VPP4ISLANDS

Virtual Power Plants for Interoperable and Smart isLANDS

Deliverable Report D5.6

Deliverable ID	D5.6	**Version**	5.0
Deliverable name	Assessment of GDPR, standards and SSH compliance		
Lead beneficiary	Habib NASSER (RDIUP), Fatiha ZAOUIA (RDIUP), Dah DIARRA (RDIUP)		
Contributors	RDIUP, all partners through the questionnaire		
Reviewers	Stefano BIANCHI (ALWA), Dominic Heutelbeck (FTK)		
Due date	30/09/2021		
Date of final version	20/05/2022		
Dissemination level	Public/		
Document approval	Seifeddine Benelghali	**Date**	30/09/2021

Version	**Date**	**Authors**	**Actions**
V1.0	15-07-21	Inputs from RDIUP	To be improved
V2.0	10-09-21	Inputs from all partners via the survey	To be reviewed
V3.0	24-09-21	Inputs from ALWA and FTK	To include comments
V4.0	28-09-21	RDIUP	To be submitted
V5.0	20/05/2022	RDIUP	Update according to PO request

The VPP4ISLANDS project has received funding from the European Union's Horizon 2020 research and innovation programme under GA No. 957852

Executive Summary

The deliverable D5.6 presents the integration, implementation and verification of our data exchange and sharing, especially GDPR guidance, data privacy and protection. D5.6 aims to carry out the following activities:

- assess requirements and recommendations coming from Data management Plan (D1.2), and ethics requirements POPD (D9.2), existing standards (such as GDPR), regulation, existing funded European projects (e.g. DIY4U) and policies related to the VPP4ISLANDS solutions,
- propose an approach to verify, based on check-list, those normative requirements and recommendations and in the solution design
- initiate the GDPR guide in WP6 for the VPP4IPlatform.
- consider the users' needs, trends and requirements
- define a roadmap to ensure that the VPP4ISLANDS solutions (VPP4IBox, VPP4INode and VPP4IPlatform) are GDPR compliant

In this direction, several potential dissemination and exploitation activities can be performed. In particular, consortium members interested in launching VPP4ISLANDS flexibility services can benefit from the analysis of standards and regulatory requirements to evaluate early the feasibility of involving consumers in the pilot sites. This applies, among other things, to the following aspects :

- Regulations and standards overview
- GDPR compliance regarding
- Verification methodology based on check-list
- Best practices to ensure the compliance with GDPR-related requirements

Moreover, the legal environments between the EU and the UK and Turkey could diverge (during and after the project), that's why the main source of requirements in this deliverable deals with European and international regulations which are independent of the question of EU membership, hence, they will continue to apply to the UK and Turkey energy market as well.

In particular, this document intends to integrate privacy and data protection early by design. The various rules from the standardisation agencies and clusters regarding data protection in energy and digital systems will be considered. They will inform decisions affecting privacy versus utility during later stages of the project through the activities in WP8 "Networking and dissemination activities".

Table of Contents

List of abbreviations 4
1 Introduction 7
1.1 Objectives: 7
2 GDPR definition, and regulations overview 8
2.1 General Data Protection Regulation 8
2.2 European Union Agency for Cybersecurity 10
2.3 European Standard EN 17259 10
3 International information security and privacy standards 11
3.1 Security standard ISO/IEC 27001 & 27002 12
3.2 Privacy standard ISO/IEC 27701:2019 13
3.2.1 Lawfulness principle 13
3.2.2 Data pseudonymization 14
3.2.3 Data security 15
3.2.4 Data sharing, transfer and disclosure 16
3.2.5 Data subject rights 17
3.3 Information technology — Security techniques — Information security controls for the energy utility industry 19
4 Approach for the VPP4ISLANDS solutions 20
4.1 Adherence to regulations and standards 22
4.2 Privacy issues and possible solutions 25
4.2.1 Privacy policy: 25
4.2.2 User registration 25
4.2.3 CPU classification 26
4.2.4. SAPL for authentication and authorization (Task 5.5) 27
4.2.5. The blockchain technology (Task 5.3 and Task 5.4) 29
4.3. A Questionnaire for the GDPR and regulation compliance 30
5. Results of the questionnaire 32
6. Best practices: 54
7. Conclusion 55

Table of figures:

FIGURE 1. INFORMATION VS ANONYMITY 15
FIGURE 2. OUR DATA SHARING METHODOLOGY (SOURCE RDIUP) 16
FIGURE 3. DATA SUBJECT RIGHTS (SOURCE LAWINFOGRAPHIC) 18
FIGURE 4. DATA PROTECTION AND PROCESSING APPROACH (SOURCE RDIUP) 21
FIGURE 5. THE VPP4ISLANDS SECURITY ARCHITECTURE(SOURCE RDIUP: TASK 5.2) 22
FIGURE 6. THE PARALLEL CLASSIFICATION AND ANONYMIZATION OF DATA RECEIVED FROM RTUS (SOURCE AMU) 27
FIGURE 7. THE ARCHITECTURE OF THE SAPL (SOURCE FTK) 28
FIGURE 8. AN EXAMPLE OF A BLOCKCHAIN UTILIZATION 29
FIGURE 9. GDPR AND REGULATION COMPLIANCE QUESTIONNAIRE 31

List of tables

TABLE 1: LIST OF PARTNERS: 4
TABLE 2: GDPR PRINCIPLES 8
TABLE 3: SWOT ANALYSIS 53
TABLE 4: KEY BEST PRACTICES 54

List of abbreviations

AWI: Approved Work Item **CEN:** European Committee for Standardization **CENELEC:** European Committee for Electrotechnical Standardization **DLT**: Distributed Ledger Technologies **DMP**: Data Management Plan **DT**: Digital Twin **EN:** European Standard **GDPR:** General Data Protection Regulation **IEC:** International Electrotechnical Standardization Organization **ISO:** International Standardization Organization	**IT:** Information Technology **JTC:** Joint technical committee **KB:** Knowledge Base **POPD**: Protection of Personal Data **prEN:** Preliminary European Standard **RTU**: Remote Terminal Units **SC:** Sub-committee **TEE:** Trusted Execution Environment **TC:** Technical committee **VPP**: Virtual Power Plant **WG:** Working group

Table 1: List of partners:

No	Participant organisation name	short name	Country
1	AIX MARSEILLE UNIVERSITY	AMU	FR
2	AlgoWatt	ALWA	IT
3	SCHNEIDER ELECTRIC ESPANA SA	SCHN	ES
4	BLOCKCHAIN2050 BV	BC2050	NL
5	BRUNEL UNIVERSITY LONDON	BUL	UK

6	REGENERA	REGE	ES
7	CARDIFF UNIVERSITY	CU	UK
8	CIVIESCO ESCO	CIVI	IT
9	INAVITAS	INAVITAS	TU
10	INGENIERIA Y DISEÑO ESTRUCTURAL AVANZADO S.L.	IDEA	ES
11	RDIUP	RDIUP	FR
12	FORSCHUNGSINSTITUT FUR TELEKOMMUNIKATION UND KOOPERATION	FTK	DE
13	AGENCIA ESTATAL CONSEJO SUPERIOR DE INVESTIGACIONES CIENTIFICAS	CSIC	ES
14	TROYA CEVRE DERNEGI	TROYA	TU

	Participant organisation name	**short name**	**Country**
Lead Islands			
15	ULUDAG ELEKTRIK DAGITIM A.S.: Gökçeada Island	UEDAS	TU
16	CONSELL INSULAR DE FORMENTERA: Formentera Island	FORM	ES

	Participant organisation name	**short name**	**Country**
Follower Islands			
17	BORNHOLMS VARME A/S: Bornholm Island	BEOF	DK
18	BOZCAADA BELEDIYE BASKALIGI: Bozcaada Island	BOZI	TU
19	GRADO MUNICIPALITY	GRADO	IT

Terminology of the deliverable

Actor: A logical component of Smart Grid or Smart Metering systems on which Personal Data can reside.

Cyber security: All activities necessary to protect network and information systems, their users, and affected persons from cyber threats[1]

Data Controller (GDPR, Art. 7). Any entity which separately or jointly with others, determines the means and purposes of personal processing data.

Data Processor (GDPR, Art. 8). Any entity which processes personal data on behalf of the controller. Consent (GDPR, Art. 11). It is the freely given data subject's agreement for the processing of his/her data.

DPO - Data protection officer is a person whose task is to ensure that the processor and controller are compliant with GDPR (can be a company employee or an external person). It is necessary when processing operations require regular and systematic monitoring of data subjects on a large scale (GDPR, Art. 37).

Personal data. According to GDPR "Personal data is any information which is related to an identified or identifiable natural person". Identifiers are attributes that allow to directly or indirectly identify a person: name, location information, identification number, online identification number. There is a subcategory of personal characteristics called "sensitive personal data" which are subject to more restrictive security; it includes genetics, biometric, health data, racial and ethnic origin, political, religious or ideological convictions or trade union membership. The lifetime of personal information is from a person's birth to the person's death; only data that belongs to living persons is under the protection of the personal data law.

Privacy: The right to be left alone and includes elements of protecting private life such as integrity of a person's home, body, conversations, data, honour and reputation pursuant to Article 7 of the Charter of Fundamental Rights of the European Union.

Processing. Any operation which uses personal data or sets of personal data.

Scenario: A possible sequence of interactions within a Use Case i.e. one of the possible routes in the description of a sequence of steps that compose a Use Case. A Scenario is described as a sequence of activity steps, each of them involving an activity performed by an Actor or other component, or an interaction between components [SG-CG/M490/E].

Use case: A specification of a set of actions performed by a system (for example an IT system that is involved in VPP), which yields an observable result that is, typically, a value for one or more Actors or other component of the system. [SG-CG/M490/F].

Vulnerability: The Vulnerability of a Supporting Asset is a weakness that can be exploited by one or more Threats.

[1] Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act''), Art. 2.

1 Introduction

The deliverable D5.6 reports on the standards and regulations relevant for the VPP4ISLANDS digital solutions to be addressed in the upcoming development cycles, the GDPR document aims to elaborate best practices and identify lessons learnt throughout the ongoing project lifetime. A first evaluation has been carried out till Month 8 through a questionnaire to report on how technical partners, pilot sites (mainly leading islands), the available digital solutions and the proposed platform meet GDPR and other relevant regulations. Furthermore, this deliverable serves as a basis for the VPP4IPlatform and VPP4INode design which will be detailed in Deliverable D5.6 to report on how proposed design meets relevant regulations.

