Virtual Power Plant for Interoperable and Smart isLANDS

VPP4ISLANDS

LC-SC3-ES-4-2020

GA 957852

Deliverable Report

Deliverable ID	D 1.2	**Version**	0.3
Deliverable name	Data Management Plan		
Lead beneficiary	AMU		
Contributors	AMU, ALWA, RDIUP, BC2050, SCHN		
Reviewer	BUL, RDIUP		
Due date	31/03/2021		
Date of final version	13/04/2021		
Dissemination level	PU: Public		
Document approval	Seifeddine BEN ELGHALI (AMU)	13/04/2021	

Acknowledgement: VPP4ISLANDS is a Horizon 2020 project funded by the European Commission under Grant Agreement no. 957852.

Disclaimer: The views and opinions expressed in this publication are the sole responsibility of the author(s) and do not necessarily reflect the views of the European Commission

REVISION AND HISTORY CHART

Version	Date	Main Author(s)	Summary of changes
0.1	29/03/21	All Partners	Partners inputs
0.2	31/03/21	AMU	AMU inputs after review from BUL and RDIUP
0.3	13/04/21	AMU	Addition of the DPO's name p14. Removal of examples of DPR tables p20.

List of abbreviations and Acronyms

Abbreviation	Meaning
ALWA	AlgoWatt
AMU	Aix-Marseille Université
BC2050	Blockchain2050
BornholmsVarme	Bornholms Varme A/S
BoZI	Bozcaada Belediye Baskanligi
BUL	Brunuel University
CIVI	CIVIESCO srl
CSIC	Consejo Superior de Investigaciones Científicas
CU	Cardiff University
DAFNI	Network of Sustainable Greek Islands
DER	Distributed energy resources
DL	Digital Twin
DLT	Digital Ledger Technologies
FORM	Consell Insular de Formentera
FTK	FTK Forschungsinstitut fur Telekommunikation und Kooperation EV
GHG	Greenhouse gases
GRADO	Comune di Grado
IDEA	Ingenieria Y Diseno Estructural Avanzado
INAVITAS	INAVITAS Enerji AS
LIS	Laboratoire Informatique des Systèmes
RDIUP	RDI'UP
REGENERA	REGENERA LEVANTE
SCHN	Schneider Electric
TROYA	TROYA CEVRE DERNEGI
UEDAS	Uludag electric dagitim
VESS	Virtual energy storage systems
VPP	Virtual Power Plant
GDPR	General Data Protection Regulation
DC	Data Controller
DCL	Data Collection Guidelines
DEG	Data Exchange Guidelines
DP	Data Processor
DPG	Data Processing Guidelines
DPL	Data Processing Log
	Data Protection Officer
DDPO	Deputy Data Protection Officer
DPR	Data Processing Record
DSS	Decision Support System
EC	European Commission
GA	Grant Agreement
GDPR	General Data Protection Regulation
SERI	Secretariat for Education, Research and Innovation

KB	Knowledge Base
ML	Machine Learning

Table of Contents

The VPP4Islands project has received funding from the European Union's Horizon 2020 research and innovation programme under GA No. 957852

1 Executive Summary

The purpose of this document is to provide a first draft of the Data Management Plan (DMP) for the VPP4ISLANDS project, following the Open Research Data Pilot principles. Those principles aim to improve and maximise access to and re-use of research data generated by Horizon 2020 projects and consider the need to balance openness and protection of scientific information, commercialisation and Intellectual Property Rights (IPR), privacy concerns, security as well as data management and preservation questions.

The following sections explain how the project activities comply with Protection of Personal Data (POPD) requirements established by the EC and national regulations, as well as with GDPR with respect to the privacy of EU and Turkish citizen. The DMP describes the principles on data management (including security) to show how data are collected, stored, documented, shared and reused during and after the project lifespan. It also describes the data management life cycle for the data to be collected, processed and/or generated by VPP4ISLANDS and includes preliminary information on:

- the handling of research data during and 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).

As the Consortium will enter a more operative phase with a peak in development, integration and testing activities – and with more intensive data production and exchange – the DMP could undergo further revisions, according to actual needs and findings.

The structure of this DMP strictly follows the indications provided by the Guidelines on FAIR Data Management in Horizon 2020.

The information contained in this plan is ultimately meant to support the Consortium in undertaking all necessary actions to fulfil the obligations as for Article 29.3 “Open access to research data” of the Grant Agreement:

> ***29.3 Open access to research data***
> *Regarding the digital research data generated in the action (‘data’), the beneficiaries must:*
> *(a) deposit in a research data repository and take measures to make it possible for third parties to access, mine, exploit, reproduce and disseminate — free of charge for any user — the following:*
> *(i) the data, including associated metadata, needed to validate the results presented in*
> *scientific publications, as soon as possible;*
> *(ii) not applicable;*
> *(iii) other data, including associated metadata, as specified and within the deadlines laid down in the ‘data management plan’ (see Annex 1);*
> *(b) provide information — via the repository — about tools and instruments at the disposal of the beneficiaries and necessary for validating the results (and — where possible — provide the tools and instruments themselves).*
> *This does not change the obligation to protect results in Article 27, the confidentiality obligations in Article 36, the security obligations in Article 37 or the obligations to protect personal data in Article 39, all of which still apply.*

The VPP4Islands project has received funding from the European Union’s Horizon 2020 research and innovation programme under GA No. 957852

> *As an exception, the beneficiaries do not have to ensure open access to specific parts of their research data under Point (a)(i) and (iii), if the achievement of the action's main objective (as described in Annex 1) would be jeopardised by making those specific parts of the research data openly accessible. In this case, the data management plan must contain the reasons for not giving access.*

First of all, the data which will be managed throughout the project duration can be categorized as following:

- **#1 Information about the consortium:** Data about the consortium, such as personal information, emails, etc. will be handled and stored in private and secure storage. Access will be restricted to the members of the consortium.
- **#2 Project files:** All data gathered from meetings, workshops, and any type of internal communication will be stored and protected suitably.
- **#3 Research activities:** Data presented and discussed in the individual deliverables will be stored and protected suitably.
- #**4 Development data, implementations and codes**: Development and codes, as well as implementations derived from the project, will be performed in a private repository (GitLab).
- **#5 Pilot and testing activities:** In the cases of pilots any information and data will be stored and managed locally by the respective leading partner. In the case of an end-user using their own repositories (or a copy of specific data for testing purposes), their local policies and data management restrictions will apply. In any case, data will be deleted when the corresponding validation finishes.

