

**MASTERPIECE -
Multidisciplinary Approaches and Software
Technologies for Engagement, Recruitment and
Participation in Innovative Energy Communities in
Europe**

Deliverable 1.2

MULTI-ASPECT TECHNICAL, QUALITY, ETHICS AND DATA MANAGEMENT PLAN

| | |
|-----------------------------|--|
| Title | Multi-Aspect Technical, Quality, Ethics and Data Management Plan |
| Document description | It specifies the technological and scientific processes to be followed in the project development; defines the procedures and mechanisms to manage quality assurance as well as anticipate, prevent, and mitigate possible risks; describes the processes for ethics/data management to ensure the compliancy with the EU data protection regulations. |
| Nature | Type and dissemination level: DMP - SEN |
| Task | T1.2, T1.3, T1.4 |
| Status | On Progress |
| WP | WP1 |
| Lead Partner | CERTH |
| Partners Involved | CERTH, UMU, ALWA |
| Date | |

| Revision history | Author | Delivery date | Summary of changes and comments |
|-------------------------|---|----------------------|--|
| Version 01 | Iakovos Michailidis | 15/05/2023 | Initial ToC |
| Version 02 | Charalampos Lazaridis, Thanasis Moustakas | 08/06/2023 | Chapters 1, 2 and 3 |
| Version 03 | Stefano Bianchi | 15/06/2023 | Chapter 4 |
| Version 04 | Alfonso Ramallo | 22/06/2023 | Review |
| Version 05 | Stefano Bianchi | 23/06/2023 | Review |
| Version 06 | Charalampos Lazaridis, Thanasis Moustakas | 27/06/2023 | Minor changes according to reviews |

Disclaimer:

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Swiss Confederation. Neither the European Union nor the granting authority can be held responsible for them.

Contents

| | |
|--|-----------|
| 1 INTRODUCTION | 6 |
| 1.1 OBJECTIVES AND SCOPE | 6 |
| 1.2 RELATION TO OTHER ACTIVITIES | 6 |
| 1.3 SUMMARY AND STRUCTURE OF THE DELIVERABLE | 6 |
| 2 TECHNICAL MANAGEMENT PLAN | 8 |
| 3 QUALITY ASSURANCE AND RISK MANAGEMENT | 9 |
| 3.1 QUALITY ASSURANCE | 9 |
| 3.2 RISK MANAGEMENT | 10 |
| 4 DATA MANAGEMENT PLAN | 15 |
| 4.1 OBJECTIVES | 15 |
| 4.2 PRINCIPLES | 15 |
| 4.2.1 INFORMATION SHARING PRINCIPLES | 15 |
| 4.2.2 PSEUDO-ANONYMIZATION APPROACH | 16 |
| 4.3 PROCEDURES | 16 |
| 4.3.1 DATASET RECORD | 17 |
| 4.3.2 DATA PROTECTION OFFICER (DPO) | 19 |
| 4.4 DATA SUMMARY | 20 |
| 4.5 FAIR DATA | 22 |
| 4.5.1 MAKING DATA FINDABLE | 23 |
| 4.5.2 MAKING DATA OPENLY ACCESSIBLE | 24 |
| 4.5.3 MAKING DATA INTEROPERABLE | 26 |
| 4.2.4 MAKING DATA REUSABLE | 26 |
| 4.6 ALLOCATION OF RESOURCES | 28 |
| 4.7 DATA SECURITY | 29 |
| 4.8 ETHICAL ASPECTS | 30 |
| 4.9 OTHER ISSUES | 35 |
| 5 REFERENCES | 37 |

TABLES

Table 1. MASTERPIECE risks and proposed mitigating measures.....11

1 INTRODUCTION

1.1 Objectives and scope

The aim of this deliverable is to define all the processes that will assure the quality of the delivered results from MASTERPIECE. Precautious actions are planned to promptly recognize and effectively handle any possible threats that are related to the progress of the project. A series of operations are also prepared to make sure that project outcomes achieve excellence, competing with the state-of-the-art implementations of the market.

1.2 Relation to other activities

Deliverable 1.2 has a cross-cutting relation to activities throughout MASTERPIECE, reporting on the coordination and monitoring of technical aspects of the whole project while providing feedback towards novel solutions and ideas. Therefore, the involved partners are expected to provide feedback about the potential risks and to report on the technical development of the technological solutions / innovations / products.

1.3 Summary and structure of the deliverable

Chapter 1 - Introduction

Introduction of the deliverable, presenting the scope and objectives, the structure of the document and the interdependencies with other tasks.

Chapter 2 – Technical Management Plan

The Technical Management ensures that novel implementations are delivered, competing with existing innovative solutions in the respective fields. The relevant activities that will be undertaken as part of the Technical Management strategy are defined and the roles that will coordinate these activities/processes are set.

Chapter 3 – Quality Assurance Plan and Risk Management

The Quality Assurance Plan describes the general quality control measures and actions, and it defines more specific standards for deliverables, documentation, dissemination actions and issues handling between partners. The Risk Management Plan outlines possible weaknesses and vulnerabilities of the project, analysing their impact and defining corrective actions to mitigate them. The techniques that are applied to monitor those events are aiming towards positively affecting the project outcome. However, risk management is a dynamic process that is constantly updated by all partners during the project.

Chapter 4 – Data Management Plan

Data Management establishes the framework under which the MASTERPIECE consortium will monitor/generate, will process and will collect data during project's demonstration activities and citizen engagement actions. It tackles how the data will be used, exploited and made accessible for verification and re-use as well and how the data will be curated and preserved after the project completion.

2 TECHNICAL MANAGEMENT PLAN

Technical Management is focused on the successful design, development and deployment of the technical aspects of the project that should result into achieving its objectives. A well-defined strategy is necessary to meet the project technical requirements, overcome challenges and make sure that the solutions developed within the context of MASTERPIECE project are able to address specific stakeholders' needs.

The goal of the Technical Management is to provide detailed descriptions of the overall MASTERPIECE framework and the specifications for each of its key components, modules and their functionalities.

The MASTERPIECE Technical Management Strategy will be thus based on the following activities in order to ensure that successful project results are delivered:

- Monitoring of the technical progress considering at what extent the technical targets are met
- Monitoring of the innovation progress of the proposed solution in terms of Technology Readiness Level (TRL) and assessment of the novelty of the developed components of each solution
- Participation in various dissemination activities such as conferences, workshops or market exhibitions. The aim is to communicate the project results to a targeted audience, receive feedback and at the same time follow the latest technological advancements on the field, and get informed about the market needs
- Participation in events and initiatives in order to encourage collaboration and networking among the relevant stakeholders of the field, facilitating knowledge transfer and following regulatory and policy guidance
- Collaboration with other research projects targeted towards the deployment and operation of smart residential buildings. Encouraging knowledge transfer for the development of specific components and communicating results in order to maximize impact
- Communication with end-users receiving feedback for the solutions developed, making corrective actions so that the end product is user-friendly and it receives high level of acceptance

Technical Management activities are coordinated and supervised by the Scientific & Technical Manager (STM), Iakovos Michailidis (CERTH). The STM will have the responsibility to drive and coordinate all scientific decisions, addressing and solving any technical issues that might arise, as well as ensure that the MASTERPIECE technical objectives are met with high-quality and in time. He will be responsible for the management of the technical integration and interoperability activities,

including technology components, services, platforms, AI resources and datasets, both intra-MASTERPIECE and third-party.

3 QUALITY ASSURANCE AND RISK MANAGEMENT

3.1 Quality Assurance

In order to make sure that the project deliverables match the established quality requirements, quality assurance is a proactive strategy. The project consortium may greatly improve the overall quality of the project outputs by establishing solid processes, managing requirements, doing reviews and audits, implementing efficient testing, managing non-conformities, and promoting a culture of continuous improvement and competence. Effective quality assurance procedures boost stakeholders' confidence, reduce risks, and support the project's success. Through the course of the project lifecycle, it comprises taking a methodical and proactive approach to defect prevention, non-conformity detection, and quality enhancement. More specific instructions about roles, review procedures and deliverables naming and conventions are described in Deliverable 1.1. The main elements of quality assurance for the project are described in the list that follows.

1. Processes and Methods

Setting up reliable procedures to control project operations is the first step in quality assurance. To ensure consistency and adherence to best practices, these processes specify the steps, rules, and regulations to be followed during the project execution. A framework for quality assurance efforts by including legislative requirements, project-specific standards, and corporate quality policies is provided

2. Requirements Management

Understanding and controlling the project requirements is the second step in quality assurance. To make sure the requirements are comprehensive, accurate, and traceable, they must be thoroughly documented, reviewed, and validated. Potential quality problems brought on by misunderstandings or ambiguities can be reduced by handling requirements efficiently.

3. Quality Planning and Documentation

A thorough quality management plan directs quality assurance efforts. The strategies, tactics, and materials needed to reach the specified level of quality are described in this plan. It offers a roadmap for quality assurance throughout the project and it outlines the quality objectives, metrics, and acceptance criteria. To maintain uniformity and standardization, quality-related documentation such as quality checklists, templates, and forms are also created.