The main methodology on which this document is based is legal research[2]. Moreover, we will take a first look on the data management plan defined by AMU and RDIUP in D1.2. We will analyze typical issues regarding privacy that may occur in such systems and discuss some of the solutions that exist today.

Existing European and international standards, regulations and policies revolve around the topics of cybersecurity and data protection will be presented. Mainly, the General Data Protection Regulation (GDPR) sets down its principles in its Article 5. However, several legislative acts and standards provide further detail on requirements and recommendations concerning the digital components of the VPP4ISLANDS platform and energy information system.

The structure of the D5.6 includes: Firstly, providing an overview over regulation, standards and policies across Europe in Section 2, then, Section 3 assesses cybersecurity, and information privacy requirements at European and international level. Section 4 provides a specific approach in the VPP4ISLANDS that addresses the requirements previously analyzed. Section 5 presents the questionnaire's answers and a short evaluation of the consortium GDPR compliance. The best practices will be showcased in Section 6. Finally, conclusions will be provide in Section 7 for this deliverable D5.6.

1.1 Objectives:

This deliverable aims to describe how VPP4ISLANDS meets the requirements for GDPR. The following steps should be carried out:

- Regulatory overview,
- GDPR definition, rights and obligations required and applicable in the VPP4ISLANDS ecosystem
- Methods and techniques to verify GDPR implementation in VPP4ISLANDS

[2] Pocs, M., "Will the European Commission be able to standardize legal technology design without a legal method?" Computer Law & Security Review 28/2012, pages 641-650

- How VPP4ISLANDS solution design, especially WP5, respects the GDPR and other elated regulations

2 GDPR definition, and regulations overview

European and international regulations and standards consider the topics of data security and protection. At European level, the main sources of requirements are legislation and policy-making but also European standards. In this direction, several projects have worked in these topics and provided an overview of existing requirements such as DIY4U (A H2020 project where RDIUP is involved and responsible for updating a deliverable D2.7: DIY4U standardization and policies document relevant for the DIY4U platform to deliver D2.10 "DIY4U GDPR document based on DIY4U learning".

2.1 General Data Protection Regulation

The GDPR[3] defines a uniform set of legal requirements about personal data protection at European level. The main building blocks of the **EU Regulations and standards are summarized** in this subsection (based on definition in D2.7 and REGULATION (EU) 2016/679[4]) , since they are relevant for VPP4ISLANDS tools and platforms.

GDPR is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). The GDPR is an important component of EU privacy law and of human rights law, in particular Article 8(1) of the Charter of Fundamental Rights of the European Union. It also addresses the transfer of personal data outside the EU and EEA areas. The GDPR's primary goal is to enhance individuals' control and rights over their personal data and to simplify the regulatory environment for international business. Superseding the Data Protection Directive 95/46/EC, the regulation contains provisions and requirements related to the processing of personal data of individuals (formally called data subjects in the GDPR) who are located in the EEA, and applies to any enterprise—regardless of its location and the data subjects' citizenship or residence—that is processing the personal information of individuals inside the EEA.

Table 2: GDPR principles

Principles	Articles	details
Lawfulness and consent	GDPR Articles 5(1) and 6 to 8	require any processing of personal data to be based on a legal act, for example, consent by the data subject
protection for sensitive data	GDPR Article 9,	requires additional assurance of lawfulness and allows EU Member States to deviate from the uniform set of requirements that the GDPR provides
Data security	GDPR Articles 5(1)(f) and 32	Pursuant to these articles, a certain level of security needs to be ensured that corresponds to the level of risks for the data subjects

[3] General Data Protection Regulation

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Data subjects rights	GDPR Articles 5(1)(a) and 12 to 18	They include information about the processing of their data, notices, the need to collect data directly from the subjects, the right to data portability, information about the algorithmic logic, the right to access, correction, deletion and blocking of their data, as well as the right to be forgotten
Data protection	Article 25	The related requirements force organizations acquiring IT solutions to make the developers take certain measures for pseudonymization (mainly at VPP4I-Node level), data minimization and other privacy objectives (see GDPR Article 5(1)(c) and (e))
Limitation	GDPR Articles 5(1)(b) and 6(4)	Limitation and minimization of the amount of data that are processed and the duration of processing to what is necessary or at least compatible with the intended processing objectives at the time of data collection
Accountability	Articles 5(2) and 24(1).	It intends to respect certain requirements are not only responsibility anymore for adherence to the requirements but also need to "demonstrate" this.

In the case of the VPP4ISLANDS project, the requirements, needs, motivations and expectations expressed by the consumers are considered as personal data. So the scope of the requirements mentioned above applies to them. This includes any consumer's information, as follows :

- *Consumer registration data*: names and locations of data subjects, etc.
- *Usage data* (energy consumption, in particular household consumption, demand information and time stamps), as these provide insight in the daily life of the data subject.
- *Amount of energy and power* (e.g. kW) provided to grid (energy production), as they provide insight in the amount of available sustainable energy resources of the Data Subject.
- *Profile of consumers and users*, as they might influence how the consumer or prosumers is approached;
- *Facility operations profile data* (e.g. hours of use, how many occupants at what time and type of occupants).
- *Frequency of transmitting data* (if bound to certain thresholds), as these might provide insight in the daily life of the data subject.
- *Billing data* and consumer's payment method.
- *Needs of consumers* (e.g. comfort, ease of use, low Price, added value claims and Friendliness to the environment).

One of the requirements of the GDPR is the prohibition of so-called automatic decision-making (also called profiling). If the VPP4IPlatform and VPP4INode will be defined in a way that classifies people into certain consumer and prosumer groups this could be subject to additional measures that protect the interests of the data subjects. At this stage it is not yet carried out but early learning on energy needs and revenue streams point to different possible methods of classification of users, consumers or prosumers groups. Additionally, for further guidance, consider VPP processes that typically require processing Personal Data, thus, requiring the deployment of a GDPR assessment:

- Remote readings for billing purposes
- Frequent remote readings for network planning
- Dynamic and advanced tariffing Provide information to consumer online (e.g., Website, mobile App)
- Remote switching.
- Profiling of consumers (e.g. people interested in technology, ecologists, consumers looking only for prices),

2.2 European Union Agency for Cybersecurity

The European Union enacted legislation on network and information security[5] [6]. One of the agencies set up by this legislation is the European Union Agency for Cybersecurity (ENISA), formerly known as the European Network and Information Security Agency. This agency gives guidance on cybersecurity[7]. For example, ENISA gives guidance on pseudonymization techniques, including cryptographic hashes, data encryption, tokenization, masking and more[8]. This is in addition to the European Data Protection Board that is set up under the GDPR, which has also provided guidance on anonymization techniques[9]. The European Data Protection Board is composed by the national supervisory authorities for data protection.

The topic of pseudonymization and anonymization is relevant for the VPP4ISLANDS three layers (VPP4I-Box, VPP4I-Node and VPP4I-platform) see D2.4 “report on VPP4ISLANDS concepts”. The findings of [10]the will be fully by our consortium. Especially the energy services might lead to personal data relating to niche consumer groups. Hence, there is a risk of re-identification even if the main direct identifiers (e.g., name and address) are removed. The energy consumption that could lead to re-identification of consumers. Moreover, the identifiability of people is also increased by the usage patterns of different loads throughout all the day, which are needed for tailored services and scheduling for specific cases.

2.3 European Standard EN 17259

[5] Council Directive 2008/114/EC on the identification and designation of European critical infrastructure the assessment of the need to improve their protection, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32008L0114

[6] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

[7] European Union Agency for Cybersecurity (ENISA) guidelines available at https://www.enisa.europa.eu/publications/

[8] European Union Agency for Cybersecurity (ENISA), "Recommendations on shaping technology according to GDPR provisions - An overview on data pseudonymisation", 2019

[9] ARTICLE 29 Working Party on Data Protection (WP29, now: European Data Protection Board (EDPB)), "Opinion 05/2014 on Anonymisation Techniques onto the web (WP 216)," Brussels, 2014

[10] Blueprint Energy Solutions GmbH ”Final Report of a study on cybersecurity in the energy sector of the Energy Community” December 2019

In addition to regulation and policies, the European Committee for Standardization and the European Committee for Electrotechnical Standardization CEN-CENELEC JTC 13/WG 5 works on cybersecurity and data protection[11]. This group was created in early 2015 on the basis of European Commission Standardisation Request M/530 with the mission to develop a European Standard on "privacy by design"[12]. The committee is composed by European national bodies and a European consumer organization called ANEC. Managed by the German national body Deutsches Institut für Normung (DIN), the European Standard (EN) is still in the making.

The title of the standard is prEN 17529 'Data protection and privacy by design and by default[13]. The standard is intended for manufacturers and software developers providing products and services for the use as data controllers and for the use by controllers when they select their products and services for data processing. The standard would apply to future VPP4ISLANDS developments after the project.

The standard is based on the concept of a management system standard. At the time of submission of this deliverable, this European Standard is under development so its content cannot be considered final. However, the table of contents gives a good indication of the requirements and recommendations defined in this standard.
In addition to standards, European legislation came into effect - the so-called Cybersecurity Act (CSA) - that set up a certification framework. Accordingly, ENISA[14] can identify certain cybersecurity certification schemes to propose them to the several EU bodies for recognition as a European scheme under this framework. Currently, ENISA identified a candidate scheme based on Common Criteria which is to replace the certification scheme of SOG-IS MRA and to broaden the applicability to all EU Member States.

3 International information security and privacy standards

[11] CEN-CENELEC/JTC 13 'Cybersecurity and data protection', https://standards.cen.eu/dyn/www/f?p=204:7:0::::FSP_ORG_ID:2307986&cs=1E7D8757573B5975ED287A29293A34D6B

[12] European Commission Implementing Decision C(2015) 102 final, on a standardisation request to the European standardisation organisations as regards European standards and European standardisation deliverables for privacy and personal data protection management http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction= search.detail&id=548

[13] prEN 17529:2020 "Data protection and privacy by design and by default", June 2020 (CEN-CENELEC)

[14] https://www.enisa.europa.eu/

Apart from the European standards and regulations, there exists extensive international standardization on data security. The well-known 27000-series security standards[15] have been developed by the international committee ISO-IEC/JTC 1/SC27.

3.1 Security standard ISO/IEC 27001 & 27002

ISO/IEC 27001 is widely known, providing requirements for an information security management system (ISMS). Using them enables organizations[16] of any kind to manage the security of assets such as financial information, intellectual property, employee details or information entrusted by third parties. ISO/IEC 27001 requires that management systematically (1) examine the organization's information security risks, taking account of the threats, vulnerabilities, and impacts; (2) implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment and (3) adopt an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis. Based on the requirements and recommendations of ISO/IEC 27001[17], ISO/IEC 27002 defines measures - so-called "controls"[18]. These controls cover topics such as: Training of staff, Non-Disclosure Agreements (NDA), Mobile device security (teleworking), Staff privacy, Information classification, Secure media handling, Access and authorization control, User rights management, Cryptographic controls, Equipment security, Anti-malware protection, Backups, Logging (audit trails) and Network/communication security.