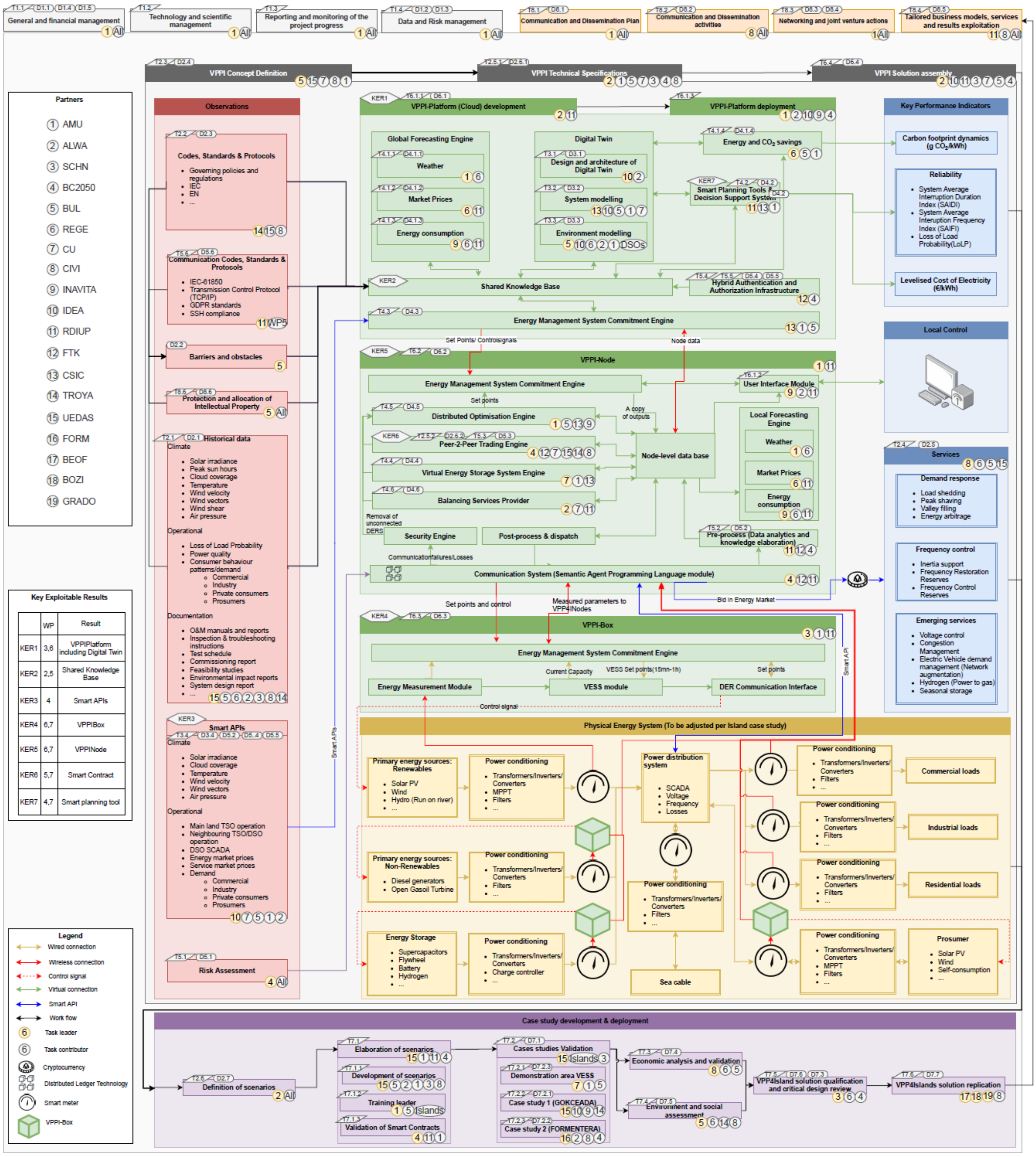
2 Data Summary

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

The purpose of the data collection/generation within the VPP4ISLANDS project activities is mainly related to demonstration activities (WP7) meant to validate the technical results as for the components developed by WP3, WP4, WP5, WP6. In particular, as for the relation to the main objectives of the project, the data that will circulate in the VPP4ISLANDS architecture will be of 2 main categories:

- **Network/device data:** these are data coming from the monitored field/pilot (e.g. in the case of architectures with remote devices such as smart meters, gateways, RTU, primary station/substation control systems, batteries, distributed energy sources, etc.) and constitute the main input for the monitoring/analytical components of the VPP4ISLANDS systems;
- **Analytical data:** these are data produced by the components according to the analytical work carried out by the platform to achieve the expected functionalities – e.g. optimization, AI/ML;

The VPP4Islands project has received funding from the European Union's Horizon 2020 research and innovation programme under GA No. 957852