4. Quality Reviews and Audits

In order to determine if project activities and deliverables adhere to set quality standards, regular reviews and audits are carried out. Project Manager reviews, walkthroughs, and inspections are a few examples of these reviews, where project artifacts are methodically

checked for mistakes, omissions, and compliance with requirements. Internal and external audits are carried out to assess the general efficacy of the quality management processes.

5. Test Planning and Execution

A crucial part of quality assurance is testing, which makes sure that the project deliverables comply with the requirements and work as planned. The process of test planning entails creating an all-encompassing test strategy, test plans, and test cases. Executing tests entails performing them, recording and analyzing test findings, and resolving any flaws or problems found.

6. Non-Conformance Management

A strong non-conformance management strategy is crucial when deviations from established quality standards or non-conformities are found. This procedure covers recording, monitoring, and resolving non-conformities as well as putting remedial and preventative measures into practice. It makes sure that concerns are quickly resolved and that lessons learnt are used to stop them from happening again.

7. Competence and training

Ensuring that project consortium has the abilities, knowledge, and competence to perform their roles successfully supports quality assurance. Their understanding of quality assurance principles, methodologies, tools, and techniques will be improved through familiarization with the relative documents. The consortium will be up to date with the most recent industry practices and quality standards thanks to ongoing professional development.

3.2 Risk Management

Effective risk management is a key element of a project's effective execution. Project managers can limit the negative impact on project objectives and could increase the possibility of attaining desired outcomes by proactively recognizing, assessing, and resolving potential risks. By putting in place a strong risk management framework, the consortium is better equipped to reduce risks' negative effects, take advantage of opportunities, and raise the likelihood that the project will be successful overall. A number of crucial procedures that are incorporated into the entire project management framework make up the risk management process are presented below:

1. Risk Identification

The first stage in risk management is to meticulously identify every risk that might have an impact on the project. To create a thorough list of hazards, this calls for involving stakeholders, the consortium, and subject matter experts. Finding internal and external risks can be accomplished using a variety of strategies, including brainstorming, documentation review, and expert interviews. Risks should be taken into account across a range of categories, such as technological, organizational, environmental, and financial ones.

2. Risk assessment

After risks are identified, they must be evaluated in terms of their probability and impact on the project's goals. Prioritizing risks and allocating the right resources for any risk contingency are both aided by this step. For risk assessment, both qualitative and quantitative analysis methods can be used. The probability and impact of each risk are given subjective values, such as low, medium, or high, through qualitative analysis. To better accurately identify risks, quantitative analysis uses numerical values and statistical techniques. The method that will be used in this project is Expanded Failure Modes and Effects Analysis (EFMEA). By employing this approach, valuable insights are obtained regarding the crucial components of the entire system. It enables the assessment of appropriate measures and mitigation tactics, all aimed at supporting the project's contingency plans.

- EFMEA (Z.Bluvband, 2004) is a process that provides information to identify key system components, assess appropriate responses, and develop mitigation techniques, with the main objective of assisting in the project's contingency preparations. Risk analysis is carried out in EFMEA in two stages: Identification of Risks and Risk Reduction. EFMEA classifies risks into four main categories:
 - Technical (physical features of hardware, coding elements of software)
 - Legal (based upon existing policies and laws in each nation)
 - Behavioural (resulting from user's behaviour)
 - Organisational (in relation to disaster mitigation plans and actor's roles).

3. Risk Response Planning

The consortium creates risk response plans based on the hazards that have been evaluated. These tactics either pass the risk to outside parties or attempt to alleviate it. Contingency plans can be created, project processes can be improved, safety measures can be put in place, and more resources can be acquired as contingency measures. Planning for risk response also takes into account risk acceptance when the impact is minimal or when the expense of mitigation outweighs the potential repercussions.

4. Risk Monitoring and Control

Throughout the course of a project, risk management is a continuous process. Risks must be closely monitored, their status must be tracked, and they must be reevaluated as necessary. The timely detection of any changes in the risk landscape is made possible by routine project progress reviews and risk status updates. It is important to take the proper steps to address hazards as they arise and change. The consortium can quickly react to reduce or take advantage of new risks and opportunities by maintaining a proactive approach to risk monitoring and control.

5. Risk Communication

Effective and transparent communication is crucial to risk management. To ensure that all stakeholders are aware of the project's risks, project managers should explain the potential effects. Sharing risk information openly enables stakeholders to set realistic expectations and make well-informed decisions. Progress reports and regular risk communication updates help to engage stakeholders and encourage their participation in risk response initiatives.

6. Risk Documentation and Lessons Learned

For knowledge transfer and organizational learning, it is essential to document risks, reaction plans, and results. An accurate historical record of risks encountered and the success of mitigation strategies is maintained by proper documentation. It aids in enhancing risk management procedures and serves as a reference for upcoming initiatives. Additionally, by carrying out a post-project evaluation, the consortium can pinpoint lessons learned and gather crucial insights to improve risk management procedures in subsequent initiatives.

In the following table we present possible risks and categorize them based on their impact and likelihood of happening. We also propose reduction methods and mitigation plans for each distinct risk case.

| Risk description | Risk mitigating measures proposed |
|--|---|
| <p>Development and deployment risks due to the energy community sources data availability (reduced set of historical data)</p> <p>Impact/Probability: High/Medium - WP2-5</p> | <p>Risk Reduction: We will engage with our end users from the project outset quite early during its lifecycle (WP2,WP5). Additionally, our advisory board will be constructed in such a manner as to ensure we have covered all aspects of deploying technology in the project context. Also, we have ensured that the technologies to be deployed at pilot sites have already been tested in similar contexts elsewhere. The availability of data has already been investigated and is intended to be partially addressed through appropriate instrumentation/sensory-equipment measures at the pilot sites. The technical and methodological developments foreseen in MASTERPIECE WP2-WP4 will follow an up-scaling approach starting from the minimum requirements in terms of resources (computations, data, storage, etc.). This approach will allow different granularity levels to be identified along the way. Moreover, through the active engagement of energy community facilitators in WP5 implementation; the consortium will also have access to historical data from other real cases which could be exploited for the project's purposes as well. Finally, the technology providers have long experience in similar innovation topics as well as in the implementation of large and complex systems for demos, thus the occurrence possibilities of such issues during the project are low. Mitigation Plan: Deployment of additional sensors on-site; Up-scaling developments for different resource granularities; Exploit relevant external data sources; Appropriate, alternative technology solutions will be suggested to the providers involved.</p> |
| <p>Incomplete & improper project development due to the size and</p> | <p>Risk Reduction: All MASTERPIECE members have long experience in large research projects as well as in the implementation of large and complex systems, thus the possibilities of such problems compromising the project are low. Management structure</p> |

| | |
|--|--|
| <p>complexity of use-case tests Impact/Probability: High/Medium - WP2-4</p> | <p>with experienced managers for WPs & pilots. Mitigation Plan: Reorganisation and rescheduling of tasks combining the consortium resources.</p> |
| <p>Poor WP internal compatibility and communication leading to delayed / failed objectives. - Impact/Probability: High/ Low - WP1</p> | <p>Risk Reduction: MASTERPIECE will reduce this risk by periodic (monthly, bi-weekly, or weekly basis) WP meetings and audio conferences based on the currently identified situation of their progress. A common architectural view of the project solution will derive early during the project from WP2 so all partners share the same view. Robust communications tools and development tracking processes (keeping history of each meeting's conclusions) will be deployed throughout the project. Moreover, occasional steering committee meetings will also be held to support the cross WP communication and sharing. Mitigation Plan: As is the case with poor partner performance, any serious issue which may cause delays/failure will be identified from the outset. Partners will be asked, and helped, to increase their efforts and communications, failing which they may be appropriately replaced.</p> |
| <p>Platform/Tools developed having insufficient/ unadaptable functionality for user evaluation - Impact/Probability: High/Low - WP2-4</p> | <p>Risk Reduction: Risk is minimised through tight control of WP2-4 management and milestones, also enforced by WP1. Additionally, all selected MASTERPIECE tools will be specified and adapted in Task 5.1 for each demonstrator. Mitigation Plan: Considering different platform tools for each pilot case as well as adopting a double development cycle (refining the initial developments based on the preliminary test observations) allows MASTERPIECE to flexibly readapt the functionalities offered accordingly.</p> |
| <p>Technological risks: a competing solution makes the MASTERPIECE objectives/approaches obsolete and/or an external technology rise during the project is exploitable within MASTERPIECE - Impact/Probability: High Medium - WP1</p> | <p>Risk Reduction: MASTERPIECE will have a technology observatory in Task 1.2 to monitor relevant external digital and methodological tools availability and detect any competitive evolutions early enough to be addressed in the project, so that the proposed approaches and objectives are accordingly adapted and still innovative. The Advisory Board (foreseen to be formed at the beginning of the project) will contribute to identification of new tools and technologies that may have an impact on the project. Mitigation Plan: MASTERPIECE Scientific and Technical Manager (see section 3.3.1) will use focus groups to bring on board MASTERPIECE third parties that will have expertise in new technologies and will exploit these within the project to further promote its targeted results. WP2 will adjust its specifications accordingly in the final release of the technological blueprint. The Plenary and Steering Committees will be the vehicle to communicate and ensure that MASTERPIECE's competitive advantage is sustained.</p> |
| <p>COVID-19 pandemic restrictions cause delays in tasks which require direct contact with involved users, specifically for the needs collection, engagement and demonstration activities - Impact/Probability: Medium / Low - WP2,5,6</p> | <p>Risk Reduction: Ensure efficient communication action plans are planned in WP2, WP5 and WP6 with users and stakeholders even when face to face meetings are not possible. MASTERPIECE will take full advantage of teleconferencing solutions for remote interviews and meetings with stakeholders and end-users. Desk based studies and technical characterization will be accelerated and completed to a high level to make up for possible delays and restrictions in such activities. Mitigation Plan: MASTERPIECE mainly considers an ICT-oriented context which can be easily managed remotely, minimising the difficulties caused by lack of physical meetings. Additionally, the consortium will increase the number of remote developments and integration meetings if and when required.</p> |