Those controls are mainly relating to security. However, there are some controls that are of special importance for privacy, such as the security controls (clauses 6) related to:

- *Responsibility*: including information and communication technology supply chain,
- *Data protection by design*: through the system change control procedures, a technical review of applications after operating platform changes, restrictions of changes to software packages, a secure development environment and a system security testing,
- *Accountability*: that considers the intellectual property rights, regulation of cryptographic controls and compliance with security policies and standards.

[15] ISO/IEC 27000:2018 "Information technology - Security techniques - Information security management systems - Overview and vocabulary"

[16] "Eight things organizations should do to ensure compliance with cyber security regulations, International standards can provide guidance and support for complying with regulations such as Europe's GDPR or California's CCPA" By Michael A. Mullane, 15 March 2020

[17] ISO/IEC 27001:2013 "Information technology - Security techniques - Information security management systems - Requirements"

[18] ISO/IEC 27002:2013 "Information technology - Security techniques - Code of practice for information security controls"

In the VPP4ISLANDS, this will be relevant when determining the recipient organizations and systems. In a B2B context, there could be several entities which will receive the personal data from the energy systems. These might include the following users:

- DSOs/TSOs
- Aggregators
- Energy Services Companies
- VPP operators
- Technology manufacturers
- Industrial companies

Moreover, the recipients may be other services and systems. Therefore, it is vital to monitor the evolution of the independent software modules of the VPP4ISLANDS solutions. Possibly these will include API modules, machine learning algorithms for profiling, carbon footprint calculation, digital twin (e.g. pre-design of existing portfolio), environmental modelling, enterprise blockchain infrastructure, rules engine, end-to-end encryption, dashboards, and so forth.

3.2 Privacy standard ISO/IEC 27701:2019

In this document, the privacy standard ISO/IEC 27701:2019 on privacy management[19] has been taken into account. This standard aims to support compliance with the GDPR. It includes roles of controllers and processors and the broad range of privacy requirements (data subject rights, data security, etc.). While ISO/IEC 29100 defines the privacy principles[20], 27701 focuses on the more practical aspect of privacy management. Some examples are given in this section.

3.2.1 Lawfulness and consent management

Article 4(11) of the GDPR[21] defines consent as: “any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.” The basic concept of consent remains similar to that under the Directive 95/46/EC and consent is one of the lawful grounds on which personal data processing has to be based, pursuant to Article 6 of the GDPR. 9 Besides the amended definition in Article 4(11), the GDPR provides additional guidance in Article 7 and in recitals 32, 33, 42, and 43 as to how the controller must act to comply with the main elements of the consent requirement. The consent is one of six lawful bases to process personal data, as listed in GDPR Article 6. To proceed personal data, there are various principles to be respected. Article 6 states the lawful purposes are:

[19] ISO/IEC 27701:2019 "Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines"

[20] ISO/IEC 29100:2011 "Information technology - Security techniques - Privacy framework"

[21] Article 29 working party “Guidelines on consent under Regulation 2016/679”

1. If the data subject has given consent to the processing of his or her personal data;
2. To fulfill contractual obligations with a data subject, or for tasks at the request of a data subject who is in the process of entering into a contract;
3. To comply with a data controller's legal obligations;
4. To protect the vital interests of a data subject or another individual;
5. To perform a task in the public interest or in official authority;
6. For the legitimate interests of a data controller or a third party, unless these interests are overridden by interests of the data subject or her or his rights according to the Charter of Fundamental Rights (especially in the case of children)

3.2.2 Data pseudonymization[22]

In VPP4ISLANDS, anonymisation techniques will be utilized before data was sent for analysis or if personal data is required in the analysis process, this process will be clearly defined in the privacy policy and already considered by our SAPL solutions (provided by FTK).
According to the GDPR (Articles 5 and 29, pseudonymisation is a required process for stored data that transforms personal data in such a way that the resulting data cannot be attributed to a specific data subject without the use of additional information (as an alternative to the other option of complete data anonymisation). For example the encryption technique, which renders the original data unintelligible in a process that cannot be reversed without access to the correct decryption key. The GDPR requires for the additional information (such as the decryption key) to be kept separately from the pseudonymised data. Pseudonymisation techniques (e.g. tokenization) also requires much fewer computational resources to process and less storage space in databases than traditionally-encrypted data. Therefore, the pseudonymisation will be done in powerful CPU and in cloud computing resources.

Pseudonymisation is a privacy-enhancing technology and is recommended to reduce the risks to the concerned data subjects and also to help controllers and processors to meet their data protection obligations. In VPP4ISLANDS pseudonymisation will be used before data analysis at the node-level and especially when encryption and anonymisation processes cannot be used. Moreover, Pseudo-anonymization could be a better approach if data mapping is kept by the same entity who has the data.

[22] https://en.wikipedia.org/wiki/General_Data_Protection_Regulation#Principles

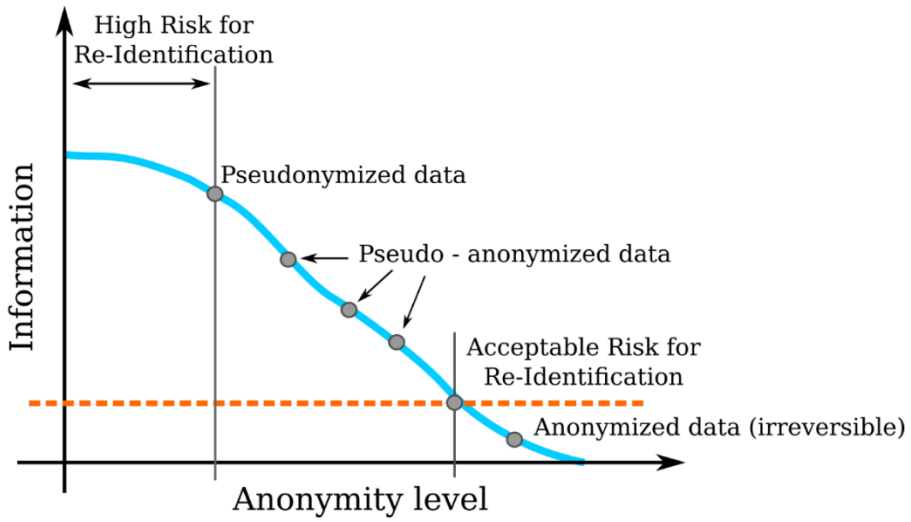

Figure 1. Information Vs Anonymity[23]

To summarize, General Data Protection Regulation (GDPR) makes clearly the difference between anonymization and pseudonymization. The main difference between these methods is that during the anonymization process the anonymized data is modified irreversibly (see Figure 1), while pseudonymization processes cannot prevent privacy breaches, as shown in the literature of medical data anonymization. The red line, in Figure 1, represents the threshold, where the re-identification of the anonymized or anonymous data is impossible.

3.2.3 Data security

Concerning the data security, ISO/IEC 27701 defines requirements and recommendations for a list of controls equivalent to the ones mentioned by ISO/IEC 27002 in the previous section of this document. One example that is more detailed in ISO/IEC 27701 is subclause 6.13.1.1, which explains responsibilities in data breach management. In subclause 5 "Response to information security incidents", it is recommended an incident that involves personal data to trigger a review by the organization, as part of its information security incident management process, to determine if a breach involving personal data that requires a response has taken place. This review is not done on every event, however. The clause also discusses the need to notify relevant authorities in cases of data breach, with a list of possible items that should be included in such a notification:

- contact point where more information can be obtained
- description of and the likely consequences of the breach
- description of the breach including the number of individuals concerned as well as the number of records concerned
- measures taken or planned to be taken

[23] Gergely Márk Csányi, Dániel Nagy, Renátó Vági, János Pál Vadász and Tamás Orosz "Challenges and Open Problems of Legal Document Anonymization" 13 August 2021 Symmetry by MDPI

3.2.4 Data sharing, transfer and disclosure

In relation to responsibilities in personal data sharing, ISO/IEC 27701:2019 Clauses 7.5 and 8.5 “PII sharing, transfer, and disclosure” state the objective to determine whether and document when personal data are shared, transferred to other jurisdictions or third parties and/or disclosed in accordance with applicable obligations.

To meet the overall objective on responsibility, several recommendations are given in ISO 27701. One example is the subclause 6.10.2.3 'Electronic messaging', which recommends, in the implementation guidance, the protecting messages against unauthorized access, change or denial of services in line with the organization’s classification schemes. Other examples of data sharing responsibilities are detailed in across the standard:

- Inform the customer in a timely manner of the basis for personal data transfers between jurisdictions and of any intended changes in this regard, so that the customer has the ability to object to such changes or to terminate the contract (clause 8.5.1)
- Specify and document the countries and international organizations to which personal data can possibly be transferred (clauses 7.5.2 and 8.5.2)
- Records for transfers and disclosures (see subclauses 7.5.3, 7.5.4 and 8.5.3)
- Personal data disclosures (see subclauses 8.5.4, subclause 8.5.5)

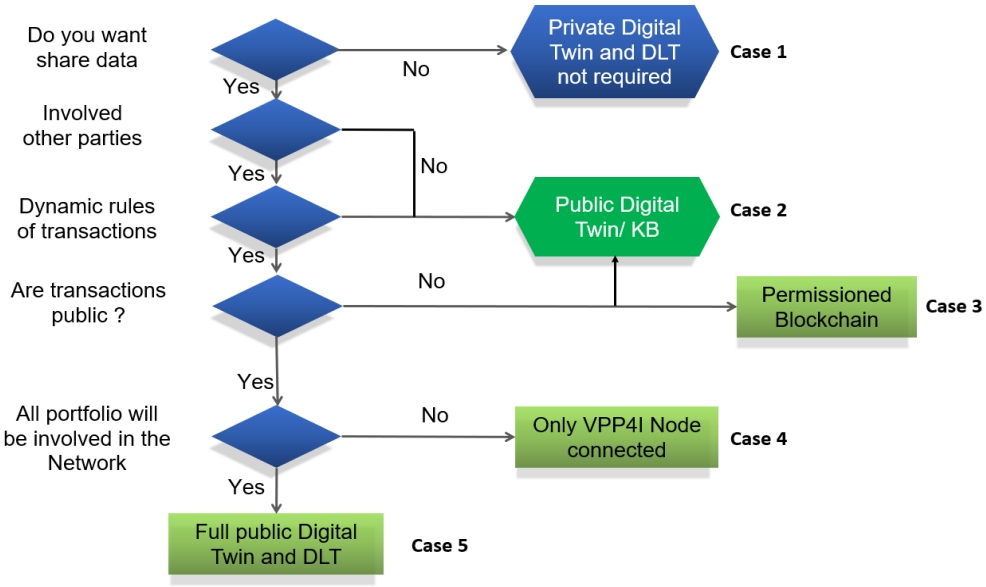

Figure 2. Our data sharing methodology (source RDIUP)

To maximize the data sharing protection, privacy and the large deployment of our solutions, VPP4ISLANDS, we have defined mainly 5 scenarios while considering that case 5 can represent a full trust configuration. Therefore, based on the needs of users we will have the following categories:

- Case 1: VPP4I-Nodes that don’t share their experiences with other VPP4I-Nodes (e.g. because of the presence of competitors). Then, they pay for the cloud-based services and improvements

coming from digital shadow, accurate forecasting and the KB of other users. The revenues of this category will be fairly distributed to the owners of KB taking into account the service provisions.