General and financial management
Technology and scientific management
Reporting and monitoring of the project progress
Data and Risk management
Communication and Dissemination Plan
Communication and Dissemination activities
Networking and joint venture actions
Tailored business models, services and results exploitation
VPPI Concept Definition
VPPI Technical Specifications
VPPI Solution assembly
Partners
AMU
ALWA
SCHN
BC2050
BUL
REGE
CU
CIVI
INAVITA
IDEA
RDIUP
FTK
CSIC
TROYA
UEDAS
FORM
BEOF
BOZI
GRADO
Observations
Codes, Standards & Protocols
Communication Codes, Standards & Protocols
Barriers and obstacles
Protection and allocation of Intellectual Property
Historical data
Smart APIs
Risk Assessment
VPPI-Platform (Cloud) development
VPPI-Platform deployment
Global Forecasting Engine
Weather
Market Prices
Energy consumption
Digital Twin
Design and architecture of Digital Twin
System modelling
Environment modelling
Energy and CO2 savings
Smart Planning Tools & Decision Support System
Shared Knowledge Base
Hybrid Authentication and Authorization Infrastructure
Energy Management System Commitment Engine
Set Points/ Controlsignals
Node data
VPPI-Node
User Interface Module
Distributed Optimisation Engine
Peer-2-Peer Trading Engine
Virtual Energy Storage System Engine
Balancing Services Provider
Local Forecasting Engine
Node-level data base
Security Engine
Post-process & dispatch
Pre-process (Data analytics and knowledge elaboration)
Communication System (Semantic Agent Programming Language module)
Bid in Energy Market
VPPI-Box
Energy Measurement Module
VESS module
DER Communication Interface
Control signal
Physical Energy System (To be adjusted per Island case study)
Primary energy sources: Renewables
Primary energy sources: Non-Renewables
Energy Storage
Power conditioning
Power distribution system
Sea cable
Commercial loads
Industrial loads
Residential loads
Prosumer
Key Performance Indicators
Carbon footprint dynamics (g CO2/kWh)
Reliability
Levelised Cost of Electricity (€/kWh)
Local Control
Services
Demand response
Frequency control
Emerging services
Key Exploitable Results
Legend
Wired connection
Wireless connection
Control signal
Virtual connection
Smart API
Work flow
Task leader
Task contributor
Cryptocurrency
Distributed Ledger Technology
Smart meter
VPPI-Box
Case study development & deployment
Definition of scenarios
Elaboration of scenarios
Development of scenarios
Training leader
Validation of Smart Contracts
Cases studies Validation
Demonstration area VESS
Case study 1 (GOKCEADA)
Case study 2 (FORMENTERA)
Economic analysis and validation
Environment and social assessment
VPP4Island solution qualification and critical design review
VPP4Islands solution replication

	WP	Result
KER1	3,6	VPPIPlatform including Digital Twin
KER2	2,5	Shared Knowledge Base
KER3	4	Smart APIs
KER4	6,7	VPPIBox
KER5	6,7	VPPINode
KER6	5,7	Smart Contract
KER7	4,7	Smart planning tool

Figure 1. Conceptual VPP4ISLANDS architecture.

According to the current version of the conceptual architecture of the project (that will evolve to be adapted to the needs to be addressed, see Figure 1) and to the nature of the components included therein, the Consortium preliminary provided a description of the types/format of data that will be managed within the scope of the project, as described in the following paragraphs.

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

Collected: Csv file (smart meter), Distributed Energy Resources (DER) signals, commands and statuses

The VPP4Islands project has received funding from the European Union's Horizon 2020 research and innovation programme under GA No. 957852

Generated: JSON, PDF, figures, CSV file, information exchange through communication protocols

The smart contracts we will create will govern the individual transactions in the VPP framework. The existence or not of some metadata per case (and not their contents) will trigger respective smart contracts to act and the outputs will be conditions and permissions for the transactions to go further.

► Will you re-use any existing data and how?

At the time of the first delivery of this document (M6, March 2021), the Consortium has not identified any specific need to re-use existing data sets, although this possibility is not excluded (training data sets might be necessary to train the systems according to e.g. historical data available at pilot level).

► What is the origin of the data?

Smart meter, VPP4IBox, existing local repositories, weather station, other monitoring and control devices that could be already available at each of the demonstration sites.

► What is the expected size of the data?

At the time of the first delivery of this document (M6, March 2021), the Consortium is not able to accurately define the size of the used data.

► To whom might it be useful ('data utility')?

The data that will be collected during the project will be mainly used by:

- Developers at the level of the VPP4IPlatform and the VPP4INode for the development of prediction tools and the evaluation of the decision-making tool. Decision makers, Policy makers, TSO/DSO, islands communities,

3 FAIR data

3.1 Making data findable, including provisions for metadata

3.1.1 Communication System

The communication system provides the required means for collecting data from VPP4IBoxes according to standard communication technologies. The collected meta data will be identifiable and discriminable via unique connection IDs.

► 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)?

Partially, the key data will be identifiable via unique IDs and other metadata.

► What naming conventions do you follow?

For classes and names RDIUP will respectively uppercamelcase and snakecase

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

The VPP4Islands project has received funding from the European Union's Horizon 2020 research and innovation programme under GA No. 957852

Yes, mostly for reader data

► Do you provide clear version numbers?

RDIUP will provide a clear numerical versioning for different databases.

► 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.

Firstly, the identifiers will be created to access to other data. Also, we will be use the consumption profiles to describe and represent the consumers behaviours, number and activities (e.g. presence).

3.2 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. (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.)

This question has to be mainly answered by Islands. The shared knowledge base (RDIUP, IDEA, REGE, FTK, AMU, BUL) will be totally accessible.

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

This issue will be addressed later in the project.

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

The KB will accessible via an API, protected by Authentication and authorization protocols for example (JWT and or SAPL) and we will define HTTPS resources' requests.

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

In the related deliverables, clear, comprehensible, and intuitive guides and user manual will be provided.

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

We use mainly open source frameworks (e.g. Django REST Framework) and python-based codes.

► 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.

The information related to the demonstration will be stored in local repositories (e.g. Node-level database) and the elaborated Knowledge and documentations will be stored in European data centers (cloud).

► Have you explored appropriate arrangements with the identified repository?

Not yet

The VPP4Islands project has received funding from the European Union's Horizon 2020 research and innovation programme under GA No. 957852

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

This issue will be addressed later in the project.

► Is there a need for a data access committee?

IT will be worth to build a data access committee in order to verify the compliance with regulations.

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

Our authorisation and authentication modules can be useful for access management.

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

We will propose tokenisation technique for access verification.

3.3 Making data interoperable

3.3.1 Pre-processing (Data Analytics and Knowledge Abstraction)

The collected data from different VPP4IBoxes would be analysed, and unified to meet the processing requirements of different processing modules of the VPP4INodes. After this pre-process, the data will be stored in Node-Level data base. The structure of the entities in this database corresponds with that of the shared knowledge base at the cloud platform for VPP4ISLANDS.

► 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)?

We will deploy solutions for unified data collection and data normalisation. Also, for information exchange we will use interoperable JSON format in the Node and cloud layers and OPC for physical layer.

► What data and metadata vocabularies, standards or methodologies will you follow to make your data interoperable?

As mentioned before, we will use controlled vocabularies, OPC, JSON and ISO 8601

► Will you be using standard vocabularies for all data types present in your data set, to allow inter-disciplinary interoperability?

Yes, we will use the methods and techniques proposed by OHDSI (e.g. OMOP, CDM)

► 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?

It depends on the requirements of demo sites.

The VPP4Islands project has received funding from the European Union's Horizon 2020 research and innovation programme under GA No. 957852

3.4 Increase data re-use (through clarifying licences)

3.4.1 Node-Level Data Base

The required mechanism for reuse and interoperability of data will be provided by the Node-Level Data base. By defining and provisioning the required access privileges with time-stamps, not only the a secure mechanism for data reuse will be provided, also the third-parties.

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

Our generated information (analytic results, recommendations and best practices) will be openly accessible without licence.

► 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.

Once information is generated and stored, they will be available for re-use (e.g. replications)

► 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.

The produced knowledge will be certainly reused by other islands, DSOs, and RTOs.

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

Forever

► Are data quality assurance processes described?

T5.2 will ensure the quality of data through cleaning and pre-processing services.

4 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, equipments (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 2020 grant and own contributions.

Provided 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), and

The VPP4Islands project has received funding from the European Union's Horizon 2020 research and innovation programme under GA No. 957852

- costs are eligible for reimbursement during the duration of the project under the conditions defined in the H2020 Grant Agreement, in particular Art. 6[1] and Art. 6.2.D.3[2], but also other articles relevant for the cost category chosen,

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.

► Who will be responsible for data management in your project?

AMU

► 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)?

Not yet.

5 Data security

5.1 Communication System

The security mechanism provided along with communications, will ensure the security of data that transfers between different modules of the VPPI-Node.

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

That will be mainly ensured by Blockchain and SAPL modules in WP5.

On what concerns blockchain coding it will be secured due to the secure environment it'll be created in.

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

Yes.

6 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 main issues are the personal data protection and privacy. Mainly in WP9, T5.6 will ensure the verification of GDPR compliance in WP5.

[1] http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/amga/h2020-amga_en.pdf#page=36

[2] http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/amga/h2020-amga_en.pdf#page=83

The VPP4Islands project has received funding from the European Union's Horizon 2020 research and innovation programme under GA No. 957852

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

Yes, it is planned and will be carried out.
Yes, each pilot owner has provided preliminary informed consent forms that will be used to enrol testers and participants in pilots.

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

No other specific national/funder/sectorial/departmental procedures for data management is used within the project activities, that are carried out according to the Operative DMP Guidelines issued internally and reported in Annexes.

Yes, we will consult the French CNIL organization to enhance our data management procedures.

7 Operative DMP Guidelines

7.1 Introduction

7.1.1 Definitions

Terms such as *'Personal Data'*, *'Process/Processing'*, *'Data Controller'*, *'Data Processor'*, *'Data Subject'* shall have the same meaning as in the Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR) of the European Parliament and of the Council of 27 April 2016. In line with the above-mentioned references and for the purposes of these clauses,

a) *'Personal Data'* are any collected data that can be linked by reasonable means to a physical person (*'Data Subject'*). Data that cannot be linked to a physical person by reasonable means, including data linked to a pseudo and/or fully anonymized data, are not considered as *Personal Data*;
b) *'Developers'* are understood as any individual or legal entity developing and/or using (e.g. for testing, piloting and/or evaluation purposes) the VPP4ISLANDS applications or tools, including any *Data Provider*, *Data Controller* and *Data Processor*, affiliated to the committed beneficiaries;
c) *'Processing of Personal Data'* (*'Processing'*) shall mean any operation or set of operations which is performed upon *Personal Data*, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;
d) *'Data Controller'* shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data;
e) *'Data Processor'* shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

The VPP4Islands project has received funding from the European Union's Horizon 2020 research and innovation programme under GA No. 957852

f) *'DATA PROVIDER'* shall mean a natural or legal person, public authority, agency or any other body which, according to the purposes and means determined by the *DATA CONTROLLER*, provides data to the *DATA PROCESSOR* for *PROCESSING* purposes;

g) *'CONSENT'* shall mean any freely given specific and informed indication of wishes by which the *DATA SUBJECT* signifies his/her agreement to *PERSONAL DATA* relating to him/her being processed;

h) *'SENSITIVE DATA'* means *PERSONAL DATA* revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life;

i) *'END-USER'* means any natural person using an on line and/or electronic communication service and/or an application in the context of the VPP4ISLANDS project, for private or business purposes;

j) *'SUB-PROCESSOR'* means any processor engaged by the data processor or by any other sub-processor of the data processor who agrees to receive, from the data processor or from any other sub-processor of the data processor, personal data exclusively intended for processing activities to be carried out on behalf of the data controller after the transfer in accordance with his instructions, the terms of these clauses and the terms of the written subcontract;

k) *'APPLICABLE DATA PROTECTION LAW'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the State in which the data controller is established;

l) *'TECHNICAL AND ORGANISATIONAL SECURITY MEASURES'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

7.2 Rules and commitments

7.2.1 General rules

► **The following general rules are binding all VPP4ISLANDS *DEVELOPERS*.**

Any VPP4ISLANDS *DEVELOPER* commits to respect the rules and guidelines defined in the present section, in addition to any other relevant disposition found throughout this document, and to make them respected by other internal agents (collaborators, students, employees, etc.) affiliated to the committed beneficiary:

1. Any *PERSONAL DATA* shall be processed in compliance with the General Data Protection Regulation[3].
2. Any *PERSONAL DATA* shall be processed solely for the purposes of the performance, management and monitoring of the activities described in the GA, i.e. any *PERSONAL DATA* collected within the project activities shall be used only for the achievement of the expected project results and not for other research.
3. Any *PERSONAL DATA* shall be processed internally for the purposes of the performance, management and monitoring of the activities described in the GA, i.e. any *PERSONAL*

[3] 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

The VPP4Islands project has received funding from the European Union's Horizon 2020 research and innovation programme under GA No. 957852

Data shall be disclosed only to beneficiaries that formally committed to abide by these rules and guidelines.

4. Each committed beneficiary undertakes to adopt appropriate technical and organisational security measures (having regard to the risks inherent in the *Processing* and to the nature of the *Personal Data* concerned) in order to:
    a. prevent any unauthorised person from having access to computer systems *Processing Personal Data*, and especially:
        i. unauthorised reading, copying, alteration or removal of storage media;
        ii. unauthorised data input as well as any unauthorised disclosure, alteration or erasure of stored *Personal Data*;
        iii. unauthorised using of *Processing* systems by means of data transmission facilities;
    b. ensure that authorised *Developers* of a *Processing* system can access only the *Personal Data* to which their access right refers;
    c. record which *Personal Data* have been communicated, when and to whom;
    d. ensure that *Personal Data* being processed on behalf of third parties can be processed only in the manner prescribed by the GA;
    e. ensure that, during communication of *Personal Data* and transport of storage media, the data cannot be read, copied or erased without authorisation;
    f. design its organisational structure in such a way that it meets data protection requirements, and especially:
        i. proper mitigation action shall be immediately undertaken in case a risk is identified that these rules may be breached;
        ii. in case any breach is identified, both beneficiary's internal hierarchy and the DPO must be immediately notified.

Stefano Bianchi, ALWA Research & Innovation Manager (stefano.bianchi@algowatt.com) was appointed **Data Project Officer of the VPP4islands project** due to his experience as the company Data Protection Officer.

7.2.2 General commitments

► The following general commitments are binding all VPP4ISLANDS *Developers*.

All *Developers* commit to process any *Personal Data*:

- fairly and lawfully;
- for limited purposes;
- in an adequate, relevant and not excessive way;
- limited to what is needed and relevant for the research;
- collected on a voluntary basis from the *End-Users*;
- privileging aggregated and/or anonymous data;
- not kept longer than necessary;
- in accordance with the *Data Subject*'s rights;
- in a secure way;
- without transferring it to countries in lacking of adequate protection.

Furthermore, all *Developers*:

- acknowledge that VPP4ISLANDS is committed to promote sustainable development, human rights, democracy, peace, gender equality and environment protection - and prohibits the use of its platform for any experiment which may by contrary to those values;

- acknowledge that VPP4ISLANDS is a multidisciplinary research platform, and by contributing data, explicitly authorize the use of non-personal data, including aggregated and anonymized data, for research purpose, including for publications;
- understand that the VPP4ISLANDS platform is provided on a best-effort basis, as is, and relies on a free and voluntary participation;
- acknowledge and agree that data that cannot be linked to a physical person by “reasonable means” are not considered as *Personal Data*;
- acknowledge that the use of pseudo to log on the platform to create an account without providing the real name and/or physical address of the *User* constitutes a valid form of pseudonymization, which amounts to a robust security measure in line with European norms;
- ensure that adequate security, technical and procedural measures are adopted in order to avoid the commission of cybercrimes and/or of intellectual property violations and/or of any other crimes through the use of VPP4ISLANDS platform;
- acknowledge that VPP4ISLANDS services cannot be subcontracted/sup-provided to third parties without express and written agreement from the VPP4ISLANDS Consortium;
- renounce to any claim against the VPP4ISLANDS project, committed beneficiaries, partners and agents for any damage or prejudice, which has not been intentionally caused by one or several members of the VPP4ISLANDS project - in case of intentional damage, the claims should be targeted exclusively to the intentional author of the damage[4].

7.2.3 Specific commitments

► The following commitments are binding VPP4ISLANDS all *Data Controllers* and *Data Processors*.

Each VPP4ISLANDS *Data Controller* and *Data Processor* commits to:

- request a written commitment to abide and respect the present rules from their agents (collaborators, students, employees etc.) who can access *Personal Data*;
- inform the *End-User* for how long their *Personal Data* will or may be retained;
- ensure to *End-User* the possibility to access, rectify, delete or block his/her *Personal Data*;
- inform the project DPO about:
  - the location(s) of all data centres where *Personal Data* shall be processed, and, where and how they may be stored, mirrored, backed up, and recovered;
  - the identity of sub-contractors and sub-processors participating in the *Personal Data Processing*, ensuring that all the requirements used to protect data are fulfilled;
  - changes concerning the addition or replacement of subcontractors or sub-processors, giving the project at all times the possibility to object to such changes or to terminate the contract;
  - relevant changes concerning applicable cloud computing services with an impact on *Personal Data*, such as the implementation of additional functions;

[4] For Swiss Partners - this clause is void under the Swiss law. Art. 100 of the Swiss Code of Obligations states: - Exclusion of liability - 1 Any agreement purporting to exclude liability for unlawful intent or gross negligence in advance is void.

The VPP4Islands project has received funding from the European Union’s Horizon 2020 research and innovation programme under GA No. 957852

  - any data breach, without delay and, where feasible, not later than 72 hours after having become aware of it (otherwise, to be accompanied by the reasons for the delay), indicating the typology of damage realized and, at the end of the duly internal investigation, the possible cause;
  - whether *Personal Data* might be transferred outside the EU, backed-up and/or recovered across borders, in the regular course of operations or in an emergency.

Each *Data Controllers* and *Data Processors* is individually responsible for its *Personal Data Processing* and no joint control is to be created, nor joint liabilities accordingly.

7.2.3.1 Data Controller's specific commitments

Each VPP4ISLANDS *Data Controller* commits to the following guidelines:

- collect and use only the *Personal Data* that is required for declared purposes;
- whenever any *Personal Data* is collected, explicitly state the precise purpose for the collection and all the ways that the information might be used, including any plans to share it with other parties;
- explicitly state how long this *Personal Data* will be stored and used, consistently with the “minimization” principle;
- communicate the VPP4ISLANDS privacy policy to *Data Subjects* whose *Personal Data* is being collected;
- provide clear and accessible details on how to contact the DPO to obtain additional information or to resolve problems relating to stored personal information;
- ensure that personal information is sufficiently accurate and up-to-date for the intended purposes;
- ensure the *Data Subjects*’ rights of access and rectification of *Personal Data*;
- ensure that all corrections are propagated in a timely manner to all parties that have received or supplied the inaccurate data;
- promote accountability for how *Personal Data* is collected, maintained, and shared;
- enforce adherence to privacy policies through such methods as audit logs, internal reviews, independent audits;
- maintain provenance – information regarding the sources and history of *Personal Data* – for at least as long as the data itself is stored as *Personal Data*.

In particular, the *Data Controller* shall:

- ensure internal accessibility to the information about its identity, address and role;
- enable the *End-User* to actively decide which *Personal Data* he/she is willing to share and inform the *End-User* about where and in which modalities his/her *Personal Data* are stored;
- inform the *End-User* about the methods available or employed to delete data and whether data may be retained after the *End-User* has deleted (or requested deletion of) the data, or after the termination of the contract with the VPP4ISLANDS Project, and in each case the period during which they will retain the data;
- implement systematic mechanisms to evaluate, reduce, and destroy unneeded and stale *Personal Data* on a regular basis, rather than retaining it indefinitely – this mechanism is considered as achieved when *Personal Data* are fully anonymized;

- provide mechanisms to allow individuals to determine with which parties their *Personal Data* has been shared, and for what purposes, unless legally exempted from doing so;
- before deployment of new activities and technologies that might impact personal privacy, carefully evaluate them for their necessity, effectiveness, and proportionality: the least privacy-invasive alternatives should always be sought;
- ensure that the parties most able to mitigate potential privacy risks and privacy violation incidents are trained, authorized, equipped, and motivated to do so.

The *Data Controller* agrees and warrants:

- that the processing of the *Personal Data* will be carried out in accordance with the relevant provisions of the *Applicable Data Protection Law* (and, where applicable, has been notified to the relevant authorities of the Member State where the data controller is established) and does not violate the relevant provisions of that State;
- that throughout the duration of the *Personal Data* processing services it will instruct the *Data Processors* to process the *Personal Data* transferred only on the *Data Controller*'s behalf and in accordance with the *Applicable Data Protection Law* and these clauses;
- that any subject appointed as *Data Processor* will provide sufficient guarantees in respect of the technical and organisational security measures indicated in these clauses and in the Annex 1 of the GA;
- that after assessment of the requirements of the *Applicable Data Protection Law*, the security measures are appropriate to protect *Personal Data* against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the *Processing* and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- that it will ensure compliance with the security measures indicated in Annex 1 of the GA;
- that, if the processing will imply the transfer of *Personal Data* outside the European safety area, the *Data Subject* has been informed (at the time when *Personal Data* have been obtained) or will be informed (before, or as soon as possible after, the transfer) that its data could be transmitted to a third country not providing adequate protection within the meaning of the European Directive 95/46/EC;
- to make available to the *Data Subjects* a summary description of the security measures adopted;
- that, in the event of sub-processing, the *Processing* activity is carried out by a sub-processor providing at least the same level of protection for the *Personal Data* and for the rights of the *Data Subject* as the *Data Processor*.

The *Data Controller* shall ensure that:

- the *End-User* will be notified about the purpose and the scope of the VPP4ISLANDS project;
- the principle of informed consent by the *End-Users* is respected (participants to experiments in the context of VPP4ISLANDS project shall always have previously given their formal consent to take part in it, with a clear information on the collected data and their potential use and dissemination);

The *Data Controller* finally acknowledges that:

- the *End-User* is free to grant a consent which can be fully or partially withdrawn with easy modalities, whenever the *End-User* wants;
- geolocalization, if performed, requires previous *End-User*'s consent and shall provide, if reasonably implementable, the possibility to choose the level of "granularity of geolocalization".

7.2.3.2 Data Processor's specific commitments

Each *Data Processor* agrees and warrants:

- to process the *Personal Data* only on behalf of the *Data Controller*, according to specific agreement, and in compliance with its instructions and these clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform without undue delay and not later than 72 hours after having become aware of it the *Data Controller* of its inability to comply, in which case the *Data Controller* is entitled to suspend the transfer of data and/or terminate the contract;
- that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the *Data Controller* and its obligations under this data *Processing* agreement and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by these clauses, it will notify the change to the *Data Controller* without undue delay and not later than 72 hours after having become aware of it, in which case the *Data Controller* is entitled to suspend the transfer of data and/or terminate the contract;
- that it has implemented the technical and organisational security measures indicated in Annex 1 of the GA before processing the *Personal Data* transferred;
- that it will without undue delay notify the *Data Controller* about:
    - any legally binding request for disclosure of the *Personal Data* by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
    - any accidental or unauthorised access (without undue delay and, where feasible, not later than 72 hours - otherwise the reasons for the delay must be declared), and
    - any request received directly from the *Data Subjects* without responding to that request, unless it has been otherwise authorised to do so;
- to deal promptly and properly with all inquiries from the *Data Controller* relating to its processing of the *Personal Data* subject to the transfer and to abide by the advice of the competent supervisory authority with regard to the processing of the data transferred;
- at the request of the *Data Controller* to submit its data processing facilities for audit of the processing activities covered by these clauses which shall be carried out by the *Data Controller*;
- to make available to the *Data Subject* upon request a copy of the data *Processing* agreement, or any existing contract for sub-processing, and a summary description of the security measures in those cases where the *Data Subject* is unable to obtain a copy from the *Data Controller*;
- that, in the event of sub-processing, it has previously informed the *Data Controller* and obtained its prior written consent.

The *Data Processor* shall not subcontract any of its processing operations performed on behalf of the *Data Controller* under these clauses without the prior written consent of the *Data Controller*. Where the *Data Processor* subcontracts its obligations under these

The VPP4Islands project has received funding from the European Union's Horizon 2020 research and innovation programme under GA No. 957852

clauses, with the written consent of the *Data Controller*, it shall do so only by way of a written agreement with the sub-processor in the name and on behalf of *Data Controller*, which imposes the same obligations on the sub-processor as are imposed on the *Data Processor* under these clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data processor shall remain fully liable to the *Data Controller* for the performance of the sub-processor's obligations under such agreement.

Each *Data Processor* in the context of VPP4ISLANDS project agrees that on the termination of the provision of data *Processing* services, the *Data Processor* and the sub-processor shall, at the choice of the *Data Controller*, return all the *Personal Data* transferred and the copies thereof to the *Data Controller* or shall destroy all the *Personal Data* and certify (by means of a self-declaration indicating the applicable **Data Processing Record**) to the *Data Controller* that it has done so, unless legislation imposed upon the *Data Processor* prevents it from returning or destroying all or part of the *Personal Data* transferred. In that case, the *Data Processor* warrants that it will guarantee the confidentiality of the *Personal Data* transferred and will not actively process the *Personal Data* transferred anymore.

The *Data Processor* and the sub-processor warrant that upon request of the *Data Controller* and/or of a supervisory authority, it will submit its data *Processing* facilities for an audit of the measures.

7.2.4 Operative guidelines

7.2.4.1 Data exchange guidelines

The herein included **Data Exchange Guidelines** provide reference instructions for all VPP4ISLANDS *Developers* to properly manage all data exchanges, independently from the nature of the exchanged data (i.e. *Personal Data* or other types of data), within all VPP4ISLANDS project's activities.

The VPP4ISLANDS *Developers* engaged in sharing *Personal Data* (or other types of data) are required to include a description of their respective data sharing agreements in terms of formal **Data Processing Records (DPR)** to be included in an overall project's **Data Processing Log (DPL)** maintained by the DPO.

Any time a new exchange of *Personal Data* (or other types of data) is previously agreed in written form between a *Data Controller* and *Data Processor*:

- a new DPR must be filled in;
- the filled-in DPR must be sent to the DPO for notification (within a reasonable period, but at the latest 72 hours after editing the new DPR);
- the filled-in DPR must be added accordingly by the DPO to the DPL.

The DPR can be filled in by any agent (researcher, employee, etc.) affiliated to the *Data Controller* or to the *Data Processor*, according to the agreements undertaken.

A separate DPR is needed each time the same data is handed by the *Data Controller* to another *Data Processor* for *Processing*.

The DPO is responsible for updating the DPL according to the DPR received, to be stored in chronological order and numbered consequently.

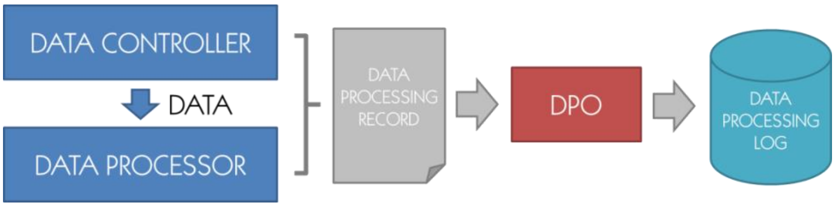


Figure 2. Data Exchange Procedure (DEP)

The procedure of DPR issue and DPL update is meant to:

- homogenize the reporting of data exchanges;
- formalize the process of notification to the DPO;
- keep a tracked history of any data exchange within the project activities;
- alleviate compliance burden for partners who do not need to exchange data;
- identify each partner's role in data exchanges[5];
- specify the nature of data exchanged (Data Type field);
- describe the data exchanged (Data Description/Notes field);
- formalize the use of the data exchanged (Processing Purpose field);
- associate the use of the data exchanged to technical activities (Related WPs/Tasks field);
- contextualize the use of the data exchanged to demonstration activities (Related Use Cases field);
- record the data storage facility for the data exchanged (Data Processor Storage field).

The procedure described above, as well as all consequent internal activities for both *DATA CONTROLLERS* and *DATA PROCESSORS*, are bound by the constraints expressed in rules and commitments reported in Section 7.2.

The following table illustrates the template of a DPR:

Data Processing Record #<N>	
Created on	<dd.mm.yyyy>
Created by	<Name Surname> (<Beneficiary Short Name>, <email>)
Data Protection Officer	<Name Surname> (<Beneficiary Short Name>, <email>)
Data Controller	<Beneficiary Short Name>
Data Processor	<Beneficiary Short Name>
Data Exchange Channel	…
Data Type	…
Processing Purpose	…
Retention Time	… - <dd.mm.yyyy>
Data Processor Storage	…
Related Use Cases	<Use_case_reference>
Related WPs/Tasks	WP<N>
Data Description/Notes	…

[5] E.g. to avoid that all project partners might be considered 'co-controllers' according to the signature of the GA, as by default they all determined the purpose and use of *PERSONAL DATA* on the VPP4ISLANDS project.

The VPP4Islands project has received funding from the European Union's Horizon 2020 research and innovation programme under GA No. 957852

Method used to return/destroy	

The fields *Data Controller* and *Data Processor* of the DPR must be filled in with beneficiaries' short names.

7.2.4.2 Data processing guidelines

The herein included Data Processing Guidelines provide reference instructions for all VPP4ISLANDS *Developers* to properly manage all data *Processing*, independently from the nature of the data (i.e. *Personal Data* or other types of data), within all VPP4ISLANDS's project activities.

They are therefore meant to be applied by *Data Controller* and *Data Processor* as for their operational roles:

- any *Data Controller* is bound to respect these guidelines before providing data to a *Data Processor* within the agreement formalized by a DPR (data preparation phase);
- any *Data Processor* is bound to respect these guidelines once data have been received by a *Data Controller* and the *Processing* is operated accordingly to the Purpose expressed in the DPR (data elaboration phase).

covering respectively the Data Preparation phase and Data Elaboration phase, which are both part of the overall Data *Processing* procedure.

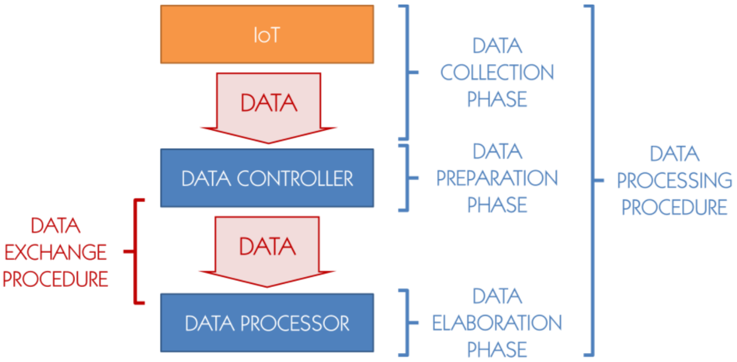


Figure 3. Overview of data-related procedures.

The following instructions are formalized to cover all data-related procedures:

- **Data Collection Phase**
  - VPP4IBoxes data collection details (to be technically defined)
  - VPP4IPlatform data collection details (to be technically defined)
  - Smart contract data management details (to be technically defined)
  - Hybrid Authentication and Auhorization Infrastructure (to be technically defined)
- **Data Preparation Phase**
  - Pseudonymization: the *Data Controller* shall adopt 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. This task will be done by the Data Controller in the event that there is a written agreement by which the Data Processor cannot receive personal identifiable data.

  - Password-protection: in order to secure the Data Exchange Procedure, data transferred as archive files (e.g. .zip/.rar) shall be protected by a password exchanged only between the Data Controller and the Data Processor as indicated in the DPR.

- **Data Elaboration Phase**
  - Any (and all personally identifiable) information will be either pseudonimized or anonimized by any Data Processing module before being transferred to the GUIs so as to ensure that no reidentification is possible. In the event that as result of the previous written agreement between the task of data anonymization or pseudonymization is assigned to the Data Controller, then if the Data Processor receives identifiable Personal Data from the Data Controller, the Data Processor will: (a)return or destroy the received data; (b) raise an incidence to the Data Controller and the DPO about this fact and (c) request for an anomimyzed version of the data.
  - Any data that is not strictly necessary for the elaboration carried out by Data Processing components (e.g. for monitoring and/or enforcement of security/privacy policies) should be automatically discarded by the component itself.

For all the aforementioned phases (and elaboration in particular), the following general principles, restrictions and solutions also apply:

- **Access control to premises and facilities**
  Unauthorized access (in the physical sense) must be prevented.
  Technical and organizational measures to control access to premises and facilities, in particular to check authorization, shall be implemented, e.g.:
  - Access control system (ID reader, magnetic card, chip card)
- **Access control to systems**
  Unauthorized access to IT systems must be prevented.
  Technical (ID/password security) and organizational measures for user identification and authentication shall be implemented:
  - Password definition procedures (incl. special characters, minimum length, expiration)
  - Automatic blocking (e.g. password or timeout)
- **Access control to data**
  Activities in IT systems not covered by the allocated access rights must be prevented.
  Requirements-driven definition of the authorization scheme and access rights, and monitoring and logging of accesses, shall be implemented:
  - Differentiated access rights (profiles, roles, transactions and objects)
  - Reports regarding accesses and access attempts
- **Disclosure control**
  Aspects of the disclosure of Personal Data must be controlled: electronic transfer, data transport, transmission control, etc.
  Proper measures to transport, transmit and communicate or store data on data media (manual or electronic) and for subsequent checking must be implemented:

The VPP4Islands project has received funding from the European Union's Horizon 2020 research and innovation programme under GA No. 957852

  - Encryption/tunneling (VPN = Virtual Private Network)
  - Transport security
- **Input control**
  Full documentation of data management and maintenance must be maintained.
  Measures for subsequent checking whether data have been entered, changed or removed (deleted), and by whom, shall be implemented:
  - Logging and reporting systems employed
- **Job control**
  Commissioned data processing must be carried out according to instructions.
  Measures (technical/organizational) to segregate responsibilities shall be implemented:
  - Unambiguous wording of the internal guidelines and logs (see DPR and DPL above)
  - Receiver must follow Controller's directions and guidelines when storing and granting access to the Personal Data
- **Availability control**
  The data must be protected against accidental destruction or loss.
  Measures to assure data security (physical/logical) shall be implemented and documented:
  - Backup procedures ensuring regular backups
  - Mirroring of hard disks, e.g. RAID technology
  - Uninterruptible Power Supply (UPS)
- **Segregation control**
  Data collected for different purposes must also be processed separately.
  Measures to provide for separate processing (storage, amendment, deletion, transmission) of data for different purposes shall be implemented:
  - Segregation of functions (e.g. production/testing)

The VPP4Islands project has received funding from the European Union's Horizon 2020 research and innovation programme under GA No. 957852