| | |
|---|--|
| <p>Integration difficulties due to unforeseen complexity. - Impact/Probability: High / Medium - WP2,5</p> | <p>Risk Reduction: MASTERPIECE has formed a solid safety net which could ensure technical compatibility of different technologies: A clear definition of the integration process and communication to all MASTERPIECE partners in Task 5.1 based on the blueprints defined in Task 2.5; review and consolidation of intervention plans/programs in Task 5.2, 5.3 and 5.4; clear definition and communication of use case objectives through scene selection and technology mapping from Task 2.3; following standardized solutions where available. Mitigation Plan: If complexity is escalating, alternative technologies will be suggested to the WPs. Additionally, the consortium will increase the number of face-to-face and remote development and integration meetings if and when required.</p> |
| <p>Demonstration Risks (2 implementation and demo cycles) for the complexity of the proposed innovations - Impact/Probability: High/ Medium - WP2-5</p> | <p>Risk Reduction: Project timing and agile development process ensures rapid early prototyping to address critical technical/deployment issues as early as possible (WP2, WP3, WP4 and Task 5.1). Moreover, early coherent tests, preliminary evaluation results and MASTERPIECE integration planning will be aligned (WP5) to ensure harmonised delivery of functional MASTERPIECE platform versions. Mitigation Plan: The 2 pilot cycles can be deployed in a staggered manner, rather than in a partially-overlapping manner (see section 3.1.1) - there is enough flexibility in the WP plans to cover this need.</p> |
| <p>Disengagement and low communication of the large number of participants/end-users and stakeholders - Impact/Probability: High/ Medium - WP2, WP5, WP6</p> | <p>Risk Reduction: Segmented communication approach will engage targeted user communities from the start and throughout the whole project up to the evaluation process. Use case leaders, WP leaders and SSH experts will monitor these engagement levels. The users are engaged and mobilised via partners with whom they already have established strong commitment and trust. Mitigation Plan: Alternate end-users will be mobilised from the network of contacts of partners in the pilots and/or local networks; Besides targeted communication, SSH-based engagement mechanisms (from WP2) will be used (demonstrated & evaluated) to activate participants/create active follow-up communities.</p> |
| <p>Potential failure of innovative business models - Impact/Probability: Medium / High - WP2, WP6</p> | <p>Risk Reduction: MASTERPIECE has a good balance of industrial partners with initial exploitation plans in Section 2. Moreover, WP6 will develop detailed business models and sustainability strategies for MASTERPIECE outcomes, capitalising also on open-research principles to attract multi-disciplinary external interest on the project outcomes, when combined with solid dissemination measures. Mitigation Plan: The main measure is to develop faster than competitors and ensure innovations with the appropriately identified - from WP2 activities - requirements and added value for the energy communities' sector.</p> |

Table 1. MASTERPIECE risks and proposed mitigating measures

4 DATA MANAGEMENT PLAN

4.1 Objectives

This Data Management Plan (DMP) describes the data management life cycle for the data to be collected, processed and/or generated by the MASTERPIECE project. To make research data Findable, Accessible, Interoperable and Re-usable (FAIR), the DMP includes information on:

- the handling of research data (during & after the end of the project);
- what data will be collected, processed and/or generated;
- which methodology and standards will be applied;
- whether data will be shared/made open access; and
- how data will be curated and preserved (including after the end of the project).

IMPORTANT: The DMP is meant to be a living document that will undergo further reviews/integrations during the life of the project, to allow proper tracking of all associated activities and results. The version included here thus represents the overall plan, defined according to previous relevant and successful experience, to be followed by all interested parties - modifications to operational procedures might be necessary to mitigate issues/criticalities or simply to maximize results. As for Grant Agreement clauses, on the basis of the accumulated updates/integrations/reviews, the formal update of the DMP is expected at M30.

4.2 Principles

4.2.1 Information sharing principles

In the scope of the MASTERPIECE project, effective sharing of information between involved actors/stakeholders - i.e., Energy Communities (ECs) members/managers, aggregators, renewables plants owners, market operator - is essential for the correct functioning of most of the services to be provided and validated.

This DMP generally considers the key principles of information sharing reported below, adopted for the needs of the energy domain. Seven key principles (information/data features) are identified, of which six describe properties that shared information should have (i.e., necessary, proportionate, relevant, accurate, timely and secure) while the last describes a function that agent that share data should support (i.e., trackable).

Necessary and proportionate: When taking decisions about what information to share, you should consider how much information you need to release. Not sharing more data than necessary to be of use, is a key element of the GDPR and Data Protection Act 2018. Information must be proportionate to the need and level of risk.

Relevant: Only information that is relevant to the purposes should be shared with those who need it. This allows others to do their job effectively and make informed decisions.

Adequate: Information should be adequate for its purpose. Information should be of the right quality to ensure that it can be understood and relied upon.

Accurate: Information should be accurate and up to date and should clearly distinguish between fact (i.e., measures or money transaction) and opinion (i.e., forecasting). If the information is historical then this should be explained.

Timely: Information should be shared in a timely fashion to reduce the risk of missed opportunities to offer support from AI, forecasting engine and digital twin. The aggregation tools should ensure that sufficient information is shared, as well as consider the urgency with which to share it.

Secure: Wherever possible, information should be shared in an appropriate and secure way. Any aggregation tool must follow their policy on security for handling personal information of their users.

Trackable: Information sharing decisions should be recorded, whether or not the decision is taken to share. If the decision is to share, reasons should be cited including what information has been shared and with whom, in line with policy procedures. If the decision is not to share, it is good practice to record the reasons for this decision and discuss them with the requester. In line with each organisation's own retention policy, the information should not be kept any longer than is necessary. In some rare circumstances, this may be indefinitely, but if this is the case, there should be a review process scheduled at regular intervals to ensure data is not retained where unnecessary.

4.2.2 Pseudo-anonymization approach

Pseudo-anonymization of personal data (as defined in Article 4(5) GDPR) means replacing any information which could be used to identify a data subject with a pseudonym (e.g., an alphanumeric identifier) which does not allow the individual to be directly identified.

Data can be instead considered anonymised when individuals are no longer identifiable: in this case, the original information should be securely deleted to prevent any reversing of the anonymization process. In most cases, if this deletion does not occur, then the data is classified as pseudo-anonymised rather than anonymized and is still considered personal data.

In the scope of the MASTERPIECE project and in accordance to the definitions above, whenever possible, all collected personal data will be at least fully pseudo-anonymized before being provided to project data processors for elaboration (total anonymization will be considered only if not affecting the provision of the services and the significance of the project results and findings).

4.3 Procedures

The implementation of the DMP will primarily consist of the following steps, provisionally defined at the beginning of the project considering previous successful experiences:

1. Creation of a **Dataset Repository**. Unless there would be a possible conflict with confidentiality, security or commercial sensitivity or GDPR, all data needed to validate the results as presented in any of the publications will be made available through an open

research data repository linked with the MASTERPIECE website as soon as possible. The URL for the website is [HTTPS://MASTERPIECE-HORIZON.EU/](https://masterpiece-horizon.eu/) whereas the URL to access linking to the data sets will be available in the Resources section. The open research data repository to be used will likely be Zenodo ([HTTPS://ZENODO.ORG/](https://zenodo.org/)) considering the adoption of the ARGOS suite.

2. Each partner should fill a **Dataset Record** for each of the major datasets created. A dataset is defined as any collection of research data that is particular or special from the data management perspective. This means that data about different topics might be grouped in a dataset if no particular aspect makes its management different (e.g., confidentiality, security, intellectual property). The template of the Dataset Record is provided below.
3. Once the Dataset Record is filled, each partner should store it in the Project Dataset Repository alongside the actual dataset, with the support of the DPO. Functionalities natively exposed by adopted tools (e.g., ARGOS) will be used to formalize the provided information and attach it univocally to the provided dataset.
4. Some datasets might have specific data management policies or procedures (e.g., experiments/piloting). Accordingly, each partner should define/formalize/upload the associated policies and procedures too.
5. On a regular basis (at least every 3 months), the DPO will review these records to internally update the DMP accordingly and to ask for additional feedback to the involved partners/beneficiaries. At a minimum, the DMP would be reviewed and - if necessary - updated in the context of the project plenary meetings.

4.3.1 Dataset record

| Data Summary | |
|---------------------------|--|
| Name of dataset | <i>A short and descriptive name for the dataset</i> |
| Work Package(s) | <i>Work packages for which the dataset is created</i> |
| Task(s) | <i>Tasks for which the dataset is created (if can be detailed)</i> |
| Nature of the data | <i>Data collection / Data generation</i> |
| Purpose of the data | <i>What is the purpose of the dataset?</i> |
| Relation to the project | <i>What is the relation of the dataset to the objectives of the project?</i> |
| Type of data | <i>What type of data contains the dataset?</i> |
| Data format | <i>What is the format of the dataset?</i> |
| Reuse in project | <i>Will be the dataset reused in other parts of the project?</i> |
| Reuse outside the project | <i>Will be the dataset reused outside the project?</i> |
| Origin of the data | <i>What is the origin of the data?</i> |
| Expected size of dataset | <i>What is the expected size of the data in observations/instances? And in storage size (Mb, few Gb, dozens of GB, ...)?</i> |
| Data utility | <i>To whom might it be useful?</i> |
| Making data findable | |
| Discoverability | <i>Are the data discoverable with metadata?</i> |
| Identifiability | <i>Are the data identifiable and locatable using a standard identification mechanism (e.g. persistent and unique identifiers such as DOI)?</i> |

| | |
|----------------------------------|---|
| Naming | <i>Does the data follow naming conventions? What conventions do you follow?</i> |
| Keywords | <i>Will search keywords be provided that optimise possibilities for re-use?</i> |
| Versions | <i>Do you provide clear version numbers?</i> |
| Metadata | <i>What metadata will be created? In case metadata standards do not exist in your discipline, please outline what type of metadata will be created and how.</i> |
| Making data accessible | |
| Availability | <i>Will the dataset be made openly available as the default? If certain datasets cannot be shared (or need to be shared under restrictions), explain why clearly separating legal and contractual reasons from voluntary restrictions. Note that in multi-beneficiary projects it is also possible for specific beneficiaries to keep their data closed if relevant provisions are made in the consortium agreement and are in line with the reasons for opting out.</i> |
| Accessibility | <i>How will the dataset be made accessible (e.g. by deposition in a repository)?</i> |
| Repository | <i>Where will the data and associated metadata, documentation and code be deposited? Preference should be given to certified repositories which support open access where possible. Have you explored appropriate arrangements with the identified repository?</i> |
| Access support | <i>What methods or software tools are needed to access the data? Is documentation about the software needed to access the data included? Is it possible to include the relevant software (e.g. in open source code)?</i> |
| Access policy | <i>How will access be provided in case there are any restrictions? If there are restrictions on use, how will access be provided? Is there a need for a data access committee? Are there well-described conditions for access (i.e. a machine-readable license)? How will the identity of the person accessing the data be ascertained?</i> |
| Making data interoperable | |
| Interoperability | <i>Are the data produced in the project interoperable, that is allowing data exchange and re-use between researchers, institutions, organisations, countries, etc. (i.e. adhering to standards for formats, as much as possible compliant with available (open) software applications, and in particular facilitating re-combinations with different datasets from different origins)? What data and metadata vocabularies, standards or methodologies will you follow to make your data interoperable?</i> |
| Standardisation | <i>Will you be using standard vocabularies for all data types present in your data set, to allow interdisciplinary interoperability? In case it is unavoidable that you use uncommon or generate project specific ontologies or vocabularies, will you provide mappings to more commonly used ontologies?</i> |
| Making data reusable | |
| License | <i>How will the data be licensed to permit the widest re-use possible?</i> |
| Timing | <i>When will the data be made available for re-use? If an embargo is sought to give time to publish or seek patents, specify why and how long this will apply, bearing in mind that research data should be made available as soon as possible.</i> |
| Third-parties | <i>Are the data produced and used in the project usable by third parties, in particular after the end of the project? If the re-use of some data is restricted, explain why.</i> |
| Length of time | <i>How long is it intended that the data remains re-usable?</i> |
| Quality | <i>Are data quality assurance processes described?</i> |
| Allocation of resources | |
| Costs | <i>What are the costs for making data FAIR in your project? How will these be covered? Note that costs related to open access to research data are eligible as part of the Horizon 2020 grant (if compliant with the Grant Agreement conditions).</i> |
| Responsible(s) | <i>Who will be responsible for data management in your project?</i> |
| Long-term preservation | <i>Are the resources for long-term preservation discussed (costs and potential value, who decides and how what data will be kept and for how long)?</i> |
| Data security | |
| Provisions | <i>What provisions are in place for data security (including data recovery as well as secure storage and transfer of sensitive data)?</i> |
| Certified repositories | <i>Is the data safely stored in certified repositories for long-term preservation and curation?</i> |
| Ethical aspects | |
| Ethical and legal issues | <i>Are there any ethical or legal issues that can have an impact on data sharing? These can be discussed in the context of the ethics review. If relevant, include references to ethics deliverables and ethics chapter in the Description of the Action.</i> |

| | |
|---|--|
| Informed consent | <i>Is informed consent for data sharing and long-term preservation included in questionnaires dealing with personal data?</i> |
| Other procedures for data management | |
| Other data management procedures | <i>Do you make use of other national/funder/sectorial/departmental procedures for data management? If yes, which ones? Provide that procedure if possible.</i> |

4.3.2 Data Protection Officer (DPO)

The project Data Protection Officer (DPO), Stefano Bianchi, R&I manager in algoWatt SpA (ALWA), is also the company's DPO - as such, in addition to the proactive participation in ISO 9001:2015 and ISO 27001:2013 certifications, he has the following duties, applied as well to the MASTERPIECE project:

- ensure that controllers and data subjects are informed about their data protection rights, obligations and responsibilities and raise awareness about them;
- give advice and recommendations to the institution about the interpretation or application of the data protection rules;
- create a register of processing operations within the institution and notify the EDPS those that present specific risks (so-called prior checks);
- ensure data protection compliance within her institution and help the latter to be accountable in this respect.
- handle queries or complaints on request by the institution, the controller, other person(s), or on her own initiative;
- cooperate with the authorities (responding to requests about investigations, complaint handling, inspections, etc.);
- draw the institution's attention to any failure to comply with the applicable data protection rules.

He is the DPO for other 2 running EC-funded projects in the energy domain:

- **VPP4ISLANDS** [HTTPS://CORDIS.EUROPA.EU/PROJECT/ID/957852](https://cordis.europa.eu/project/id/957852) (Grant agreement ID: 957852)
- **FlexCHESS** [HTTPS://CORDIS.EUROPA.EU/PROJECT/ID/101096946](https://cordis.europa.eu/project/id/101096946) (Grant agreement ID: 101096946)

and he has been the DPO for the recently closed EC-funded project:

- **TRUSTONOMY** [HTTPS://CORDIS.EUROPA.EU/PROJECT/ID/815003](https://cordis.europa.eu/project/id/815003) (Grant agreement ID: 815003)

According to the DOA, the project DPO is referred to as GDPR, Data & Ethics Manager (GDEM), appointed to ensure accuracy, integrity, confidentiality and security of personal data, applying knowledge of regulations (i.e., GDPR, NIS, eIDAS), policies, protocols and procedures to control and maintain accurate records. GDEM will supervise ethical aspects and will be supported by Dr. Julián Valero Torrijos (DPO, UMU) for all aspects associated to privacy and FAIR data management (e.g., findability, accessibility, interoperability and reusability).

4.4 Data Summary

What is the purpose of the data collection/generation and its relation to the objectives of the project?

MASTERPIECE aims at creating a digital coordination and cooperation arena that will facilitate the creation and operation of energy communities throughout Europe. The facilities given to members of the community to contribute to services and other developments will represent the distinction of the solution offered in this proposal, making it participative-by-design. Objectives are:

- i) to develop technical and social innovations to empower traditional energy consumers and to make them active agents of collaborative energy communities, paving the way towards a new energy market paradigm;
- ii) to create user-centric solutions that are based on participatory approaches such as co-creation and naturally accelerate citizens' involvement;
- iii) to propose new business strategies and incentive mechanisms that activate the reactions of market participants craving for business opportunities that imply energy use and cost reduction;
- iv) to configure a standardised and sound cyber-security infrastructure so the active citizens are protected against cyberattacks, while privacy is defended in accordance with the revised EPBD and the GDPR law; and
- v) to demonstrate the applicability and replicability of methodological, technical and business innovations in a variety of real life pilots in different geographical locations, with heterogeneous social and economic environments and different regulatory/administrative frameworks.