- Case 2: VPP4I-Nodes accept to share experiences but without involve other nodes in their portfolio. So as they participate in the elaboration of the shared KB, then they pay only for the digital twin services
- Case 3: VPP4I-Nodes accept to share experience, involve other nodes in their portfolio but with restricted transactions. So as they participate in the elaboration of the shared KB, then they pay only for the digital twin services.
- Case 4: Users accept to share experiences and transactions of only the main VPP4I-Node. They pay through the smart contract for the digital twin services and commission on transaction validated.
- Case 5: Fully optimized and flexible VPPs where end-users commit to share their experiences and knowledge with other Nodes and VPPs. As this project promotes the transparency and the open sharing of valuable data then this category will be rewarded for the flexibility offered in the network.

The sequence diagram presented in Figure. 2 will facilitate the sharing of data in a secure manner while verifying the consent of end-users and consumers. Moreover regarding to this diagram, Consumer-Permissioned Data (CPD) as an emerging model for data sharing between consumers and businesses (during exploitation and post-project commercialization phase) can be used in VPP4ISLANDS to allow consumers trading meaningful information in a secured way. That is quickly changing the way in which consumers can harness the power of their personal data in exchange for products and services. It is the potential to expand this model beyond fintech to offer consumer-permissioned data sharing for energy trading, energy communities building and digital twin creations.

3.2.5 Data subject rights

ISO/IEC 27701:2019 clauses 7.3 and 8.3 “Obligations to data subjects” state the objective to ensure that data subjects are provided with appropriate information about the processing of their personal data and to meet any other applicable obligations to data subjects related to the processing of their personal data. To meet the overall objective on data subject rights and participation, several recommendations are detailed in 27701.

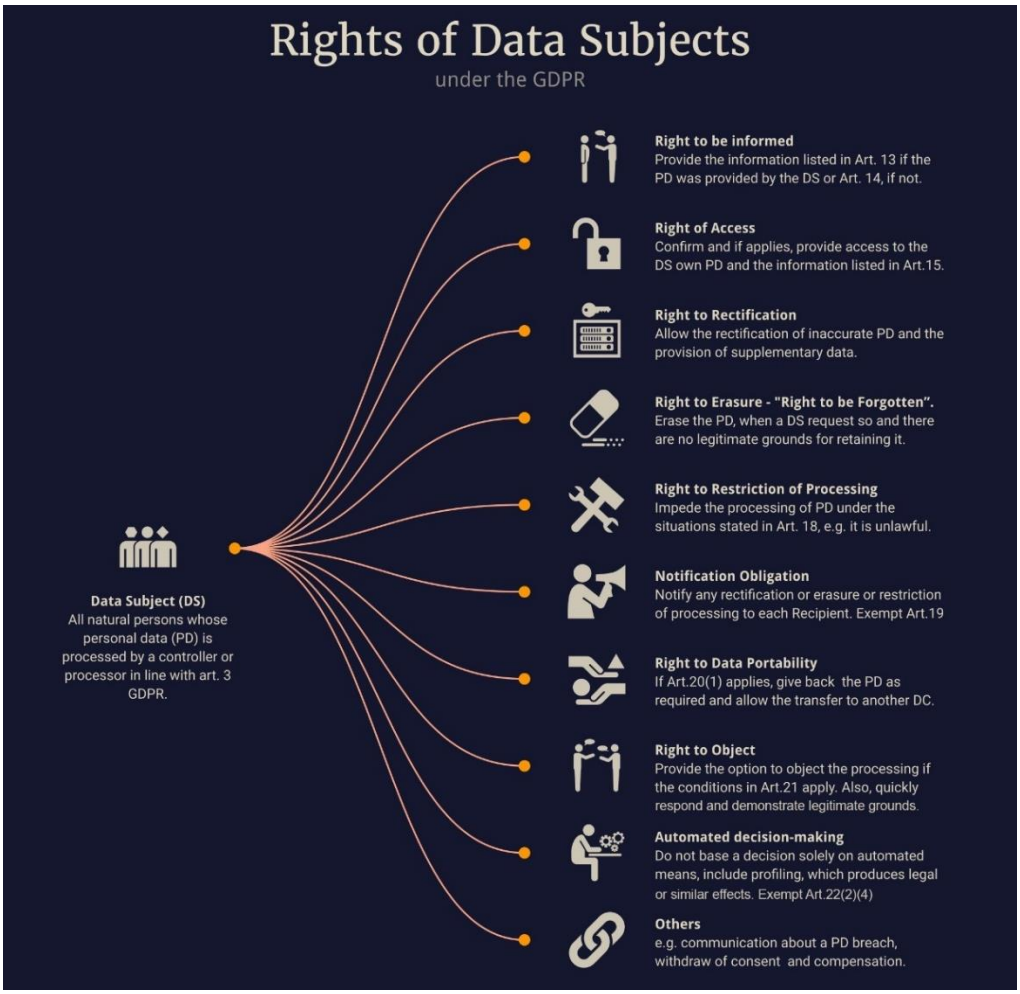

Figure 3. Data subject rights (source law infographic)

As listed in GDPR articles, there are 8 essential data subject rights to meet transparent information, communication and modalities for the exercise of the rights of the data subject stipulates. The principles regarding the processing of personal data, the lawfulness of processing (which is about those mentioned legal grounds, including consent), and the duties regarding the processing of special personal data categories, stretch much further than the data subject rights (see Figure. 3). However, when data subjects want to exercise one of those data subject rights – and have the right to – then the controller (and processors) need to be able to deliver upon it within the rule of the law (in this case the Regulation).

In GDPR, there are mainly 8 fundamental data subject rights.

- **The right of access** which means 1) the right to know whether data concerning him or her are being processed and 2) if so, access it with loads of additional stipulations (GDPR Article 15).
- **The right to rectification**: When personal data are inaccurate, then controllers need to correct them indeed (GDPR Article 16).

- **The right to erasure or right to be forgotten[24]:** individuals have the right to have personal data erased. This is also known as the 'right to be forgotten' (GDPR Article 17).
- **The right to restriction of processing:** Simply said, the right of the consumer or whatever you call the natural person under the scope of the GDPR, to limit the processing of his/her personal data with, once more, several rules and exceptions of course (GDPR Article 18).
- **The right to be informed[25]**: In general, the GDPR gives individuals a right to be informed about the collection and use of their personal data, which leads to a variety of information obligations by the controller (GDPR Article 19).
- **The right to data portability:** gives individuals the right to receive personal data they have provided to a controller in a structured, commonly used and machine readable format. It also gives them the right to request that a controller transmits this data directly to another controller (GDPR Article 20).
- **The right to object:** gives individuals the right to object to the processing of their personal data at any time. This effectively allows individuals to stop or prevent you from processing their personal data (GDPR Article 21)
- **The right not to be subject to a decision** based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. This is pretty much a copy and paste of GDPR Article 22, Paragraph 1, which ends the 'official' list of data subject rights.

3.3 Information technology — Security techniques — Information security controls for the energy utility industry

A specific ISO/IEC 27019:2017[26] provides guidance based on ISO/IEC 27002:2013 applied to process control systems used by the energy utility industry for controlling and monitoring the production or generation, transmission, storage and distribution of electric power, gas, oil and heat, and for the control of associated supporting processes. This includes in particular the following:

- central and distributed process control, monitoring and automation technology as well as information systems used for their operation, such as programming and parameterization devices;
- digital controllers and automation components such as control and field devices or Programmable Logic Controllers (PLCs), including digital sensor and actuator elements;
- all further supporting information systems used in the process control domain, e.g. for supplementary data visualization tasks and for controlling, monitoring, data archiving, historian logging, reporting and documentation purposes;
- communication technology used in the process control domain, e.g. networks, telemetry, telecontrol applications and remote control technology;

[24] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/#ib1
[25] https://gdpr-info.eu/issues/right-to-be-informed/
[26] https://webstore.iec.ch/preview/info_isoiec27019%7Bed1.0%7Den.pdf

- Advanced Metering Infrastructure (AMI) components, e.g. smart meters;
- measurement devices, e.g. for emission values;
- digital protection and safety systems, e.g. protection relays, safety PLCs, emergency governor mechanisms;
- energy management systems, e.g. of Distributed Energy Resources (DER), electric charging infrastructures, in private households, residential buildings or industrial customer installations;
- distributed components of smart grid environments, e.g. in energy grids, in private households, residential buildings or industrial customer installations;
- all software, firmware and applications installed on above-mentioned systems, e.g. DMS (Distribution Management System) applications or OMS (Outage Management System);
- any premises housing the above-mentioned equipment and systems;
- remote maintenance systems for above-mentioned systems.

The security techniques defined in ISO/ICE 27019 will be carefully considered by VPP4ISLANDS in order to comply with requirements and guidelines by establishing, implementing, monitoring, reviewing and, if necessary, improving the applicable measures set forth in this standard. That will allow to attain the specific security and business objectives of VPP4ISLANDS. It is important to give particular consideration here to the special role of the energy utilities in society and to the economic necessity of a secure and reliable energy supply. Ultimately, the overall success of the cybersecurity of energy industries is based on collaborative efforts by all stakeholders (vendors, suppliers, customers, etc.).

4 Approach for the VPP4ISLANDS solutions

Figure 4 describes how the VPP4ISLANDS meets the GDPR. It is a simplified version of the VPP4ISLANDS solution, and not all modules and details are visible. The first step to being compliant with the GDPR is to understand the rules, and in previous chapters, it was described what the main requirements for this regulation are. After following the requirements, the next step was designing the architecture with these rules in mind. In the VPP4ISLANDS, personal data is used based on the user's consent; because of this, acquiring consent is a mandatory step. In this paper are also given some small guidelines on what information should be listed in the privacy policy. Based on user consent, the three VPP4ISLANDS layers will use data only for purposes agreed by users and should ensure data privacy against any malicious or curious party that does not have the right to access data. Personal data is collected either when an account is created, or when an order is placed. Data protection is achieved either by personal data anonymisation techniques, or by cryptographic techniques (more details in following sections). VPP4ISLANDS uses a DLT solution that can achieve resilience, secure storage, transparency (for stakeholders with enough access rights over that data) and undeniable history. System functionalities utilize the underlying DLT layer; each functionality module needs to ensure personal data protection during the processing if the processed data cannot be anonymized.

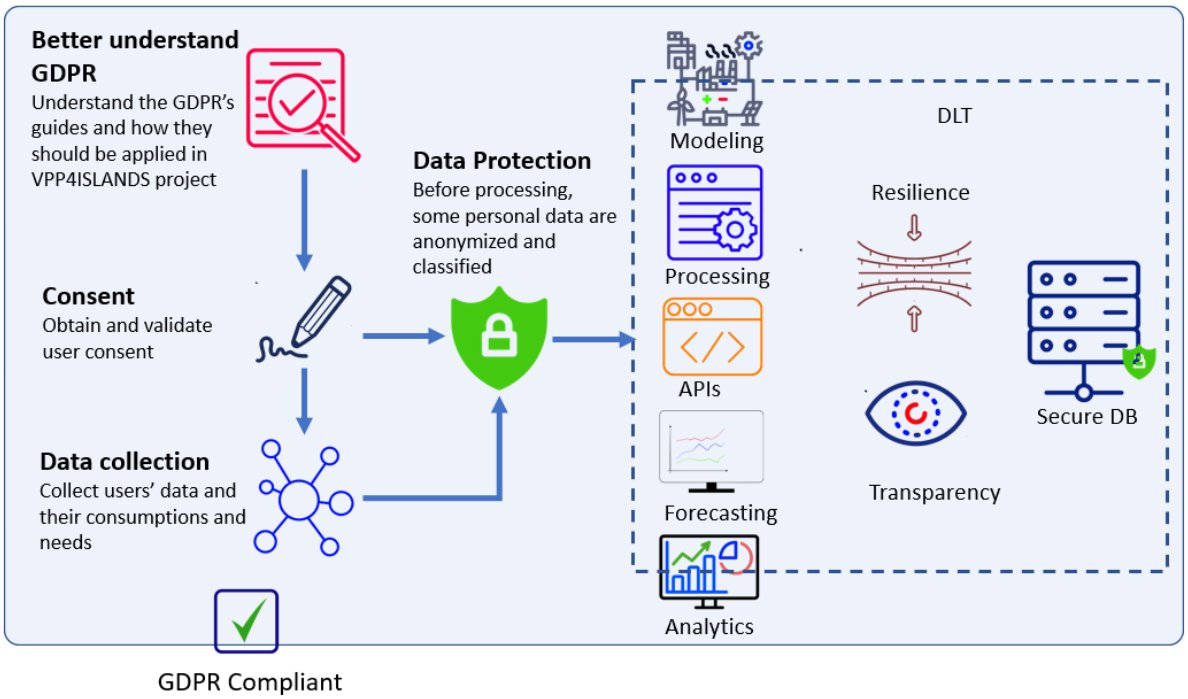

Figure 4. Data protection and processing approach (source RDIUP)

More specifically, the VPP4I-platform will incorporate a "digital twin" of energy systems which will allow users to obtain a copy of the existing portfolio and simulate specific scenarios, and using simulations and AI techniques, digitally test their behaviors, propose improvements and once the optimal VPP is achieved, send it back to the node-level to enhance the performance of the operating VPP.

Figures 4 and 5 present a high-level security architecture of the VPP4ISLANDS platform. Users will interact with the visualization components. A knowledge base stores behaviors that can be reused. A blockchain network stores intellectual property from different companies participating to the platform and ensures that it is secure. An AI and data analytics component are used to analyze and simulate digital versions of the user created formulations and propose modifications to the operators according to their preferences and the knowledge base.

To create their personalized solutions, the system requires users to share some personal information. This may include among others, a user's household composition (the number and ages of occupants, their occupation etc.), their shopping habits (e.g. the material or brands of their appliances), the consumption profile of energy (such as heavy use, ecologists), the user's location and time of year since different locations and seasons may have different requirements when it comes to energy consumption. Finally, a history of a user's previous bills is stored and may be required by the AI learning component.

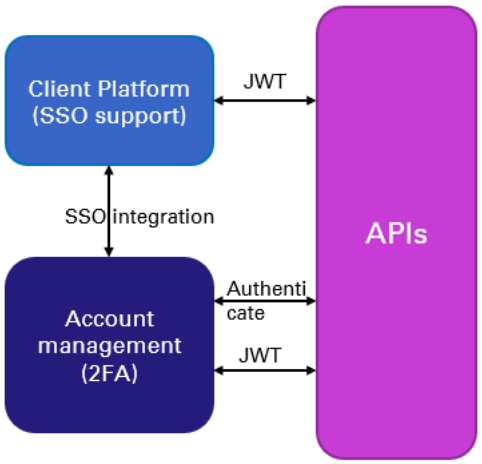

Figure 5. The VPP4ISLANDS security Architecture(Source RDIUP: Task 5.2)

To ensure that the information exchanged with the digital twin platform will be protected against any security issue, the connection will be encrypted using ECDSA encryption algorithm over a the HTPPS connection. All the Rest API endpoints exposed by the platform will be secured using a standard JSON (ISO/IEC 21778:2017) web token (JWT). Strict procedures will govern the expiration and the refresh of the JWT mitigating any possible threats that may occur. Using OAuth and SSO integration, the authentication may be performed using trusted external authentication providers, eliminating the need to keep any account detail on the platform level. Optionally the SSO providers may use two-factor authentication (2FA) or one-time password (OTP) mechanisms to enforce superior security level. To serve the needs of a multi-organization platform, the data exchange between the organizations that are already part of the trusted network will be governed by a federated blockchain network of boxes (participants). All the Extensions that are designed to operate within this environment will follow the governance rules of the network.

4.1 Adherence to regulations and standards

When registering to the system, a user will need to accept to the privacy policy of the platform. By registering, the user consents to the collection of relevant information about herself which will help with creating suitable products. However, the collected personal information can be used to identify them and extract information beyond their consent. The user needs to be given guarantees that the system will prevent such actions from occurring.

Privacy threats can be placed in two main categories.

1. Internal threats, where the adversary may be an active stakeholder within the system (users, server administrators etc.).
2. External threats, where the adversary is someone that is not involved within the system itself but attacks any possible vulnerabilities in order to gain valuable information. These threats can be performed by exploiting vulnerabilities on the application server to get access to the stored data. Or attacking the communications between user's and the system, or between the different parts of the system.

These threats can occur on multiple points within the data lifecycle. To reduce user exposure to these risks, the following principles as instructed by regulations such as the GDPR and the privacy by design paradigm will need to be considered when collecting and storing user data:

Data minimization which states that the amount of personal data that is collected needs to be restricted to the minimal amount possible that allows the system to provide the proposed functionality. When users register to the system, only relevant information for the registration purposes is collected. Additional information that may be desirable for the balancing or other functionalities of the platform should be collected from the users when required.

Cryptographic principles need to be applied when transmitting, storing and processing over personal data to ensure data confidentiality. More specifically, all communications between boxes, nodes and the platform, as well as between the different components of the platform need to be secured. Moreover, stored data at rest need to be encrypted. Finally, techniques for privacy preserving computations can be used when dealing with sensitive information.

Distribution of data across multiple locations. Additional to the distributed techniques for the computations discussed above, data at rest should also be distributed across multiple devices. This way if one location is compromised, a smaller amount of user data is at risk.

Data aggregation techniques should be used when processing personal data to ensure that the aggregated data contain the least possible level of detail while still being able to provide the proposed functionalities. Privacy Enhancing Techniques can be used for data anonymization. Such techniques include k-anonymity[27], l-diversity[28], t-closeness[29] and can be applied to the collected data before those are processed (or when required, published). Differential privacy[30] can also be considered. There exist several applications that take advantage of such techniques to protect user data[31] [32]. The ISO/IEC 20889:2018[33] standard provides a description of privacy enhancing techniques for data de-identification and anonymization.

[27] L. Sweeney, "k-anonymity: A model for protecting privacy", International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, vol. 10, p. 557–570, 2002

[28] A. Machanavajjhala, D. Kifer, J. Gehrke and M. Venkitasubramaniam, "l-diversity: Privacy beyond k-anonymity", ACM Transactions on Knowledge Discovery from Data (TKDD), vol. 1, p. 3–es, 2007

[29] N. Li, T. Li and S. Venkatasubramanian, "t-closeness: Privacy beyond k-anonymity and l-diversity", in 2007 IEEE 23rd International Conference on Data Engineering, 2007

[30] C. Dwork, "Differential Privacy", in Proceedings of the 33rd International Conference on Automata, Languages and Programming - Volume Part II, Berlin, 2006

[31] A. Kapadia, N. Triandopoulos, C. Cornelius, D. Peebles and D. Kotz, "AnonySense: Opportunistic and privacy-preserving context collection", Pervasive Computing, p. 280–297, 2008

User control over their data. Finally, users need to be in control of their personal data. They have the right to revoke their consent at any time and remove any data from the system. Moreover, the system needs to ensure users for the integrity of its different functions and that personal data is used only for the purposes the user has provided their consent.

As part of adherence to the GDPR a Data Privacy Officer (DPO) would need to be assigned. The main task of the DPO is to ensure that the platform processes any shared personal data in compliance with the data protection rules and privacy policy in place. Some of the DPO's responsibilities include the task of ensuring that any users are informed about the data that are collected and their uses, ensure data protection compliance within the platform, and help with accountability, handle queries and requests by users, manufacturers or third other third parties and more[34]. Moreover, user rights as they are defined in the GDPR need to be considered within the platform.

Adherence to the security and privacy standards ISO/IEC 27001, 27002:2013, and 27701:2019 can assist with GDPR compliance. The first one provides requirements for information security management systems (ISMS). Employing an ISMS, leads to a more comprehensive solution to secure data management. More specifically, the standard requires that information security risks, threats, vulnerabilities, and impacts should be systematically examined. A comprehensive suite of Information security controls that address the identified issues should be implemented and finally have a process which ensures that the implemented controls meet the security needs of the platform on an ongoing basis.

ISO/IEC 27002:2013 provides "guidelines for organizational information security standards and information security practices". It specifies security controls and their objectives for all different aspects within an information security management system. These controls are considered best practices for achieving the specified objectives.

Finally, the ISO/IEC 27701 standard is a privacy extension to the ISO/IEC 27001 mentioned above. Purpose of this standard is to provide guidelines in order to enhance an existing ISMS with additional requirements which aim at improving data privacy. The standard outlines a framework for managing

[32] K. V. et al., "Efficient algorithms for k-anonymous location privacy in participatory sensing", in IEEE INFOCOM, 2012

[33] ISO/IEC 20889:2018, "Information security - Privacy enhancing data de-identification terminology and classification of techniques"

[34] "European Data Protection Supervisor, "Data Protection Officer (DPO)", https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en

privacy controls and reducing the risk to privacy rights of the users when dealing with their "Personally Identifiable Information (PII)".

4.2 Privacy issues and possible solutions

Addressing privacy and data protection requirements in VPP4ISLANDS can be done through four main techniques, which are described in this section.

4.2.1 Privacy policy:

A GDPR privacy notice is an important way to help your customers make informed decisions about the data you collect and use. A privacy notice is a public document from an organization that explains how that organization processes personal data and how it applies data protection principles. Articles of the GDPR (12, 13, and 14) provide detailed instructions on how to create a privacy notice, placing an emphasis on making them easy to understand and accessible. VPP4ISLANDS must provide people with a privacy notice that is:

- In a concise, transparent, intelligible, and easily accessible form
- Written in clear and plain language, particularly for any information addressed specifically to vulnerable persons
- Delivered in a timely manner
- Provided free of charge

If a member from VPP4ISLANDS is collecting information from an individual directly, it must include the following information in its privacy notice:

- The identity and contact details of the organization, its representative, and its Data Protection Officer
- The purpose for the organization to process an individual's personal data and its legal basis
- The legitimate interests of the organization (or third party, where applicable)
- Any recipient or categories of recipients of an individual's data
- The details regarding any transfer of personal data to a third country and the safeguards taken
- The retention period or criteria used to determine the retention period of the data
- The existence of each data subject's rights
- The right to withdraw consent at any time (where relevant)
- The right to lodge a complaint with a supervisory authority
- Whether the provision of personal data is part of a statutory or contractual requirement or obligation and the possible consequences of failing to provide the personal data
- The existence of an automated decision-making system, including profiling, and information about how this system has been set up, the significance, and the consequences

4.2.2 User registration

Interested users who want to subscribe in the VPPs will need to register to the system first. During this step, some initial information about the user will need to be collected. This may include the user's email. Even though this is a very simple process, adversarial entities might be able to exploit the system for their own benefit. For example, a server administrator having access to the users' contact information, can find other applications that the user might have used the same contact and infer other sensitive information about her identity and interests. Therefore, registration information will need to be stored encrypted on the server. Very few works deal with privacy issues during the registration process.

During this process, a user ID may be generated for the user. This user ID can be used to track the interactions of the user with the platform. In the PRISM platform[35], Das et al. attempt to counteract this problem by introducing an expiration time for registrations where users will have to re-register after some predefined time. In their study, registration data include dynamically updated values such as their location, mobile phone battery status etc. The authors suggest that by using expiration time to registrations, users cannot be "tracked" by the server outside of the registration period. This type of solution however will greatly reduce the utility of the platform since users will lose access to their history when the registration time expires. Moreover, GDPR defines pseudonymisation as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person". Self-chosen, by the users, pseudonyms do not constitute pseudonymisation. Other techniques would need to be implemented. Such techniques may include cryptographic hashes, data encryption, tokenization, masking and more.

4.2.3 CPU classification

According to Global Data Protection Regulation (GDPR) any data containing personal information must be anonymized before going through any of the abovementioned interrelated processes in the VPP5ISLANDS. That is, in order to establish the required degree of trust in real persons who join the VPP, a certain level of security and privacy must be provided. Two common methods for this objective are anonymization and pseudonymization[36]. The former is the changing of personal

[35] T. Das, P. Mohan, V. N. Padmanabhan, R. Ramjee and A. Sharma, "PRISM: platform for remote sensing using smartphones", in Proceedings of the 8th international conference on Mobile systems, applications, and services, 2010

[36] S. Syed, M. Syed, H. B. Syeda, M. Garza, W. Bennett, J. Bona, et al., "API Driven On-Demand Participant ID Pseudonymization in Heterogeneous Multi-Study Research," Healthcare Informatics Research, vol. 27, pp. 39-47, 2021.

information so that the individual information about personal or material relationships can no longer be assigned to a certain person or determinable natural person or only with an unreasonably great expense of time, costs, and effort. The latter is the processing of personal data in such a way that the personal data or enlistment of additional information can no longer be traced to a specific person if this additional information is to be stored separately and is subject to technical and organizational measures which ensure that the personal data cannot be assigned to an identified or identifiable natural person. in pseudonymization, the data that would allow for identification are replaced with a code, for example. However, there is a separate key (e.g., in the form of a table) between the subject and the pseudonym, so that it is ultimately still possible to the re-identify the subject if one knows his key. In anonymization, however, all identifying characteristics are deleted. Due to re-identification possibility provided by the Pseudo-anonymization, it is the more commonly accepted approach.
In VPP4ISLANDS, we propose a novel pseudonymization method (see Figure 6) that can be parallelly exploited for VPP data. In this method, the unionized data are first classified into specific flows regarding their source and destination addresses. At this step, a unique flow number is associated to each installation. The corresponding part of data that includes personal information is encrypted and stored in a secure database with the flow number as the key.

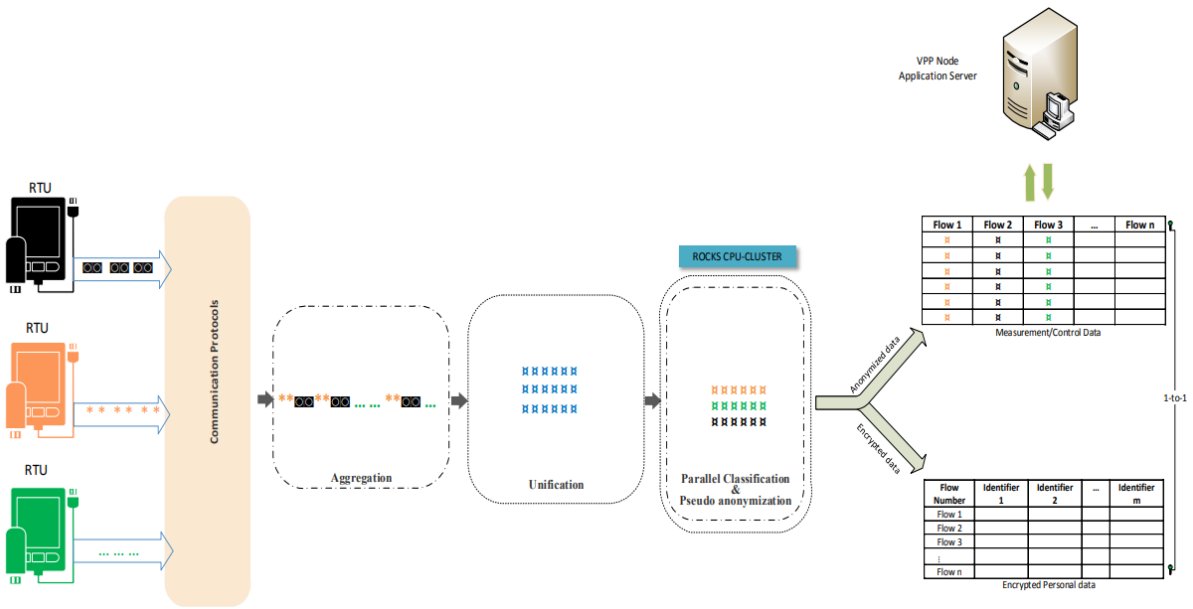

Figure 6. The parallel classification and anonymization of data received from RTUs (Source AMU)

Our parallel flow classification method classifies the Internet Packets (IPs) into certain flows according to address characteristics of their sender and receiver processes. While normalizing them for each stream, providing a certain level of access and confidentiality controls in the knowledge base of the VPP node. Figure. 3, illustrates this technique. Our method is based on the classification of internet flows (useful information and personal data).

4.2.4. SAPL for authentication and authorization (Task 5.5)

SAPL (Streaming Attribute Policy Language) describes both a domain specific language (DSL) for expressing access control policies and a publish/subscribe protocol based on JSON. Policies expressed in SAPL describe conditions for access control (see Figure 7) in applications and distributed systems. The underlying policy engine implements a variant of Attribute-based Access control (ABAC) which is enables processing of data streams and follows reactive programming patterns. Namely, the SAPL policy engine implements Attribute Stream-based Access Control (ASBAC).

A typical scenario for the application of SAPL would be a subject (e.g., a user or system) attempting to take an action (e.g., read or cancel an order) on a protected resource (e.g., a domain object of an application or a file). The subject makes a subscription request to the system (e.g., an application) for executing the action on the resource. The system implements a policy enforcement point (PEP) protecting the resources. The PEP collects information about the subject, action, resource, and potential other relevant data in an authorization subscription request and sends it to a policy decision point (PDP) which checks SAPL policies in order to decide whether access to the resource should be permitted as requested. This decision is packed in an authorization decision object and sent back to the PEP which accordingly either grants access according to the decision or prevents access to the resource. All data sources for the decision are subscribed to by the PDP and new decisions are sent to the PEP whenever indicated by the policies and data sources.

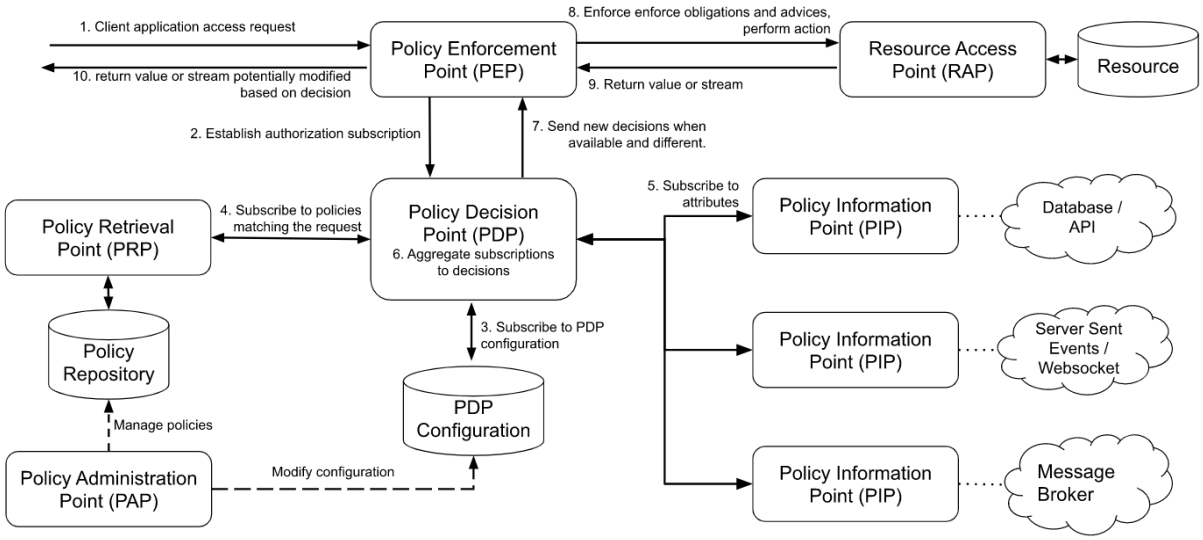

Figure 7. The architecture of the SAPL (Source FTK)

There exist several proprietary platform dependent or standardized languages, such as XACML for expressing policies. SAPL brings a number of advantages over these solutions:

- Universality. SAPL offers a generic, platform independent language for expressing policies.
- Separation of Concerns. Applying SAPL your domain model is relieved from modeling many aspects of access control.
- Modularity and Distribution. SAPL allows to manage policies in a modular fashion allowing the distribution of authoring responsibilities across teams.

- Expressiveness. SAPL provides access control schemata beyond the capabilities of most other practical languages.
- Human Readability. The SAPL syntax is designed from the ground up to be easily readable by humans.
- Transformation and Filtering. SAPL allows transforming resources and filtering data from resources (e.g., blacken the first digits of a credit card number, or hiding of birth dates by assigning individuals into age groups).
- SAPL is designed to offer low-latency authorization for interactive applications and data streams.
- Designed for a RESTful World with JSON. SAPL is designed to be easily integrated with modern JSON-based APIs.
- Supports Multi-Subscriptions. SAPL allows to bundle multiple authorization subscriptions into one multi-subscription thus further reducing connection time and latency.

4.2.5. The blockchain technology (Task 5.3 and Task 5.4)

This report aims to focus on WP5 The envisioned system makes use of distributed ledgers and the blockchain technology[37]. A blockchain is a distributed data structure that is shared among the members of a network (e.g. Figure 8). Essentially a blockchain is a ledger of timestamped blocks that each contain a list of "transactions". What constitutes a transaction depends on the type of application.

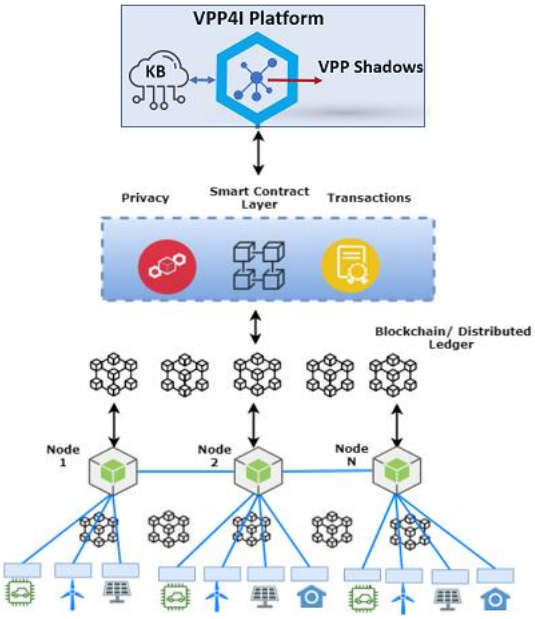

Figure 8. An example of a blockchain utilization

The use of a blockchain can offer several advantages.

[37] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2008

- It allows for completely decentralized systems, as it offers a robust and secure way to handle disputes and reach consensus.
- It is tolerant to node failures.
- It provides a method of data ownership without a central authority.
- In general, it enables a completely trustless network.

More specifically, in smart grids the characteristics of blockchains that make them appealing are that they enable secure, verified and trustable exchange of information in real time which is available to all members of the energy network and portfolio, and the possibility for automatic verification and execution of transactions with smart contracts. In the study[38], the authors discuss state of the art implementations of the blockchain technology within smart grids.

According to their findings, the most widespread implementation of blockchains is for verifying the origin of a product, and information about the path of products within the supply chain. Another application of the technology is in improved demand forecasting. Blockchains can assist with this process with their transparency since all members of the VPP or grids have access to the information contained within it. Moreover, blockchains can assist in peer-to-peer trading and with the use of smart contracts transactions can be automated. The added advantage of using blockchains is that there is no need to have a third party to act as intermediary (ESCO / Technology providers / Integrators) since smart contracts are self-executing.

Several blockchain implementations for smart grids are already available. The IBM blockchain[39] which allows the VPP members to get up-to-date information on the status and condition of their products throughout the lifetime of the value chain while keeping records of ownership and current location.

In VPP4ISLANDS proposes the blockchain as a tool to manage transactions in the smart grid. Transactions are performed with smart contracts (T5.3), and the network acts as a transaction verifier. The blockchain provides immutability of the transactions, which ensure every transaction between generators and consumers will always be executed. It also provides immutability to transaction history, which can be used for audit or solving a transaction dispute in a secure manner. Also, it should be noted that blockchains are public and not suitable for storing sensitive data since they are immutable, meaning that users who own the data will not be able to exercise their rights of deletion and modification. To comply with GDPR there will be no recording of personally identifiable information onto the blockchain. This information will be stored to external databases and the blockchain may contain links to it.

4.3. A Questionnaire for the GDPR and regulation compliance

[38] Anak Agung Gde Agung, Rini Handayani, "Blockchain for smart grid" Journal of King Saud University - Computer and Information Sciences, 2020,

[39] https://www.ibm.com/blogs/blockchain/2020/03/powering-trust-on-the-grid-with-blockchain/

Based on the sections 2 and 3 and discussions with key partners, we defined our verification technique based on a survey method, it is also useful to know some of the terminology and the basic structure of the law. Also, based on existing GDPR compliance techniques (e.g. https://gdpr.eu/checklist/), we proposed a first questionnaire to verify the GDPR and regulations compliance of our project VPP4ISLANDS at early stage. This survey will be improved and adapted during the project lifetime based on the feedback of all partners.

The questions illustrated in the Figure. 9 intends to verify compliance with standards and make a preliminary sweep of knowledge which will be used to enrich this very survey in the next phases. Subsequently, the updated survey will be distributed among the partners of the Consortium with the scope to be strengthened further. All questions refer to GDPR and regulations compliance based on their involvement in the data management. Here below the Questionnaire shared with all partners especially in WP5.

https://docs.google.com/forms/d/e/1FAIpQLSfVvRwbt3jrqIMO66x5w6mPk5KWfm7cRRdrS__EHlenEGJUBA/viewform

- Do you have a DPO? Name Him?
- How will you delete these data if you were asked to ? How will you check if all data was deleted?
- What type of data you have/plan to collect, use or treat ? Where data will be stored ?
- Are our team members are aware of the GDPR and security aspects ?
- What data you need to keep and which to let go ?
- What are you privacy policies ? Did you create a clear privacy notice for your tools ?
- How should people give their consent to you about using their data?
- Do you have an action plan in case of security breaches ?
- What data subject rights customers/users have under the GDPR ?
- Wich measures you have in place or implement to ensure that no one will leak, hack, or misplace users' data ?

Figure 9. GDPR and regulation compliance questionnaire

5. Results of the questionnaire

In the tables below, we represent the different questionnaire's answers and our recommendations to enhance the GDPR and regulation compliance for each partner.

Question 1: Do you have a DPO ? Name him ?

AMU	ALWA	SCHN	BC2050	BUL
ISAR Herve	Stefano BIANCHI	Dataprotection correspondent. cdpc.sp@se.com	Konstantinos Tsiomos	Dipa Gorsia
REGE	**CU**	**CIVI**	**INAVITAS**	**IDEA**
Mario José Lopez Romero	Meysam Qadrdan	NO	Tugçe Benek	NO
RDIUP	**FTK**	**CSIC**	**TROYA**	**UEDAS**
Habib NASSER	Jana Mertens	José López Calvo (delegadoprotecciondedatos @csic.es)	Oral Kaya	GOKSU SAFI ISIK ATTORNEY PARTNERSHIP
FORM	**BEOF**	**BOZI**	**GRADO**	
NO	SERVIA company	NO	the lawyer Paolo Vincenzotto	

For this first question, we invited and encouraged CIVI, BOZI, FORM and BOZI to name a DPO in order reinforce their GDPR compliance.

Question 2: what type of data you have/plan to collect, use or treat ? Where data will be stored ?

AMU	ALWA	SCHN	BC2050
Weather/ consumption and energy production. All data will be stored in AMU Datacenter.	Enery consumption and production data / profiles, from power system assets (e.g. DSO infrastructure) and from consumers/prosumers (e.g. energy community)	Pending to be further defined in the project. Possible measurements that could be collected by RTU and processed are: • Voltage [V] • Current [A] • Active power [kW] • Reactive power [kVAR] This data may be collected by RTU, but a copy of them	Blockchain2050 BV will acquire grid information such as power production, consumption, storing, transaction information between grid operators. All data will be stored in blockchain environments,

		is not kept in the RTU.	namely, Ethereum and LTO Network.
BUL	**REGE**	**CU**	**CIVI**
Computational models • Modelling and technical/operational design of a hybrid Regenerative Hydrogen Fuel Cell (RHFC) and Battery Energy Storage System. • Integrated renewable energy generation and storage system mathematical models (energy profiles, round-trip efficiency, LCOE, carbon-electricity impact) with optimization algorithms for effective Virtual Power Plant (VPP) design and deployment. • Modelling data informs energy system commissioning and site preparation, and overall optimised operation and maintenance aspects of the VPP4ISLANDS energy solution. Design information • Concentration of collected data on island's energy generation structures and power consumption profiles. • Energy consumption data from council owned buildings and anonymous commercial and residential buildings and privately owned power generators (this may require ethical approval process). • System's technical, environmental, and economical performance	The resources and files collected, used and treated must be controlled and stored as defined: - The processing centres and premises where the files are located or the media that contain them are stored. - The workstations, either local or remote, from which the files may be accessed. - The servers, if any, and the operating system and communications environment in which the files are located. - The computer systems, or applications established to access the data. - The files or databases containing personal data. The centres and premises where the files are located or the media that contain them are stored. - The cabinets, filing cabinets and devices where the files are kept when they are not being processed. - The structured manual file, i.e., the folders, files or dossiers containing the information by means of which the data is accessed.	Two types of data are considered – technology characteristics and operational data. Technology characteristics are essential Virtual Energy Storage System (VESS) assets data, such as energy storage system (ESS) and distributed generator (DG) capacities, and rated power of flexible loads. Operational data is divided into two parts, measurements and control signals. Measurement include, but are not limited to, power system frequency and voltages at selected busbars, in addition to measurements from ESS, flexible loads and DG. Control signals include the instructions issued by the VESS controllers to its components, and the signals sent by VPP4INodes and power systems operators to the VESS controllers. Data that will be used for simulation purposes will be stored on CIREGS ' secure data management system which is owned and managed by Cardiff team. During the test and implementation, some data will be stored at VPP4IBox level.	Feedback on energy services of the islands; data concerning the business models

and load-factor characteristics of the RHFC. • Literature support documentation on VPP system design, components, modelling, policies, etc. • Knowledge on social, regulatory, and technical barriers for implementation of VPP. • Operation & maintenance characteristics of the RHFC system. Operational information • Operation & maintenance data of the RHFC system. • Weather data (historic, real-time, and forecasted climate, weather, etc).			
INAVITAS	**IDEA**	**RDIUP**	**FTK**
We plan to collect and use consumption and production data (no personal data) of pilot sites. Data will be stored in our servers.	Data regarding the electrical grid and environment historical data	Consumption and production profiles, composition of VPPs, Prices, weather, forecasting, feedback	We do not plan to collect user data.
CSIC	**TROYA**	**UEDAS**	**FORM**
We are involved in the modelling engine for the digital twin. We will use power grid data (grid lines and transformers, consumption at the transformers, power plants characteristics, power plant production, line loads). Once deployed, data will be managed by the digital twin which will provide it to the modelling engine and store the results provided by our model. This data has been temporarily stored at IFISC	There are three main type of data. These are consumption or production data of Customers, renewable power plants and substations location on GIS System data	There are three main type of data. These are consumption or production data of Customers, renewable power plants and substations location on GIS System data and power grid data. Our IT system processes stored data in accordance with ISO 27001 Information Security Management System protocols.	Number and kW installed in each land. We prefer to have this data stored

computer servers and will be deleted once the digital twin is deployed. Files are stored in a ZFS filesystem with ACL and only IFISC researchers involved in VPP4ISLANDS have access to them.			
BEOF	**BOZI**	**GRADO**	
type of data: power/heat production data, on system level Storage of data: On local servers	We don't have a data plan.	• names for public meetings • names of people (individuals or company personnel) involved in the project	

As we will define a replication study for Bozcaada Islands, BOZI has to collect data about their existing energy systems to be decarbonized and energy community to be built. Therefore, BOZI has to define a clear data plan according to the GDPR guidelines.

Question 3: what data you need to keep and which to let go ?

AMU	**ALWA**	**SCHN**	**BC2050**
Personal data are not needed and will be not kept. Only the consumption, renewable energy production and weather profiles will be kept for research purposes	Energy consumption and production data will undergo Pseudonymization (GDPR Art.25) or Anonymization (GDPR Art.26), data will be associated to generic yet semantically significant personas / profiles and all personal data will be discarded.	As mentioned, real-time values will not be stored in the RTU.	Our purpose is not to keep data as we are responsible to just render them available for the purposes of information transaction between the project's partners.
BUL	**REGE**	**CU**	**CIVI**
Brunel SharePoint: Two-Factor Authentication login helps to stop hackers from getting into accounts, even if they have the password. •Local hard disk: Off-line backup stored in room accessible only by authorized personnel with physical key. Expertise/specialised knowledge: Non-Disclosure Agreement signed by	All information and reports required for the proper performance of staff duties shall be kept and protected. Other data will be deleted	Technology characteristics are fixed and continually used. In contrast, operational data are continually updated.	to be defined

students and staff that have access to the critical information.			
INAVITAS	**IDEA**	**RDIUP**	**FTK**
We need no personal data , we can use unlabelled consumption and production data.	The system will be stateless, will not store data within itself, only in the shared knowledge base	We will keep only analytic results, DR profiles, Knowledge and optimized VPPs	None
CSIC	**TROYA**	**UEDAS**	**FORM**
Once the digital twin is operational the data that has been stored at IFISC servers will be deleted. During operation it will be convenient to keep the digital twin data at the AMU servers for the duration of the project in order to be used for statistical analysis.	The information necessary for statistical evaluations, academic research will be kept and all the other data will be erased.	All data need to been kept, However the data can been accessible from authorized users.	To keep energy generated, installed kW and place of installation. None else.
BEOF	**BOZI**	**GRADO**	
Data will be kept, for system modeling and research	We don't collect data.	Data which will be kept: • personal data • geographical location • electric consumption	

As AMU is the responsible for the VPP4I-Node and CPU classification, it decided to not store personal data and keep only useful anonymized information. BOZI has to clearly define the data to be kept or to be deleted during the replication case.

Question 4: How should people give their consent to you about using their data? (Answer if you are concerned)

AMU	ALWA	SCHN	BC2050
According to Article 7 of GDPR, the consent must be informed, freely given and also be recorded. Hence, after presenting the information regarding the GDPR provision in the collected data, we may provide a mechanism based on smart contract to get the required consent.	By filling Informed Consent Form, as for Art.7 of GDPR	It is not defined yet if Schneider Electric RTU will make use of real-time values provided by devices associated to individuals or not. Those values could be associated to commercial buildings, DER facilities, and so on, and it is not clear if a	We are not handling any personal data or other that fall under the GDPR umbrella.

		connection with individuals will be made at this stage. In any case, all the relationship with the field installations (buildings, facilities, and so on), should be managed by the partners in charge of the demonstrator of the islands.	
BUL	**REGE**	**CU**	**CIVI**
The university's Ethical Approval process, enforced by the Information Commissioner's Office (ICO)	-We do not intend to use personal data. The acquiring of consent is the responsibility of Islands	How the data can be used is specified in the contracts between the VESS aggregator and the owners of ESS, DG and flexible loads.	to be defined
INAVITAS	**IDEA**	**RDIUP**	**FTK**
We are not concerned since we don't collect and use any personal data.	NA	Leading and followers Islands are responsible for consent acquiring	Not applicable
CSIC	**TROYA**	**UEDAS**	**FORM**
We do not intend to use personal data. The data indicated above is aggregated at least at the transformer level.	We have a Informed Consent Form which we use before conducting interviews. A copy can be supplied if requested.	The connection contracts or subscription contracts we have made with users contain articles that give the necessary permissions under the relevant law. In case of special situations such as this project, additional clarification text and an explicit consent form are signed.	We hope people will give their consent between an online form, or a physical form signed.
BEOF	**BOZI**	**GRADO**	
We will use data from smart meters at consumers	We don't collect data.	People sign the privacy notice called "information for personal data processing"; with this signature, they accept the use of their personal data within the project. The document contains the information required by the GDPR and by the Italian legislation (D.Lgs. 196/2003).	

For the replication cases and to be able used the consumers' data (e.g. smart meters etc..), BOZI and BOEF have to define early a consent form according to the GDPR Art.7.

Question 5: What data subject rights customers/users have under the GDPR ?

AMU	ALWA	SCHN	BC2050
Data subjects have a right to withdraw their consent at any time. They should be informed of this right before giving consent, and the withdrawal should be as easy as giving consent.	At the most essential level and technically speaking, there are 8 essential data subject rights as listed in GDPR Arts. 15 until 22 (as GDPR Art. 12 on transparent information, communication and modalities for the exercise of the rights of the data subject stipulates).	Those rights as per Schneider Electric policies are detailed in the following website: https://www.se.com/ww/en/about-us/legal/data-privacy.jsp	NA
BUL	**REGE**	**CU**	**CIVI**
The right to be informed about the collection and the use of their personal data. The right to access personal data and supplementary information	In addition to the person in charge of the REGENERA LEVANTE, S.L. files, the personnel affected by this regulation could be classified in some of the following categories: - System administrators, responsible for administering or maintaining the operational environment of the files. Their functions may involve the use of administration tools that allow access to protected data by bypassing the access barriers of applications or information systems. - Data Processor, is the natural or legal person, public or private, or administrative body, who alone or jointly with others, processes personal data on behalf of the Data Controller, as a consequence of a legal relationship. - Users of the files, or personnel who usually use the computer system for access to the files. - Other persons from outside companies who, by reason of their professional activities, may potentially have access to	Some of the data may be subject to GDPR, but these data can be anonymised.	to be defined

	personal information. Staff, whether in-house or external, shall only have access to those data and resources that they require for the performance of their duties. Only personnel expressly authorised by the person responsible for the files may have access to the data. From the moment of termination or change in the job, the corresponding user code shall be deleted so that it is no longer possible to access the data in the file with the same one.		
INAVITAS	**IDEA**	**RDIUP**	**FTK**
We don't use personal data of consumers.	NA	Right to be informed about the data use and the access to analytical results	Not applicable
CSIC	**TROYA**	**UEDAS**	**FORM**
To be defined	If personal data owners request information about collection and use their personal data from the Troya Environmental Association, they will be answered as soon as possible and within thirty days at the latest. In this context, personal data owners have the following rights: • to learn if their personal data has been processed, • to request information about how it has been processed, • to learn the purpose of processing of personal data and whether they are used appropriately for this purpose, • to learn about the third parties to whom personal data are transferred domestically or abroad, • to request correction of personal data in case of incomplete or incorrect processing and to request notification of the transaction made within this scope to third	Customers have “Customer name, address, ID number list” and “customer energy usage data” subjects rights under GDPR.	Parcel identification and owner.

	parties to whom personal data are transferred, • to request the deletion or destruction of personal data in the event even it has been processed in accordance with the provisions of Law No. 6698 and other relevant laws, and to request the third parties to be informed, • to object to the occurrence of a result against the person himself by analysing the processed data exclusively through automated systems, • to demand the compensation of the damage in case of damage due to the unlawful processing of personal data. Personal data owners can direct their questions, opinions or requests to any of the following communication channels: E-mail: info@troyacevre.org, by writing to Kemalpasa Mah. Yali Cad. 59 / 7, Canakkale, