and usage of data from any stakeholders, promoting the transparency of all research conducted in COMMUNITAS project.

The COMMUNITAS project requires data collection in the scope of the development and validation of solutions for the Energy Communities, but also in all interactions with the members of these communities. The data management strategy proposed follows the FAIR principles (Findability, Accessibility, Interoperability, Reusability). The use of organised repositories and common metadata descriptions will enable the data to be findable. The data will be accessible to authorized users and anonymous data used for research will be published in accordance with legal requirements. A common architecture, the COMMUNITAS Core Platform, will be built to ensure the interoperability of the data. The use of open-access repositories (e.g. GitHub) will be considered as an option to increase the reusability of the data. The data management plan also provides measures that can increase the security of the data such as encryption.

The Ethics Management Plan provides a set of measures that prioritise the privacy and confidentiality of stakeholders. Measures such as the anonymization and pseudonymization can be employed to prevent inadvertent sharing of personal data. Informed consent will be obtained for all data collection activities. Although each partner is responsible for implementation the action plan and is ultimately responsible for any data collected in its activities, an Ethics Manager will oversee and support partners in the implementation of the plan, so as to ensure compliance with GDPR practices and other guidelines. Additionally, the plan promotes fairness and equity, including details on the elimination of bias and gender balance.

The Data and Ethics Management Plan will be updated twice during the project to reflect changes that might require adaption of the currently described practices for data privacy and security. These updates will be included within the Project Management Roadmap updates corresponding to D8.4 and D8.5, due to M12 and M27, respectively.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement **No. 10196508**

2. Introduction

2.1. Objectives

The Data and Ethics Management Plan (DEMP) outlines a comprehensive action plan that ensures data privacy and confidentiality and an ethic handling of data. The goal of the DEMP is that all consortium partners involved in the collection and usage of data from external sources can implement the correct procedures to safeguard the integrity of that data, ensuring compliance with any legal requirements applicable, such as the GDPR, and handling the data following and ethical approach and the FAIR principles.

2.2. Structure of the document

The deliverable is structured in the following sections:

- Section **Error! Reference source not found.** – Data Management Plan – details all the information required to ensure the privacy and confidentiality of the data collected and used in the project.
- Section 4 – Compliance and Legal Considerations – outlines the legal requirements relating to data handling and privacy that need to be considered in the scope of the project's activities.
- Section **Error! Reference source not found.** – Ethics Management – highlights ethical methods that should be put into practice in the consortium to mitigate bias and misinformation, and to promote privacy and anonymity.
- Section **Error! Reference source not found.** – Data and Ethics Governance – details the roles and responsibilities of the structure that will be put in place to implement and oversee the practices defined in the DEMP.

A final section indicates some of the references used to build the DEMP.

2.3. Relation to other tasks

D8.3 is part of the Project Management Strategy, incorporate in D8.1 – Project Management Roadmap, and D8.2 – Quality and Risk Management Plan. Two updates will be provided throughout the project, updating all three deliverables (D8.1, D8.2, and D8.3). These updates will provide insights on any changes on the current plans and strategies that might occur due to different conditions ahead in the project. The first update, D8.4 – Project Management Roadmap – version 2, will be delivered by the end of the first year of the project, and the second update (D8.5 – Project Management Roadmap – version 3) will be delivered by M27.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement **No. 10196508**

3. Data Management Plan

3.1. Data summary

The European Commission introduced the "Clean Energy for all Europeans" package (CEP) to promote energy community projects and increase citizen participation in energy markets. To overcome barriers and facilitate the adoption of these concepts, the COMMUNITAS project aims to promote energy citizenship and empower citizens to actively engage in energy markets. It will provide a Knowledge Base with administrative, legal, technical, financial, social, and other information on ECs, streamlining their creation and expansion. Additionally, the project will develop innovative tools using technologies like IoT, Blockchain, and Cloud Computing, integrated into a digital platform called the COMMUNITAS Core Platform (CCP). These tools will enable citizens to participate in energy markets and communities, allowing them to aggregate their position in the market and explore ancillary services using various energy assets or load profiles. Throughout the project, citizens will be involved in Social and Policy Labs to incorporate their feedback and ensure their needs are considered in the project's development.

The role of data collection and generation must be fully described in order to successfully comply with the goals of the COMMUNITAS project. Data goals are actively required for the innovation generation process. Research and innovation developed throughout the project directly depends on the gathering of data. It allows for the identification of areas with potential for innovation and aspects that need to be improved upon. In order to structure the data collection and generation process, it is important to identify the project's structure.

Activities related to data collection will begin with the development of the state-of-the-art, with the gathering of already existing data from various scientific papers and relevant websites. Social engagement activities to be promoted in WP1 and WP4 will also require collection of new data amongst citizens and stakeholders, in the form of surveys and workshops. This directly impacts the definition of the Knowledge Base (to be developed in WP1) with the gathering of wishes, needs and recommendations of the involved stakeholders, benefiting the development of the creation and expansion processes of energy communities. The solution development phase will be influenced by the setting of technical, economic, and social KPIs to make use of indicators applied as inputs for the plan phase, to be implemented in later stages. This will occur through WP2, WP3 and WP5. Destination impacts are also focused on already available data regarding electrical energy consumption and generation (via smart meters), ventilation speed, room setpoint, district heating thermal consumption and production, electrical energy consumption (EV charging points) and natural gas consumption.

Collection of real data from pilots will be part of the pre-monitoring phases and baseline. Pilot sites require both data that is already available, as well as extensive data acquisition that requires consequent examination. This activity will mainly revolve around WP5. Regarding solution deployment, data utility is based upon the concept of centralizing citizens in the data collection process, as to empower them as fully-fledged energy market players via an innovative methodology for citizens and consumer engagement and value-based proposition design in ECs, which is one of the COMMUNITAS' key objectives – KO5, to be further developed in WP1, WP3, WP4, and WP5. The monitoring phase will be based upon real data collection from pilot sites and its validation. The consequent data treatment and generation of new data is key for the creation of the knowledge base and development of the innovative tools. These tools may also require constant monitoring and

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement **No. 10196508**

evaluation of certain parameters. This will account for the identification of stakeholder's needs for improvement and incentivization towards a more sustainable goal. Also, the collected data will serve for tool optimization, in order to provide improved accuracy in informing on energy efficiency and cost saving opportunities. Data collected from monitoring phases of pilot sites require harmonization and pre-processing to ensure proper data quality. It also directly supports ECs through KO7, in the collection of data from commercial platforms with a vast portfolio of clients and commercial route from the COMMUNITAS' partners. It allows for the generation and validation of sustainable Business Models targeting the uptake of ECs, local energy and flexibility markets, together with supporting policy recommendations.

Regarding the final phase, a benchmark will be comprised of both comparisons between results from other pilots or projects and already implemented market solutions. COMMUNITAS will enhance data collection by setting P2P markets and DR pilots in Leader and Learner pilots, adding 3 new data sources (weather, flexibility, and traded energy), and increasing by 25% he availability of data sources.

Data types and formats can be divided in several categories. Project deliverables, reports, questionnaires, or other document type will be shared and stored in Microsoft Word (.docx) and PDF (.pdf) formats. Visual presentations will be supported by Microsoft PowerPoint (.pptx). Data repositories and data acquisition files represented in the form of tabular data will be stored in Microsoft Excel (.xlsx) or Comma Separated Values (.csv). Dissemination materials, such as images, graphics, videos, etc., will be stored as TIFF (.tif), JPEG(.jpg), PNG(.png) and MPEG-4 (.mp4). Audio files will be added as Free Lossless Audio Codec (FLAC) (.flac). The expected data size is not yet possible to defined since there is no previous database in which the prediction of data size can be modelled upon.

3.2. FAIR data

The Data and Ethics Management Plan (DEMP) follows the EU guidelines and describes the data management procedures according to the FAIR (Findability, Accessibility, Interoperability, and Reusability) principles, which emphasize the capacity of computational systems to find, access, interoperate, and reuse data with none or minimal human intervention. COMMUNITAS is creating a European knowledge database (will implement a process of knowledge, with consolidation, enable cooperation and will allow for the creation of new knowledge), through the development of the Knowledge Base. Furthermore, energy and non-energy data from the pilots will be gathered to feed the tools of the COMMUNITAS Core Platform (CCP). Regarding these data, the following sections explain how it will be ensured that the different datasets defined in section 3.1 will comply with the FAIR data principles.

Making data findable, including provisions for metadata

Metadata and data should be easy to find, and so, to facilitate that process, COMMUNITAS will describe the datasets defined in section 3.1 by promoting a naming convention, clear versioning, and an intuitive organization of the repository.

For a proper management and usage of the datasets listed in section 3.1, COMMUNITAS will describe them with metadata previously described, that explain in more detail the available information including the specific variables and covering the 5Vs of big data (volume, value, variety, velocity, and veracity). All the aspects involving data acquiring and format will be defined in deliverable D2.1, titled

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement **No. 10196508**

"COMMUNITAS Core Platform architecture and specifications", which has the deadline for submission at the end of M12 (December/2023).

Regarding the management of the files generated by the partners during the project activities, a SharePoint channel is created and managed by EDP L as project coordinator. This SharePoint follows the work breakdown structure presented in the Grant Agreement (WPs, Tasks, and Deliverables), and includes three additional folders:

- Official documents: Grant agreement and Consortium agreement (.pdf format).
- Meetings: divided into subfolders for each WP, containing documents of every meeting related to the respective WP.
- Templates: for uniform work between the Consortium partners, with presentations (.pptx) and deliverables (.docx) templates.

Furthermore, there is a restricted file which has the contact of all the project participants, named "Mailing list". Figure 1 shows the organization of COMMUNITAS SharePoint.

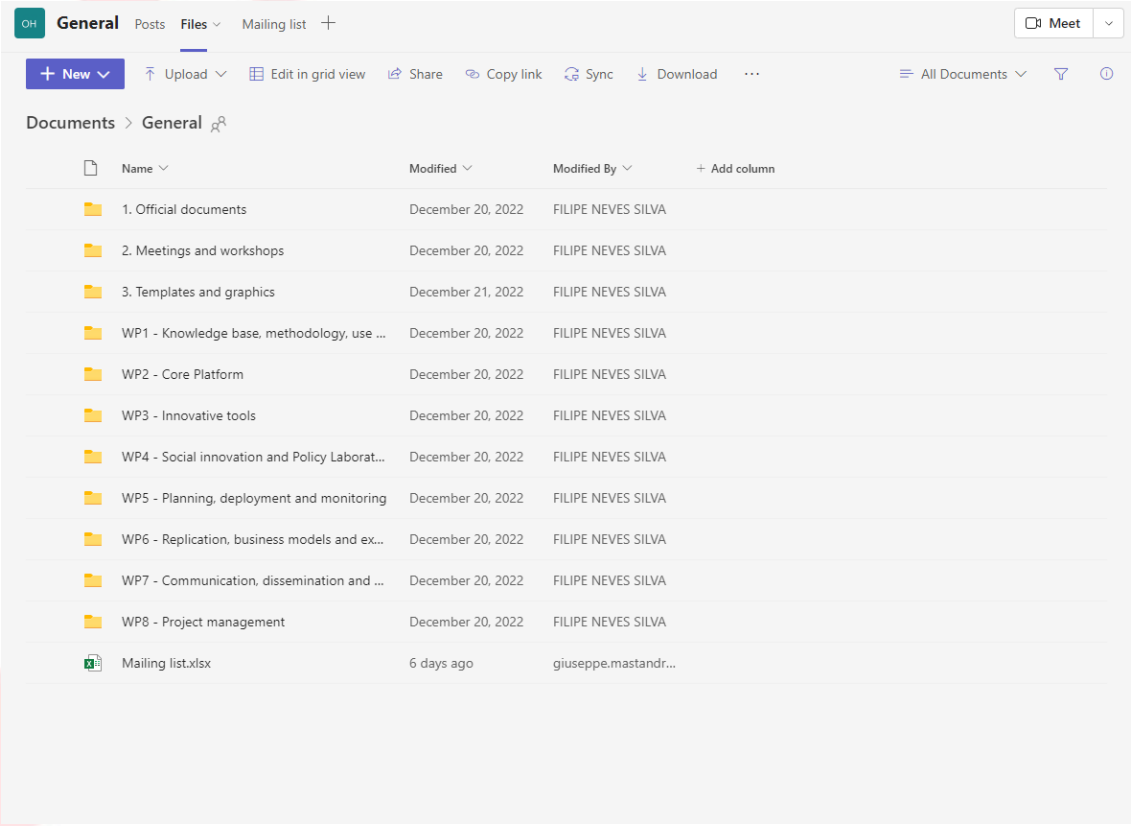

Figure 1 - COMMUNITAS Sharepoint

Making data openly accessible

Datasets tend to degrade or disappear over time because there is a cost to maintaining an online presence for data resources. Therefore, data accessibility involves ensuring long-term storage that

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement **No. 10196508**

allows for easy access and downloading. This is achieved by implementing clear licenses and access conditions, both at the metadata level and for the actual data content.

The data acquired from the pilots, which will feed the tools inside the CCP are yet not defined. The final list of the datasets, and all information derived (format, storage, metadata information etc.) will be detailed described in deliverable D2.1.

Regarding the accessibility of the data from COMMUNITAS, two different cases are defined depending on the access level: sensitive or public. The deliverables classified as sensitive, thus restricted to the consortium members, will be available on COMMUNITAS SharePoint repository, which requires the permission of the manager of the channel (EDP L). Other repositories will be used to publish public information such as project deliverables, tools, and scientific articles. All public deliverables will be automatically submitted in Cordis, the EU platform for research results (available at https://cordis.europa.eu/project/id/101096508), and public deliverables and other information will be published in the project website, at http://communitas-project.eu/.

Making data interoperable

Data Interoperability is paramount to set the grounds for a common European data environment. In fact, it is necessary to stablish a common framework to enable the communication not only at consortium level but with other sister projects and other cross sector initiatives.

In this sense, COMMUNITAS will define an open-source common reference architecture, API specifications and semantic data models as per defined in the requirements related to interoperability. The **User and Data Management modules (developed in the scope of T2.3 – COMMUNITAS Core Platform development)** manages the secure and privacy-preserved access to the data and user credentials. Aiming to deal with high velocity, volumes, and varieties of data, still guaranteeing data integrity, solution scalability and interoperability, different technologies will be evaluated in the CCP, such as PostgreSQL, MongoDB, HBase and Cassandra CCP. Furthermore, project will use recognized standards and formats for (meta)data to facilitate further usage by third-party systems. Appropriate vocabularies will be developed to ensure interoperability, key to COMMUNITAS, as its CCP (T2.3) will integrate services from diverse entities. APIs (T2.5) will be set to ensure interoperability (e.g., REST APIs, event-based APIs, data access APIs, MQTT data APIs) between the project and third-party tools (WP3). Two types will be set: Things APIs and Services APIs.

Increase data re-use (through clarifying licenses)

Data will be made available as soon as possible and published in open access repositories (e.g. Zenodo), always respecting the GDPR and other privacy directives. All public material will be available during and after the project. To ensure reusability, data will be described as much as possible with accurate attributes. Costs of making data FAIR will be determined in the Data Management Plan. Also, by adopting a DevOps approach towards the development of CCP and other project's tools (T2.6 - COMMUNITAS Core Platform DevOps and Validation), developers will merge their code changes into a central repository (e.g GitLab, GitHub), after which main stages will be implemented, such as automated builds, tests, run and release to production. Finally, as a project that will deeply involve citizens, not only the GDPR will be followed when dealing with personal data, but also the Universal Declaration of Human Rights and other relevant national laws that will be identified in the Data Management Plan. Regarding the data that will be fed into the CCP, it is assured the reusability due to

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement **No. 10196508**

the interoperability procedures described in this document. Detailed information will be described in D2.1. The data will remain reusable during the project duration. Since the CCP and its tools will remain active after the project ending, data will be reusable for the whole duration of the platform.

Regarding data quality, the process will be supervised by all the consortium, and will consist of 4 steps. The first one regards on the establishment of the way in which the collection and processing of data is managed. This should be done by distinguishing the different types of data managed in the project: data collected or generated in the different use cases, data reused from other EU project initiatives or data from project communication and dissemination activities. The second act regards on the definition of the responsibilities of each of the roles involved in the process. The next step is the determination of the quality parameters according to the six main dimensions that are commonly used to mark the quality of the same: accuracy, completeness, consistency, validity, uniqueness, and timeliness. Lastly, the implementation of the set of technical tools and KPIs that will be used to measure and ensure the quality of the data. The type of tools to be used will be defined throughout the project according to its needs.

3.3. Allocation of resources

Allocation of resources related to making data FAIR in COMMUNITAS depends on the amount of data processed during the project lifespan. This amount is associated with the cost of long-term storage solutions, which can be different according to the specific data sets that are considered and their computational size. The main project outputs will be published under an open-source license (e.g., CC-BY 4.0) and will be made available as a GitHub repository. Efforts for publications should also be considered in the allocation of resources together with their potential value and the most suitable ways for applying the open-access approach.

The estimation of the costs is influenced by many factors which are and will be discussed within the consortium. Responsibilities for data management in the project can be already defined and will be taken into charge by the Project Coordinator (EDP L). Therefore, the Project Coordinator is responsible for:

- Maintaining the project document repository.
- The quality of any scientific data outcomes.
- Identifying outputs suitable for publication in the considered repositories.
- Maintaining COMMUNITAS inputs for Open Access.
- Ensuring that data shared through the website is easily and freely available but also that backups are performed.

However, each partner is responsible for the recoverability of its own generated data.

3.4. Data security

Managing the data in a secure way is a fundamental task for the project's success. Besides data anonymization, there will be data encryption and backup distribution. The goal of these measures will be to ensure that data remains consistent over the lifetime of the project and there exist alternatives to the main files in case they disappear or get corrupted. The encryption component gives an extra

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement **No. 10196508**

layer of security to the data files and information. In COMMUNITAS Project, data governance and privacy will be achieved by guaranteeing the right to control the data at any time for data owners, monitoring and controlling the access to the data, and the Consortium undertaking all required efforts in preventing unauthorized data access. Hence, the primary responsibility to take necessary measures to ensure data security lies with the Project Partners.

The secure management of information will adhere to the guidelines of relevant standards (e.g. ISO/IEC 27001 and 27002; Code of practice for information security management) to ensure the triad of cyber security:

- Confidentiality – Preventing unauthorized disclosure of information.
- Integrity – Assuring that data cannot be modified in an unauthorized manner.
- Availability – Making information available for authorized users.

The information security management will further contain the Directive on security of network and information systems ('Cybersecurity directive', NIS-Directive 2016/1148) on the security of critical infrastructures and the ePrivacy Directive 2002/58, as well as European Union Agency for Network and Information Security (ENISA) guidance. Storage of information will fully comply with the national and EU legal and regulatory requirements.

COMMUNITAS Project Consortium members ought to appoint a person responsible for overseeing the protection of data whenever it is collected, generated, or stored. This data must be securely stored and regularly backed up, and multiple copies should be made to prevent data loss in the event of hardware failure of large-capacity hard drives. These multiple copies should be also stored at different locations, but always stored in the online collaboration tool of the Project (SharePoint), which is only accessible by authorized consortium partners (i.e., via username and password login). Further access restrictions on specific folders may be enabled if needed. Moreover, SharePoint in Microsoft 365 do not use data for anything else than providing the customers the services they have subscribed for. As a service provider, Microsoft 365 does not scan email, documents, or teams for advertising, and it does not have access to uploaded content.

3.5. Ethical aspects

COMMUNITAS' consortium is fully aware of the privacy and data protection issues that might arise, declaring its strict compliance with all European and national legislation and directives relevant to the country where the data collections are taking place. Therefore, both ethical and legal issues involving data sharing are described in Section 4 of the Description of Action of the project. These aspects, as indicated in the Grant Agreement, will be monitored throughout the development of the COMMUNITAS' by taking into account the principles of human respect, gender balance, voluntary and informed participation and mutual duty of care. These actions are to be in conformity with ethical standards and the applicable EU international regulations for data protection and handling. The consortium is required to fully respect and ensure that both privacy and individual rights of participants and stakeholders are not violated. They are aware of EU and national legislation regarding personal data and privacy protection and committed to ensure that all the project's activities follow the European Chard of Fundamental rights and all data protection relevant EU regulations, standardisation, and policy initiatives.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement **No. 10196508**

Personal data collected in the forms of surveys or questionnaires is anonymous. The documents present, on the top of the first page, a description of the purpose of the form, alongside the indication of the document being anonymous to ensure privacy. An ethics manager from EDP L will be responsible for ensuring the progression of the project in accordance with the current rules and directives, local and EU-wide on ethics and data privacy, respecting all the legal procedures. Social engagement activities performed during workshops and dissemination activities that involve the collection of workshop photos and questionnaires require clear consent of the intervener and knowledge of purpose of use and time preservation of acquired data. Therefore, any individual participation in a project's activity will only asl for the name of the company in which the person is working on and the sector or stakeholder the company belongs to. This information does not contain any type of personal data of the person responding to any questionnaire/survey. The consortium commits, during dissemination and research activities, to not using any type of profiling of personal data.

Regarding long term preservation of data collected containing personal information, it is important to reference the role of ethical aspects that revolve around personal data concerns. As mentioned in the following subsection, from GDPR, Article 5, the data will be *"collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes"* and they will be *"kept in a form which permits identification of data subjects for no longer than is necessary for the purposes"*.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement **No. 10196508**

4. Compliance and Legal Considerations

4.1. Data Protection Regulations

The European Union's General Data Protection Regulation (GDPR) stands as a cornerstone of privacy legislation, changing the paradigm of personal data handling and protection within the EU. Implemented on May 25, 2018, the GDPR offers a comprehensive set of guidelines and rights for individuals, while imposing significant responsibilities and obligations on organizations that collect, process, or store personal data. Its overarching goal is to empower individuals with control over their personal information, harmonize data protection laws across EU member states, and ensure transparency, security, and accountability in the digital era. With its wide-reaching impact and extraterritorial scope, the GDPR has become a global benchmark for data protection and privacy regulations, influencing legislation and shaping best practices worldwide.

The GDPR introduces measures that raise the bar for businesses attempting to deceive customers using unclear or ambiguous language on their websites. Moreover, it ensures that:

- Visitors accessing the website are provided with clear information regarding the data being collected.
- Visitors are required to give their consent for the collection of this information by actively clicking a button or taking other actions on the website.
- Visitors are promptly notified in the event of any compromise to their personally identifiable information stored on the website.
- A mandatory evaluation of the website's data security is currently underway.
- An assessment is conducted to determine whether a new employee is needed to fulfil the role of the data protection officer (DPO) or if an existing employee can fulfil this responsibility.

Businesses have various methods to attain GDPR compliance. Conducting audits of personally identifiable information and maintaining comprehensive records of the collected and processed data are among the pivotal measures. Moreover, it is essential for businesses to regularly update privacy notices provided to website visitors and promptly rectify any identified errors in their databases.

For the purpose of this regulation, the following definition must be considered:

'personal data': 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. Personal data include data such as internet protocol (IP) addresses (unique identifiers that can be used to identify the owner of devices connected to the internet) and data from 'smart meters' monitoring energy usage by addresses linked to identifiable persons.

'processing': any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission,

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement **No. 10196508**

dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

'restriction of processing': the marking of stored personal data with the aim of limiting their processing in the future;

'profiling': any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

'third-party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

The European Commission, on 4th June 2021, approved two sets of standard contractual clauses. One set is designed for the utilization between controllers and processors within the European Economic Area , while the other set addresses the transfer of personal data to countries beyond the borders of the European Economic Area. In addition, both the GDPR imposes obligations on:

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

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement **No. 10196508**

- **Data processor:** a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.

Under the GDPR, transferring personal data from a non-EU country to another country requires specific measures to ensure the protection of personal data. The following steps are typically followed to comply with the GDPR when transferring personal data from a non-EU country:

a) **Determine the legal basis for transfer**: identify a valid legal basis for the transfer of personal data as provided in Article 6 and, if applicable, Article 9 of the GDPR. This may include obtaining the data subject's explicit consent, fulfilling a contract, or demonstrating compliance with legal obligations.

b) **Assess adequacy**: determine if the destination country ensures an adequate level of data protection as defined by the European Commission. Adequacy can be established through an adequacy decision by the European Commission or appropriate safeguards provided by the recipient country.

c) **Implement appropriate safeguards**: if the destination country does not have an adequacy decision, implement appropriate safeguards to protect the transferred data. This can be achieved using standard contractual clauses approved by the European Commission, binding corporate rules, or other approved mechanisms such as codes of conduct or certification mechanisms.

d) **Consider derogations**: in the absence of an adequacy decision or appropriate safeguards, assess if any derogations under Article 49 of the GDPR apply. Derogations allow transfers in specific situations, such as when the transfer is necessary for the performance of a contract, the protection of vital interests, or the establishment, exercise, or defence of legal claims.

e) **Inform data subjects**: provide transparent information to data subjects about the transfer of their personal data, including the purposes, legal basis, recipients, and safeguards implemented. This information should be included in the privacy notice or provided directly to the data subjects.

f) **Maintain documentation**: keep records of the transfer, the legal basis, the safeguards employed, and any relevant documentation to demonstrate compliance with the GDPR requirements. These records should be available for inspection by supervisory authorities.

4.2. Intellectual Property Rights

As innovation plays a central role in Horizon Europe projects, it is essential to establish a robust management strategy for intellectual property (IP) rights. This strategy ensures the protection, utilization, and exploitation of project results, while adhering to the guidelines set forth by the European Union's research and innovation framework program. In line with these objectives, the IP management strategy for the COMMUNITAS project will be detailed descript in Deliverable 6.4 (D6.4) titled "Final project IP strategy and exploitation plan of the most promising Key Exploitable Results (KERs)".

In summary, the IP management strategy aims to achieve the following objectives:

Identification and Protection: identify the key intellectual property assets generated within the project, including inventions, patents, copyrights, trademarks, and trade secrets. Implement measures to safeguard and protect these assets through appropriate legal mechanisms, such as patent applications and copyrights registrations.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement **No. 10196508**

Exploitation and Commercialization: develop an exploitation plan for the most promising Key Exploitable Results (KERs) generated by the project. This plan should outline the steps for bringing the KERs to market, including licensing agreements, spin-offs, collaborations, and technology transfer activities.

Collaboration and Open Innovation: foster collaboration with relevant stakeholders, including industry partners, research institutions, and potential end-users. Encourage open innovation practices, such as sharing knowledge, data, and research findings, to maximize the impact and value of the project's results.

To ensure effective IP management, the following 4 key elements will be incorporated into COMMUNITAS' framework:

IP Ownership and Rights: clearly define the ownership and rights associated with project-generated IP, taking into account the contributions of project participants and external collaborators. Establish agreements, such as Consortium Agreements or Memoranda of Understanding, to clarify IP ownership, access rights, and potential revenue sharing.

IP Valuation and Commercialization Strategy: develop a systematic approach for assessing the value of project IP, considering its market potential, competitive advantages, and potential societal impact. Based on this valuation, establish a commercialization strategy that aligns with the project's goals, timelines, and market dynamics.

IP Risk Management: identify potential risks associated with IP management, including infringement risks, competing technologies, and regulatory constraints. Implement measures to mitigate these risks, such as conducting freedom-to-operate analyses, monitoring IP landscapes, and establishing appropriate contractual provisions with collaborators and contractors.

Dissemination and Open Access: ensure compliance with Horizon Europe's Open Access policies and promote the dissemination of project results through open access publications, data sharing platforms, and public repositories. Consider embargoes or restrictions when necessary to protect potential IP rights during the commercialization process.

Regular monitoring, evaluation, and review of the IP management strategy will be conducted throughout the project's lifespan. This includes periodic assessments of IP assets, exploitation activities, and commercialization outcomes. Lessons learned and best practices will be documented and shared within the project consortium and with relevant stakeholders to optimize future IP management strategies.

4.3. Ethical Guidelines

The COMMUNITAS project is funded under the Horizon Europe programme. Therefore, the project will comply with ethical principles and relevant legislation on local, national, and European level. The project encompasses the implementation of data collection during the piloting and validation phase, along with conducting extensive validation tests to assess the technology and effectiveness of the proposed framework under real-life conditions, specifically within occupied households. The consortium fully recognizes the potential privacy and data protection concerns that may arise and affirms its unwavering commitment to adhere to all relevant European and national legislation, as well as directives applicable to the country where the data collections are conducted. This entails a

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement **No. 10196508**

thorough examination of the collection, processing, and transmission of personal data in accordance with the following principles:

a) The GDPR (Regulation (EU) 2016/679);

b) The Universal Declaration of Human Rights and Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data; and

c) national laws that implement these provisions.

Additionally, any additional national-level regulations pertaining to data protection or other sensitive information, excluding GDPR jurisdiction, will be duly considered. The management of project data will strictly adhere to the following prerequisites:

(i) Consent from the data subject;

(ii) Necessity for performance of or entering a contract;

(iii) Compliance with a legal obligation;

(iv) Protection of the vital interests of the data subject.

To ensure compliance with these requirements, personal data handled within the COMMUNITAS project will undergo anonymization and be stored in a format that precludes user identification. COMMUNITAS will establish a comprehensive data management framework that guarantees the security of collected personal data, guarding against potential abuse, theft, or loss. While most research data generated by the project will be publicly accessible and shared, personal user data will be exempted. The DEMP will provide detailed information regarding the types of data produced by the project, its potential exploitation, accessibility for verification and re-use, as well as the strategies for curation and preservation.

The following principles govern the management of Knowledge and Intellectual Property Rights within the COMMUNITAS project and will be established in the consortium agreement to be signed at the beginning of the project. These principles align with the recommendations for Intellectual Property Rights in Horizon Europe. The consortium agreement will clearly identify the background and foreground (results) and specify access rights, where applicable.

- **Ownership**: each participant will retain ownership of the foreground they generate.

- **Joint ownership**: in cases where the foreground is jointly generated, participants will reach an agreement based on defined rules outlined in the consortium agreement.

- **Protection, use, and dissemination**: results with potential industrial or commercial applications will be protected, taking into account legitimate interests. Prior notice of dissemination will be given to other participants. Any dissemination of results must acknowledge the financial assistance provided by the Community.

- **Access rights**: partners have the flexibility to define the background they require and may exclude specific background, not necessarily prior to signing the grant agreement. Exclusive licenses to background and foreground may be granted if other partners waive their access rights, depending on previous agreements. Partners may agree to additional or more favourable access rights than those

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement **No. 10196508**

stated in the consortium agreement. Initially, the partners agreed on open access publishing, but they may consider gold or green access to peer-reviewed scientific publications in the future.

- **Management of knowledge in COMMUNITAS**: a knowledge management process will be implemented to facilitate the consolidation of the knowledge spiral, promote cooperation, and enable the creation of new knowledge. The process involves gathering and shaping information, indexing for proper dissemination, and an appropriation period for the generation of new knowledge. Tools will be developed to support social interactions, knowledge processing (organizing files through semantic links for easier searches), and intelligent distribution of knowledge (utilizing push and pull actions to optimize distribution).

- **Personal data**: to ensure anonymity, all personal data within the project will be anonymized, eliminating individual identifiers. Consumption data, which can reveal a consumer's characteristics, will be blurred to prevent its use as an identifier.

- **Right to be forgotten**: participants have the right to request the deletion of their collected data. With a formal request, the capability to delete the requested data within the period specified by the data subject will be ensured.

- **Time of storage**: research data, classified as such, will be stored for a minimum of 5 years after the project's completion. Any storage beyond this period will be evaluated and documented based on necessity and applicability.

- **Data security**: ensuring secure data management is of utmost importance. In addition to data anonymization, measures such as data encryption and distributed backup will be implemented. These measures aim to maintain data consistency throughout the project's lifespan and provide alternative options in case of file loss or corruption. Data encryption adds an extra layer of security to protect the integrity of data files and information.

4.3.1. Ethics in Social Sciences and Humanities (SSH) guidelines

COMMUNITAS has an important Social Sciences and Humanities (SSH) dimension integrated across the project. Ethical guidelines in SSH are particularly relevant in the context of the WP4 as citizen and user engagement will take place in all pilots. According to the Guidelines on Ethics in Social Science and Humanities, the primary goal of adopting ethical guidelines in research activities is to build and sustain trust in science and innovation. It encourages researchers and innovators to employ the ethics by design approach to develop knowledge, technology, and applications that improve people's lives, prospects, and possibilities. Ethics should not be perceived as mere 'red tape' for research, but rather as an empowering framework that enables researchers to make morally sound decisions for our society, based on our values and fundamental rights such as human dignity, privacy protection, and security. In line with the Guidelines for Ethics in SSH, COMMUNITAS will provide a justification for the necessity of human participation in the planned work and specify the form it will take. When citizens and users are invited to participate in COMMUNITAS, it will be done transparently, following ethical principles and data protection measures outlined in the guidelines, as well as ensuring compliance with GDPR and local/national guidelines, regulations, and codes of conduct at the pilot sites.

Any person invited to participate in COMMUNITAS activities must be provided with a transparent invitation and have a fair chance to assess the value of their participation and information sharing. They should also be informed about how their shared information will be utilized. Typically, this is

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement **No. 10196508**

ensured through participants giving their informed consent as part of the negotiation process with the research team, thereby safeguarding their rights and interests.

Most social science research endeavours within COMMUNITAS necessitate evidence of voluntary, free, and informed consent from individuals who contribute their time, insights, effort, and data to researchers. Informed consent is the default option, however, obtaining informed consent alone does not guarantee ethical research practices. In certain research settings, the act of seeking consent and aiming to protect participants' rights and well-being within the research context may inadvertently expose them to potential harm in their social environment.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement **No. 10196508**

5. Ethics Management

The COMMUNITAS requires to demonstrate solutions on the field and to collect data to develop and validate the solutions developed. The ethics management specifies the practices that will be adopted throughout the project to ensure that the project follows a strict ethics guideline, including topics such as privacy and confidentiality, consent, research ethics, and actions that promote fairness and eliminate biased decisions in the decision-making process.

5.1. Privacy and confidentiality

Protecting the privacy and confidentiality of any stakeholder of the project is a top priority for COMMUNITAS. For every different stakeholder participating in the project, measures will be implemented to prevent any personal data from being released or shared inadvertently. To achieve this, the project will follow all legal requirements applicable at European and national levels, namely the GDPR, as guidelines to ensure the privacy and confidentiality of the data.

A set of comprehensive measures will be put in place to ensure the privacy and confidentiality of all stakeholders involved in the project. Some of these key measures include:

- Anonymization and de-identification techniques – To protect the privacy of stakeholders, all data will be anonymized after it has been collected. This implies that the raw data is deleted and that only fundamental data is kept non-anonymously, although the access to this will be highly restricted.
- Informed consent – Informed consent will shall be obtained in every project activity requiring the collection of data. All participants shall be informed in accordance to the GDPR standards and be able to take informed decisions.
- Data storage and access – Any personal data collected from stakeholders will be safely storage, with restrict access to certain members of the consortium that require to use the data for the purpose of their research. The access to this data will be managed by COMMUNITAS Ethics Manager.
- Data retention, sharing, and elimination – Following the GDPR guidelines, the principle of data minimization will be applied so that only fundamental information is retained and shared in the consortium. The remaining data shall be deleted as soon as possible. All the data retained will be so until the end of the project so that the consortium can validate any results achieved to the European Commission.
- Monitoring and compliance – The assigned Ethics Manager will oversee compliance with GDPR and other fundamental practices to maintain privacy. The Ethics Manager will also be the contact for stakeholders that want clarifications or want to exercise any right pertaining to the use of their data.

Due to the importance of the anonymization techniques and the informed consent, these two topics will be explored in detail in the next section.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement **No. 10196508**

5.2. Anonymization and De-identification Techniques

The anonymization of data will be implemented in COMMUNITAS so that any risk of identification of a stakeholder is minimized. The responsible partner for collecting the information and consent, is also the responsible party for anonymizing or de-identifying the data before it is shared with other partners of the consortium.

Two main techniques will be used, the anonymization and the pseudonymization. The anonymization will be the typical technique to be used. It consists of identifying any data that could identify the stakeholder providing it and removing it. One example could be the address or name of a member of an energy community. By removing the personal data, other data such as energy consumption can be used for research, guaranteed there is no method of identification of the stakeholder through it.

The pseudonymization consist of, again, identifying any data that could identify the stakeholder, but instead of deleting this data, the data is replaced with a unique identifier and transferred to a separate document. This method might be used in situation where it might be necessary to identify a stakeholder to validate a specific result of the project. The new file that is created will have the link between the unique identifiers and the personal data, so that it is possible to do a re-identification. This file will be stored in a separate and secure folder with restricted access and managed by the Ethics Manager.

5.3. Informed consent

COMMUNITAS has a large focus on SSH that require the planning of many activities during the project period involving citizens. Activities such as the organization of workshops, surveys, the participatory laboratories, the replication academy, the social acceptance campaigns, are all examples of activities that involve citizens and that require special attention from an ethical point of view due to the necessity of usage of data provided by the citizens during these events. To use an ethical approach to develop these activities, the entity organizing the activity is responsible for obtaining informed consent.

The informed consent ensures transparency with the participants and ensures that it is clear for them that the information they are providing will be used for the benefit of the project. This enables the citizens to take individual and informed decisions on whether to share personal data.

As the standard procedure, informed consent will be provided to the participants in written form. The form provided must indicate the following information:

- Purposed and objectives of the project,
- Indicate that the participation is voluntary and that participants are able to withdraw their consent at any time during or after the activity,
- Explain the benefits or risks that may be associated with the participation in the activity, as well as the time and effort necessary for it,
- Disclose who is funding the research and who will benefit from it,
- If possible, indicate that all information will be collected anonymously,

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement **No. 10196508**

- Indicate that any personal data collected will be promptly treated, deleted, and anonymously stored for research purposes,
- Affirm that personal data will only be accessible by the responsible party for the activity and will be treated securely and confidentiality,
- Detail information of who will have access to any information collected, for how much time, when it will be deleted, and for non-personal information, where it will be stored and where it will be published,
- Detail information on where the participants may find the research results,
- Share a contact for additional questions and to withdraw any consent previously assumed.

Other information will be provided on details and rights associated to the GDPR and additional information may be provided if deemed useful for the participants. A standard document for this purpose will be created for COMMUNITAS partners so that it can be used for described activities.

In some cases, the informed consent can be provided orally, but the written option should always be preferred. In the case of written records, these should be stored in the private folder of the project until the last month of the project.

While informed consent is a crucial element in ethical data handling, it alone does not guarantee the existence of an ethical approach. Other methods will be put in place by the consortium to ensure an ethical approach in data handling.

5.4. Research ethics approval

COMMUNITAS project was reviewed by experts representing the European Commission and got cleared from ethics review. An ethics self-assessment was also performed by the consortium and the result was that data management was analysed as being the most critical ethical principal that needs to be covered during the project. Other points identified include the exploitation of results and access to background information. All three points identified will be extensively covered during the project to ensure an ethical approach. While this deliverable covers all the information on data management, deliverable 6.4 (Final Project IP strategy and exploitation plan of the most promising KERs) will cover the information regarding exploitation of results and intellectual property. The deliberations on the use of background information were proposed and signed by all partners in the Consortium Agreement.

5.5. Bias and fairness

To ensure an ethical research approach, the consortium will be promoting practices that improve the fairness of research and eliminate any bias that leads to preference or exclusion of certain groups based on their gender, race, age, or socioeconomic status.

All researchers working in the project will be selected by their own entities based on their own criteria, but all partners should aim to attain a gender balanced and diverse workforce. In new recruitment processes, it is paramount that the entities consider the use of fair principles and implement practices that promote the elimination of unconscious bias.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement **No. 10196508**

In alignment with the European Commission strategy, all partners should have, or should prepare Gender Equality Plans for their organization that should, between other topics, recommend practices for an ethical selection process. It is encouraged that all partner entities do an individual exercise of identifying bias in their selection processes and deploy active measures that can mitigate those.

Fairness and equity principles must be upheld throughout the project to enable inclusivity, equal opportunity, and respect. Promoting these principles promotes collaboration, innovation, and increases the potential to make an impact in society. The elimination of bias in selection processes and having an inclusive recruitment are some of the some of the fairness and equity considerations that should be considered by the partners. Other considerations include:

- Gender balance – COMMUNITAS will strive for gender balance and equal opportunities by encouraging the participation of women as both researchers and management positions, such as Task leaders, WP leaders, or similar.
- Accessibility – COMMUNITAS will implement, within possible, measures to ensure that all documentation and resources developed are accessible to any individual. This includes use of less technical language, use of adequate colour schemes, and the production of written resources in multiple languages and some video resources.
- Ethical data handling – COMMUNITAS will promote informed consent and will adhere to all GDPR requirements to ensure an ethical data handling.
- Equal recognition – COMMUNITAS will highlight and reference the results produced by any researcher of the consortium, independently of factors such as gender, affiliation, or seniority.
- Collaborative decision-making – COMMUNITAS will promote decision-making forums through its general assemblies that will provide an inclusive and participatory environment where every participant will have the chance to express their opinion and engage in open dialogue.
- Capacity building – COMMUNITAS will promote a collaborative environment between partners and promote sessions for experience sharing and knowledge sharing, that will provide insights that could benefit other researchers.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement **No. 10196508**

6. Data and Ethics Governance

6.1. Data and ethics committee

The Data and ethics committee is a structure organized within COMMUNITAS that will focus on the implementation of the DEMP. This committee is crucial to ensure that the plans detailed in this deliverable are actually put in practice and to ensure there is someone overseeing the ethics of activities developed along the project.

Committee composition

The data and ethics committee for COMMUNITAS project will be chaired by the Ethics Manager, which is the main responsible for overseeing the application of the practices that contribute towards the protection of data and confidentiality of stakeholders. Besides overseeing the process, the Ethics Manager is responsible for sharing information and train other partners on the correct procedures to adopt for the implementation of the DEMP.

All partners that lead activities that require data collection, such as events, surveys, monitoring activities, and others, will automatically be part of the data and ethics committee as they are responsible to follow all the procedures identified in this deliverable. The Ethics Manager can support this on a supervisory and guiding capacity.

All partners that need to access data for the development of solutions or reports may also join the data and ethics committee as an observer, which may take part in the decision-making process for the implemented practices. These partners may also be requested to join the committee in cases of breach or if significant risks arise that could jeopardise the privacy and confidentiality of the data.

Roles and responsibilities

The data and ethics committee as the role to implement and oversee the data handling techniques and ethical principals that will ensure that COMMUNITAS adheres to all essential practices that guarantee privacy and protection of stakeholders and the data collected.

The Ethics manager is responsible for reviewing and approving processes, which are analysed if are in accordance with GDPR guidelines and ethical principles. The Ethics Manager should also do an ethical risk assessment to identify potential risks that could compromise the privacy and confidentiality of stakeholders. Those risks and general practices implemented should be continuously monitored by the Ethics Manager to maintain the consistency along the project. The Ethics manager is also the responsible party for managing the consents from stakeholders and for managing access to any personal or the re-identification component of pseudonymized data.

The responsible parties for the data collected have three major roles and responsibilities that need to be considered when collecting the data and engaging stakeholders. First, ensuring data privacy is responsibility of these parties, they should adopt the methods implemented in the project to ensure that all the data they are collecting is kept confidential. The second responsibility is obtaining informed consent, as addressed on chapter 5.3. Finally, these parties should make the bridge between the stakeholders addressed and the consortium, being responsible for transmitting the perspectives of those stakeholders and ensure that their interests and concerns are addressed by the consortium.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement **No. 10196508**

The parties using the data also have the responsibility of keeping the data confidential and strictly apply any indicated norms, or in cases where no directions are provided, these partners should strictly follow all procedures indicated in the GDPR.

6.2. Data and ethics monitoring

Keeping data privacy requires all partners to work in unison as in some instances it is difficult to control all aspects that guarantee data privacy. Due to this, each partner that has access to the data may be held accountable for breaches, even if they are not part of the data and ethics committee. The committee may not be held accountable for any breaches or other issues that are caused by a specific party due to not following the practices indicated or the GDPR guidelines.

To keep this risk to a minimum, the Ethics Manager will regularly oversee who has access to the data, and revoke access if this is not required anymore. The Ethics Manager will also engage in dialogue with the partners using the data to understand what it is being used for and to ensure that they are respecting the guidelines provided.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement **No. 10196508**

7. References

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- FAIR principles, available at: https://www.go-fair.org/fair-principles/
- H2020 POCITYF D11.8 – Data Management Plan, available at https://pocityf.eu/resources/
- H2020 Smart2B D9.4 – Data Management and System Failure Management Plan, available at https://smart2b-project.eu/results/public-deliverables/

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement **No. 10196508**

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement **No. 10196508**