To demonstrate and evaluate the proposed innovations, it will leverage 4 pilot cases in different geographical areas and within different operational/policy frameworks (France, Italy, Sweden and Turkey).

Data collection/generation within the scope of the project is therefore focused on supporting the ambition of the MASTERPIECE project in:

- Nudging participation in energy communities through automation
- Boosting self-determinacy in communities' energy management through Artificial Intelligence toolbox
- Facilitating the connectivity of community members to monitor energy flows
- Demand response modification at the community and citizen level
- New conceptualisation of energy business to include philanthropic prosumers against fuel poverty

by feeding the services/ enabling the functionalities provided by the modules included in the overall MASTERPIECE architecture:

- **Community Design Toolkit**
 - Shareholder/members consensus: profile matching to create aggregated balanced energy community profile
 - Regulatory Framework and Limitations

- Models for incentives
- Technical Design and Instrumentation Blueprints: Deployment design and planning, recognizing the necessary instrumentation to implement the targeted community
- **Digital Services for Proactive Assessment, Participation and Decision Support**
 - Techno-Economic (Expected Incentives and Performance) Community Assessment
 - Community Scenario Generation Engine (different kinds of members → different community types allowed → different optimal governance strategy → different profits / incentives rates)
 - Recommended Community Governance Strategy (Decision Support)
 - Toolkits and personalised app to facilitate consumers in discovering and joining existing EC and interact with a community of peers
- **Optimized Operation Toolkit**
 - Dynamic Smart Contracting of Resources: Applied optimized governance and management strategy on aggregated community resources, optimising self-consumption and increasing efficiency (Energy, Flexibility and Data)
 - Automated Monitoring, DR and flexibility services: Interpreting the management strategy into closed-loop adaptive control decisions.
 - Community-centric optimized control schedules, integration of existing DR and flexibility solutions or development of new ones

What types and formats of data will the project generate/collect?

As for proper energy community design/management/operation (incl. members' enrolment), main data types are summarized below.

- REC energy consumption;
- REC energy production (from renewable sources);
- model, size, and location of owned distributed renewable energy resources;
- REC internal remuneration rules;
- REC incentive schemas.

Will you re-use any existing data and how?

Some of the components that will be integrated within the overall MASTERPIECE architecture already includes data integration of external sources like the energy market (e.g., EU ENTSOE, Spanish Energy Network, USEF flexibility platform) as well as international weather predictions (e.g., Weatherbit) among others. Historical data on energy consumption and production will be also used for the technical validation of the functionalities to be developed/services to be provided.

What is the origin of the data?

Historical data on energy production and energy consumption will be provided by pilots and by the VPP4ISLANDS project (3 MASTERPIECE partners already collaborate in the VPP4ISLANDS project).

What is the expected size of the data?

The following table is provided considering typical quarterly measurements associate to REC operational management, according to technical data previously collected/managed. The storage is calculated on the primary data-store, it does not represent the actual DB occupation which will certainly be more demanding. The current richest message is around 220 bytes for a single quarterly reading message.

| Meter | Daily measures | Storage (Kb/day) | Yearly measures | Storage (Mb/year) |
|-------|----------------|------------------|-----------------|-------------------|
| 1 | 96 | 20,625 | 35040 | ~7,35 |
| 5 | 480 | 103,125 | 175200 | ~36,76 |
| 10 | 960 | 206,250 | 350400 | ~73,52 |
| 20 | 1920 | 412,500 | 700800 | ~147,03 |
| 50 | 4800 | 1031,250 | 1752000 | ~367,58 |
| 100 | 9600 | 2062,500 | 3504000 | ~735,19 |
| 1000 | 96000 | 20625,000 | 35040000 | ~7351,65 |

To whom might it be useful (i.e., data utility)?

4.5 FAIR Data

Considering previous positive experiences, the project is considering to adopt the ARGOS platform ([HTTPS://ARGOS.OPENAIRE.EU/](https://argos.openaire.eu/)) for managing the Data Management Plan (DMP):

ARGOS is the joint effort of OpenAIRE ([HTTPS://WWW.OPENAIRE.EU/](https://www.openaire.eu/)) and EUDAT ([HTTPS://WWW.EUDAT.EU/](https://www.eudat.eu/)) to deliver an open platform for Data Management Planning that addresses FAIR and Open best practices and assumes no barriers for its use and adoption. It is an open extensible service - available as a standalone service (OpenDMP) and as a OpenAIRE service (ARGOS) - that simplifies the management, validation, monitoring and maintenance of Data Management Plans. It allows actors (researchers, managers, supervisors etc) to create actionable DMPs that may be freely exchanged among infrastructures for carrying out specific aspects of the Data management process in accordance with the intentions and commitment of Data owners. ARGOS is a service that is integrated within the OpenAIRE platform and is freely offered for use through the OpenAIRE Service Catalogue and the EOSC Catalogue. ARGOS enhances the OpenAIRE Research Graph while at the same time utilises its underlying services, external sources and semantics to add value to the Dataset Description templates it produces thus increasing validation of DMPs. DMPs in ARGOS are treated as research outputs that can be assigned DOIs, licenses and can be re-distributed in a FAIR manner.

The project intends to exploit the Research Data Management (RDM) functionality natively provided by ARGOS: in particular, the possibility to create DMP that are machine-actionable outputs (ma-DMPs), in the form of rich text documents, following Open and FAIR practices and are published in Zenodo. Other functionalities covering the DMP publication lifecycle that will be used to support the aforementioned procedures are:

- DMP creation and management.
- Dataset creation and management, including description (private/public modes).
- Dataset classification (by type/discipline/etc.).
- DMP and dataset versioning and updating.
- Native Zenodo integration for dataset publication and sharing.

4.5.1 Making Data Findable

Are the data produced and/or used in the project discoverable with metadata, identifiable and locatable by means of a standard identification mechanism (e.g. persistent and unique identifiers such as Digital Object Identifiers, DOI)?

By adopting the ARGOS platform, natively integrated with Zenodo, the MASTERPIECE project will follow the typical upload/describe/publish workflow for proprietary datasets, making them findable with associated domain-related metadata and locatable by a dedicated DOI.

What naming conventions do you follow?

No specific naming convention is established yet at the time of reporting.

Will search keywords be provided that optimize possibilities for re-use?

Zenodo searching capabilities will be available for the research community to foster re-use.

Do you provide clear version numbers?

ARGOS' native support to DMP and dataset versioning will be exploited to ease versioning.

What metadata will be created? In case metadata standards do not exist in your discipline, please outline what type of metadata will be created and how.

Zenodo's native support for metadata will be used to describe/enrich the datasets.

TECHNICAL NOTE: as reported by Zenodo at [HTTPS://ABOUT.ZENODO.ORG/PRINCIPLES/](https://about.zenodo.org/principles/), for findability aspects (F) the following support is natively provided:

- **F1: (meta)data are assigned a globally unique and persistent identifier**
 - A DOI is issued to every published record on Zenodo.
- **F2: data are described with rich metadata (defined by R1 below)**
 - Zenodo's metadata is compliant with DataCite's Metadata Schema minimum and recommended terms, with a few additional enrichments.
- **F3: metadata clearly and explicitly include the identifier of the data it describes**
 - The DOI is a top-level and a mandatory field in the metadata of each record.
- **F4: (meta)data are registered or indexed in a searchable resource**

- *Metadata of each record is indexed and searchable directly in Zenodo's search engine immediately after publishing.*
- *Metadata of each record is sent to DataCite servers during DOI registration and indexed there.*

4.5.2 Making Data Openly Accessible

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

Fully anonymized energy production and energy consumption data might be available by default upon proper agreement with beneficiaries in charge of the pilot premises and with all actors/stakeholders directly or indirectly involved in piloting/validation/evaluation activities. Specific constraints will be identified during the preparation of the dataset records according to the procedures illustrate above.

How will the data be made accessible (e.g. by deposition in a repository)?

Datasets will be made accessible by deposition in Zenodo.

What methods or software tools are needed to access the data?

No specific methods or software will be necessary to access the provided datasets (Zenodo's native software/API documented at [HTTPS://ABOUT.ZENODO.ORG/](https://about.zenodo.org/)).

Is documentation about the software needed to access the data included?

Not applicable (Zenodo's native software/API documented at [HTTPS://ABOUT.ZENODO.ORG/](https://about.zenodo.org/)).

Is it possible to include the relevant software (e.g. in open source code)?

Not applicable (Zenodo's native software/API documented at [HTTPS://ABOUT.ZENODO.ORG/](https://about.zenodo.org/)).

Where will the data and associated metadata, documentation and code be deposited? Preference should be given to certified repositories which support open access where possible.

Datasets and associated metadata will be deposited in Zenodo's premises by native integration as supported by the ARGOS DMP management platform (see Technical Notes).

Have you explored appropriate arrangements with the identified repository?

No specific arrangements are necessary, as Zenodo is an open platform.

If there are restrictions on use, how will access be provided?

No specific restrictions to datasets are envisaged so far. If necessary, specific attention will be given to datasets provided by partners from countries outside the EU (Turkey) to solve any potential sharing issue.

Is there a need for a data access committee?

For the time being, according to the available information, a Data Access Committee is not strictly required. Should it be established, the composition will be set up according to the key roles as defined in the Grant Agreement.

Are there well described conditions for access (i.e. a machine readable license)?

Licenses will be defined when datasets will be available and duly described. The open access status and the license will be embedded in all metadata formats (i.e., machine-readable) according to Zenodo's features.

How will the identity of the person accessing the data be ascertained?

No specific need to identify the person accessing the data is reported so far.

TECHNICAL NOTE: as reported by Zenodo at [HTTPS://ABOUT.ZENODO.ORG/PRINCIPLES/](https://about.zenodo.org/principles/), for accessibility aspects (A) the following support is natively provided:

- **A1: (meta)data are retrievable by their identifier using a standardized communications protocol**
 - Metadata for individual records as well as record collections are harvestable using the OAI-PMH protocol by the record identifier and the collection name.
 - Metadata is also retrievable through the public REST API.
- **A1.1: the protocol is open, free, and universally implementable**
 - See point A1. OAI-PMH and REST are open, free and universal protocols for information retrieval on the web.
- **A1.2: the protocol allows for an authentication and authorization procedure, where necessary**
 - Metadata are publicly accessible and licensed under public domain. No authorization is ever necessary to retrieve it.
- **A2: metadata are accessible, even when the data are no longer available**
 - Data and metadata will be retained for the lifetime of the repository. This is currently the lifetime of the host laboratory CERN, which currently has an experimental programme defined for the next 20 years at least.

- *Metadata are stored in high-availability database servers at CERN, which are separate to the data itself.*

4.5.3 Making Data Interoperable

Are the data produced in the project interoperable, that is allowing data exchange and re-use between researchers, institutions, organisations, countries, etc. (i.e. adhering to standards for formats, as much as possible compliant with available (open) software applications, and in particular facilitating re-combinations with different datasets from different origins)?

Data collected / generated by the project will be made available in simple common machine-readable format, to foster interoperability as much as possible (e.g., energy consumption and energy production data in .csv files exported by relational databases or in .json forma exported by NoSQL databases).

What data and metadata vocabularies, standards or methodologies will you follow to make your data interoperable? Will you be using standard vocabularies for all data types present in your data set, to allow inter-disciplinary interoperability?

Standard metadata vocabularies will be adopted to describe the datasets (e.g., SAREF4ENERGY, [HTTPS://SAREF.ETSI.ORG/SAREF4ENER/V1.1.2/](https://saref.etsi.org/saref4ener/v1.1.2/)), according to the nature of the data provided.

In case it is unavoidable that you use uncommon or generate project specific ontologies or vocabularies, will you provide mappings to more commonly used ontologies?

No uncommon/proprietary ontologies for metadata preparation are considered necessary at the time of reporting.

TECHNICAL NOTE: as reported by Zenodo at [HTTPS://ABOUT.ZENODO.ORG/PRINCIPLES/](https://about.zenodo.org/principles/), for interoperability aspects (I) the following support is natively provided:

- **I1: (meta)data use a formal, accessible, shared, and broadly applicable language for knowledge representation.**
 - *Zenodo uses JSON Schema as internal representation of metadata and offers export to other popular formats such as Dublin Core or MARCXML.*
- **I2: (meta)data use vocabularies that follow FAIR principles**
 - *For certain terms we refer to open, external vocabularies, e.g.: license (Open Definition), funders (FundRef) and grants (OpenAIRE).*
- **I3: (meta)data include qualified references to other (meta)data**
 - *Each referenced external piece of metadata is qualified by a resolvable URL.*

4.2.4 Making Data Reusable

How will the data be licensed to permit the widest re-use possible?

Whenever possible, licenses allowing the widest possible re-use will be adopted for data sharing, according to the informed consents adopted during the collection phase (see e.g., [HTTPS://OPENDATACOMMONS.ORG/LICENSES/](https://opendatacommons.org/licenses/)).

When will the data be made available for re-use? If an embargo is sought to give time to publish or seek patents, specify why and how long this will apply, bearing in mind that research data should be made available as soon as possible.

Data will be made available as soon as significant dataset will be collected and duly described, addressing/solving any potential issue for proper data sharing. No embargo is foreseen at the time of reporting.

Are the data produced and/or used in the project useable by third parties, in particular after the end of the project? If the re-use of some data is restricted, explain why.

Shared dataset will have no specific restriction on access from third parties once published on the identified Zenodo platform.

How long is it intended that the data remains re-usable?

No specific time limit to data re-usability is identified at the time of reporting.

Are data quality assurance processes described?

Data quality assurance processes are not identified at the time of reporting: they will be generally defined during the lifespan of the project and then instantiated according to the specific features of the shared data (e.g., criteria for filling missing measures in sampled energy metering, or for identifying out-of-scale signals).

TECHNICAL NOTE: as reported by Zenodo at [HTTPS://ABOUT.ZENODO.ORG/PRINCIPLES/](https://about.zenodo.org/principles/), for reusability aspects (R) the following support is natively provided:

- **R1: (meta)data are richly described with a plurality of accurate and relevant attributes**
 - Each record contains a minimum of DataCite's mandatory terms, with optionally additional DataCite recommended terms and Zenodo's enrichments.
- **R1.1: (meta)data are released with a clear and accessible data usage license**
 - License is one of the mandatory terms in Zenodo's metadata, and is referring to an Open Definition license.
 - Data downloaded by the users is subject to the license specified in the metadata by the uploader.
- **R1.2: (meta)data are associated with detailed provenance**
 - All data and metadata uploaded is trackable to a registered Zenodo user.
 - Metadata can optionally describe the original authors of the published work.

- **R1.3: (meta)data meet domain-relevant community standards**
 - *Zenodo is not a domain-specific repository, yet through compliance with DataCite's Metadata Schema, metadata meets one of the broadest cross-domain standards available.*

4.6 Allocation of Resources

What are the costs for making data FAIR in your project?

The costs are mainly for developers, maintenance, storage spaces in the cloud, hosting of APIs, equipment (e.g., Nodes) licences for normalization and interoperability.

How will these be covered? Note that costs related to open access to research data are eligible as part of the Horizon 2020 grant (if compliant with the Grant Agreement conditions).

Mainly by the Horizon Europe Grant Agreement and own contributions. The Consortium has not specifically extrapolated costs for making data FAIR out of the budget allocated for the work packages that include data processing activities (e.g., development of components designed to process field data). The costs will be therefore implicitly covered by each partner as for their expected roles within the project. The use of the ARGOS platform and of Zenodo is free of charge for research project beneficiaries. Also, institutions such as University of Murcia (UMU) have agreements with Elsevier to publish gold open access for free.

Who will be responsible for data management in your project?

The GDPR, Data & Ethics Manager / Data Protection Officer (Stefano BIANCHI, ALWA) will be responsible for data management in the MASTERPIECE project.

Other key roles - Project Coordinator (Antonio SKARMETA, UMU), Scientific & Technical Manager (Iakovos MICHAELIDIS, CERTH), Quality & Risk Manager (Elias Kosmatopoulos, CERTH), Exploitation & Innovation Manager (Eva COSCIA, R2M), Intervention Programme Manager (Michele VISCIOLA, EXP) and Demonstrations Manager (Rafael Marin-Perez, ODINS) - will be involved in the decision-making process related to data management whenever necessary and for the applicable responsibilities.

Are the resources for long term preservation discussed (costs and potential value, who decides and how what data will be kept and for how long)?

Resources for long term preservation have not been identified yet.

4.7 Data Security

As for Data Security aspects, it is worth noting that **Key Objective 4 (KO4)** of the MASTERPIECE project directly addresses data (cyber)security and privacy issues, thus generally supporting data integrity, availability and confidentiality within the project lifespan and beyond, through dedicated activities carried out by WP2 “Energy community requirements at national and EU levels for different stakeholders and shareholders” and WP4 “Digital platforms and tools for energy communities” (with a focus on T4.5 “DLT-based secure platform for energy data collection, elaboration and sharing”):

KO4: To configure a standardised and sound cyber-security infrastructure so the active citizens are protected against cyber-attacks, at the same time that privacy is defended in accordance with the revised EPBD and the GDPR law

Description: New digital tools acquiring data from the physical world and citizen behaviour could turn into an entry bypass for threats such as cyber-attacks. This is particularly true when the solution is also created to develop local marketplaces and actuation over devices and sub-grids. For this reason, the cyber-security of the solution is one of the key objectives of this project. The consortium includes experts in this field and will use the most robust technologies to increase the strength of the solution.

Relevant results: Privacy-Preserving Identity Management mechanisms will be integrated and extended in tandem with an advanced access control system that enables policy-based authentication and authorisation evaluation for data sharing and access while preserving privacy. These mechanisms will increase the trust of all stakeholders for using the MASTERPIECE technological innovations that require sharing private information or personal data.

Main targets: consumers, prosumers, innovators, service providers

KPI: Secure data management of stakeholder private information = 100%

WP4 is expected to leverage FIWARE’s IoT platform with bydesign security & privacy features for data collection and elaboration (ODINS), implementing and extending the FIWARE enablers associated to the Interoperable Data Space and Multiparty Data Sharing.

The overall MASTERPIECE architecture, to minimize silo effects and vendor lock-ins, as well as to increase acceptance and trustiness among different energy community stakeholders/actors, includes a vertical federated layer meant to harmonize data collection, aggregation platform (gateways, sensors/actuators, harmonized filtered data, elastic search), DLT security and authorization (security and authorization mechanisms for transparent aggregated information sharing).

What provisions are in place for data security (including data recovery as well as secure storage and transfer of sensitive data)?

Zenodo platform infrastructure will be leverage to host and secure shared data.

The MASTERPIECE project is not expected to collect in principle or process any sensitive data, as for the definition provided by the GDPR regulation, Article 4(13), (14) and (15) and Article 9 and Recitals (51) to (56) (i.e., personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs; trade-union membership; genetic data, biometric data processed solely to identify a human being; health-related data; data concerning a person's sex life or sexual orientation.)

Is the data safely stored in certified repositories for long term preservation and curation?

Shared datasets will be stored in Zenodo's repositories. Although not strictly certified, Zenodo is recommended by [HTTPS://FAIRSHARING.ORG/](https://FAIRSHARING.ORG/). Zenodo's self-assessments for the FAIR principles and Plan S is reported at [HTTPS://ABOUT.ZENODO.ORG/PRINCIPLES/](https://ABOUT.ZENODO.ORG/PRINCIPLES/) from where Technical Notes are extracted.

4.8 Ethical Aspects

Are there any ethical or legal issues that can have an impact on data sharing? These can also be discussed in the context of the ethics review. If relevant, include references to ethics deliverables and ethics chapter in the Description of the Action (DoA).

The MASTERPIECE project got a full Ethics clearance ("the proposal is 'ethics ready'") from the EC at evaluation and at Grant Agreement Preparation time.

The Ethics Summary Report included the Ethics Issues declared as addressed by the project in the Ethics Self-Assessment, reported below with a summarized evidence:

- Humans
- Personal data
- Non-EU countries
- Artificial intelligence

Accordingly, all beneficiaries will endure that all ethics issues related to activities in the grant are addressed in compliance with ethical principles, the applicable international and national law, and the provisions set out in the Grant Agreement, including the aforementioned ethics issues and any additional issue that may emerge in the course of the execution of the project. In case any substantial new ethics issues arise, beneficiaries will inform the project DPO that through the Project Coordinator will notify the granting authority.

In particular:

Ethical dimension of the objectives, methodology and likely impact

MASTERPIECE will use AI for optimization of energy community management, in a fully GDPR compliant way. Then, by application of AI, data will be processed in order to provide relevant information regarding further optimization of these processes and decision- making.

The AI developments within this project have been conceived accordingly with the trustworthiness guidelines for all the AI-based techniques/systems made in Europe. All the developments performances will be properly quantified and tracked ensuring the possible detection of deviations

from expected behavior. Considering the scope of this project, only strictly necessary personal data will be captured and processed. Considering the level of interaction of the proposed developments with humans, the work proposed here does not go into conflict with any fundamental right of individuals, safety or discrimination.

Compliance with ethical principles and relevant legislations

Activities in MASTERPIECE will be carried out in accordance with commonly agreed standards of good practice, as laid down, for example, in the European Group on Ethics in Science and New Technologies, the Declaration of Helsinki, the Economic and Social Research Council (ESRC) Research Ethics Framework.

MASTERPIECE ensures trustworthy and ethical AI within the project's activities; the consortium partners are committed to follow and fully comply with the Ethics Guidelines for Trustworthy Artificial Intelligence that was presented by the European High-Level Expert Group on AI on the 8th of April 2019. According to these Guidelines, trustworthy AI should be: 1. Lawful, meaning that it respects all applicable laws and regulations, 2. Ethical, in the sense that it respects ethical principles and values; and, 3. Robust from a technical perspective while considering its social environment. The Guidelines put forward a set of 7 key requirements that AI systems should meet in order to be deemed trustworthy: - Human agency and oversight. - Technical Robustness and safety. - Privacy and data governance. - Transparency. - Diversity, non-discrimination and fairness. - Fostering diversity. - Societal and environmental well-being. - Accountability.

MASTERPIECE will carry out an assessment of the project's activities to verify the application of each of the key requirements as according to the specific assessment list that the Guidelines has established. This assessment list for the ethical AI has gone through a pilot test until December 2019, however, MASTERPIECE commits to follow-up on any possible modifications or adaptations of the same. Furthermore, a collaboration will be established with the European AI Alliance to provide continuous possibility feedback and best practices, as well as with the AI4EU Observatory on Society and Artificial Intelligence (OSAI) that supports the distribution the discussion of knowledge about the Ethical, Legal, Socio-Economic and Cultural issues of AI (ELSEC-AI) within Europe.

NOTE: In June 2023 the European Parliament adopted its negotiating position on the Artificial Intelligence (AI) Act ahead of talks with EU member states on the final shape of the law. The rules would ensure that AI developed and used in Europe is fully in line with EU rights and values including human oversight, safety, privacy, transparency, non-discrimination and social and environmental wellbeing. The MASTERPIECE project will accordingly monitor the implementation path of the AI Act during its activities in order to comply with potential additional constraints as for the applications of AI envisaged in support to the Key Objectives declared.

Is informed consent for data sharing and long-term preservation included in questionnaires dealing with personal data?

On the basis of recent similar activities carried out in energy-related projects involving private citizens/volunteers, an informed consent will be drafted to be discussed, finalized and adopted at pilot level for the enrolment of necessary actors/stakeholders and to ease the collaboration with ongoing initiatives in the Renewable Energy Community domain.

As an example, it is provisionally reported here the form prepared by the MASTERPIECE DPO for the VPP4ISLANDS project, where a dedicated activity for enrolling volunteers to simulate a REC on the Formentera Island was completed in Spring 2023.

It is relevant to notice that, whenever applicable, the Data Protection Notice included in this form can be duly adapted for the purposed of the MASTERPIECE project. Also, the Open Data option included in the form allowed the VPP4ISLANDS to start collecting energy consumption and production data that, after a proper anonymization, will be shared outside the boundaries of the project to foster additional research activities. The VPP4ISLANDS project is in fact mentioned also in the following sections as a potential source of data/information for the validation of the MASTERPIECE technical solutions.



Virtual Power Plant for Interoperable and Smart isLANDS

Novel technologies ensure the stability of smart grids and the decarbonisation of islands

Exploiting the full potential of intermittent renewable energy sources (like the sun and wind) has received a helping hand from so-called **virtual power plants (VPPs)** that remotely aggregate **distributed energy resources** from different physical locations into a network that reliably distributes energy around the clock.

Islands face many challenges in terms of energy supply, demand side management and energy security.

The VPP4ISLANDS project is revolutionising conventional VPPs by integrating **virtual energy storage technology**, **digital twin** and **distributed ledger technology** to enable enhanced VPPs and to foster

THE CREATION OF SMART ENERGY COMMUNITIES ON ISLANDS.

The outcomes of the VPP4ISLANDS project will enhance the uptake of clean green energy on islands, reducing emissions and costs while creating new opportunities for businesses and job growth.

THE PROJECT IS LOOKING FOR VOLUNTEERS TO PROVIDE THEIR ENERGY CONSUMPTION DATA AND CREATE A VIRTUAL SMART ENERGY COMMUNITY!

FREE METER



FREE INSTALLATION



FREE WEB APPLICATION



Terms and Conditions


By joining the VPP4ISLANDS project activities, you will:

- provide a few personal data to track your kind participation;
- get **FOR FREE** an energy meter that, once installed nearby your fiscal meter and connected to your WI-FI network, will send your energy consumption data to the project servers for research on energy communities;
- get **FOR FREE** a dedicated and secured web application where you can see your energy consumption in real time (up to the end of the project);
- contribute to a key research initiative funded by the European Commission;
- join a virtual smart energy community;
- help researchers to decarbonize your island and make it **GREENER!**


Your participation is voluntary and free of charge – we reward your availability with the **FREE** meter, its **FREE** installation and the **FREE** web application, plus your name in our **WALL OF FAME!**

For its research purposes, the VPP4ISLANDS project use meters that are available on the market and are installed AS-IS in your premises – the VPP4ISLANDS Consortium is not therefore responsible for its malfunctioning, whereas it is in charge of the meter configuration and installation and is available to support you in case of technical problems.





| YOUR DATA PLEASE, SO THAT WE CAN STAY IN TOUCH! | |
|---|--|
| NAME | |
| SURNAME | |
| ADDRESS | |
| EMAIL | |
| MOBILE | |
| YES - NO | I accept the Terms and Conditions for my participation to the VPP4ISLANDS project activities. |
| YES - NO | I accept to make my anonymized energy consumption data available for further research initiatives (Open Data option). |
| YES - NO | I accept that my name and surname will be publicly available on the VPP4ISLANDS project website in its Wall of Fame . |
| YES - NO | I hereby provide my informed consent to process my personal data as indicated in the Data Protection Notice . |
| SIGNATURE | |



VPP4ISLANDS project Data Protection Notice

In accordance and in compliance with the European Regulation (EU) 2016/679 of April 27, 2016 (GDPR), the VPP4ISLANDS project collects your personal data only to the extent necessary to fulfil the precise purpose related to its research activities.

1. Who is the Data Controller and the Data Processors?
 The **Data Controller** is VPP4ISLANDS coordinator Aix Marseille Université (see <https://www.univ-amu.fr/>). All other VPP4ISLANDS project partners are **Data Processors** (see <https://vpp4islands.eu/index.php/partners/>).

2. What is the purpose of the data processing?
 The **purpose of the processing** is to process personal data to track participation to the project research activities related to the monitoring of your energy consumption.

3. Who are the Data Subjects?
 The **data subjects** concerned by this notice is any person (you!) who has decided to join the project activities by adhering to the provided Terms and Conditions.

4. What are the categories of personal data collected?
 The **categories of personal data** collected and used for the processing operations are (see form above): name; surname; address; email; mobile; consent to process personal data; passwords and usernames (assigned by default). In addition, the following data is also processed for the research activities and the provision of services: energy consumption data.

5. Who are the recipients of the collected data?
 All recipients are on a "need to know" basis:

- Any authorized staff members of the VPP4ISLANDS projects Consortium;
- Aggregated anonymous data derived from collected personal data may be disclosed to the European Commission – or any empowered agency (e.g., INEA) – for the assessment and the evaluation of project activities.

6. What are your rights as a Data Subject?

- You have the right at any time to access, rectify, erase ('right to be forgotten') your personal data.
- You are also entitled to object to the processing or request for the restriction of the processing

You can exercise your rights by sending an email with the requested change(s) to the controller via the functional mailbox indicated below.
 In any case, your data will be modified or removed accordingly and as soon as practicable (maximum within 20 working days).
 When processing is based on your consent, you have the right to withdraw your consent at any time, without affecting the lawfulness of the processing before such a withdrawal.

7. How does the VPP4ISLANDS Consortium protect and safeguard your collected data?
 Relevant organisational and technical measures are taken by the VPP4ISLANDS Consortium to ensure the security of your personal data. Access to your data is restricted on an individual need-to-know basis and by strict authentication and authorization. Your data resides on servers deployed within the European Union.

8. What are the legal basis of the data processing?

- Grant Agreement number: 957852 — VPP4ISLANDS — H2020-LC-SC3-2018-2019-2020 / H2020-LC-SC3-2020-ECES-SCC – with the Innovation and Networks Executive Agency (INEA), under the powers delegated by the European Commission
- European Regulation (EU) 2016/679 of April 27, 2016 (GDPR)

9. What are the time limits for keeping the collected data?
 Time for keeping the data is in any case limited as long as necessary with the regard to the purpose(s) of the processing and is deleted as soon as it is not needed any longer, i.e., at the end of the VPP4ISLANDS project (unless the Open Data option above is ticked, so that anonymized energy consumption data will be made publicly available for further research purposes).

10. Contact information
 In case you have any question about the collection/processing of your personal data, you may contact the data controller / VPP4ISLANDS project coordinator (contact@vpp4islands.eu) and its DPO (dpo@univ-amu.fr).
 You may also contact at any time the Data Protection Officer of the VPP4ISLANDS project (dpo@vpp4islands.eu)
 You have the right to have recourse at any time to the European Data Protection Supervisor (edps@edps.europa.eu).



This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 957852

<https://vpp4islands.eu/>

4.9 Other Issues

Do you make use of other national/funder/sectorial/departmental procedures for data management? If yes, which ones?

algoWatt SpA (ALWA) is certified according to standard EN ISO 27001:2013 (Management System) as it applies an Information Security Management System (ISMS) for the following application scope "DESIGN, DEVELOPMENT, DELIVERY, MAINTENANCE AND TECHNICAL SUPPORT OF SOFTWARE SOLUTIONS. PROVISION OF PROFESSIONAL IT SERVICES". Building on this expertise, which spreads horizontally throughout the different Business Units, the different phases of the SW life-cycle encompasses cybersecurity and privacy as well, in full compliance with General Data Protection Regulation (EU) 2016/679 (GDPR), whose constraints are considered in the definition and implementation of main functionalities of services and platforms that manages personal data. In particular, compliance with GDPR Article 32 is taken into consideration, as for the obligations for Data Controllers and Data Processors to implement technical and organizational measures that ensure a level of data security appropriate for the level of risk presented by processing personal data. Compliance with Article 32 requirements is demonstrated by adherence the aforementioned approved certification, as specifically foreseen in Article 42. Data security measures considered, at a minimum, usually include: Pseudonymizing or encrypting personal data; Maintaining ongoing confidentiality, integrity, availability, access, and resilience of processing systems and services; Restoring the availability of and access to personal data, in the event of a physical or technical security breach; and Testing and evaluating the effectiveness of technical and organization measures.

The **University of Murcia (UMU)** is certified in compliance with the National Security Scheme (in Spanish Esquema Nacional de Seguridad - ENS). The National Security Scheme, as defined by Spanish regulations, applies to the entire Public Sector and extends to suppliers collaborating with the Administration. It establishes a comprehensive framework of fundamental principles, requirements, and security measures aimed at effectively safeguarding the processed information and provided services. The scheme ensures access, confidentiality, integrity, traceability, authenticity, availability, and preservation of the data, information, and services managed electronically within their respective competencies.

The **Uppsala Municipality (UPP)** is certified according to standard ISO/IEC 27001:2017, Management system for information security, and ISO/IEC 27002:2017, Policies for information security. These certifications apply to all departments and subsidiaries. Furthermore, UPP abides by the NIS directive ((EU) 2019/1148) and subsequent national compliances together with GDPR. This establishes a framework of regulations, checks and security measures to safely process and store information. As a public actor, UPP abides by national regulation to securely enable access, traceability, eventual confidentiality, preservation and storage of data.

Odin Solutions S.L. (ODINS) has the following certifications issued by AENOR: i) ISO 9001 is a Quality Management system when the organization demonstrates its ability to consistently provide products or services that meet customer and applicable regulatory requirements. The application of ISO 9001 allows small and medium-sized companies to be at the level of the largest, equaling themselves in efficiency and competing with equal opportunities in today's aggressive market. ii)

ISO/IEC 27001:2017 - OdinS is obtaining this accreditation to demonstrate its high level of security in the management and treatment of information, both at an administrative level and in its technological solutions. It establishes a comprehensive framework of fundamental principles, requirements, and security measures aimed at effectively safeguarding the processed information and provided services. The framework ensures access, confidentiality, integrity, traceability, authenticity, availability, and preservation of the data. ODINS also complies with the national regulations of data privacy along with General Data Protection Regulation (GDPR).

The **Centre for Research and Technology Hellas (CERTH)** is compliant and applies data protection rules according to Regulation (EU) 679/2016 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). To this context, it has in place internal regulations for personal data management and protection and related data protection policy to safeguard the rights and freedoms of data subjects, and implements technical and organizational measures that ensure a level of data security appropriate to the risk of personal data processing (e.g. risk of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed).

Uludağ Elektrik Dağıtım A.Ş. (UEDAŞ) has the following certificates: i) BBS Certification Training and Surveillance Services Inc. It is certified by ISO 9001 / ISO 14001 / ISO 45001. ISO 9001 is a Quality Management system that demonstrates the organization's ability to consistently provide services that meet customer and applicable regulatory requirements. ISO 14001 accredits UEDAS for environmentally efficient and sustainable resource management. ISO 45001 is a management system that ensures the establishment, management and compliance of health and safety conditions in company activities. ii) BBS Certification Training and Surveillance Services Inc. It is certified by ISO/IEC 27001:2017. UEDAŞ receives this accreditation to demonstrate the high level of security in the management and processing of information, both at the administrative level and in its technological solutions. It establishes a comprehensive framework of fundamental principles, requirements and security measures aimed at effectively protecting the information processed and the services provided. The framework provides access to data, confidentiality, integrity, traceability, authenticity, availability and protection of data. These certifications are valid for all departments and subsidiaries.

5 REFERENCES

MASTERPIECE DoW. (2022). *Grant Agreement No. 101096836*.

Expanded FMEA (EFMEA).Z.Bluvband, P.Grabov, O.Nakar. Annual Symposium on Reliability and Maintainability, (RAMS '04), pp 31-36, 2004.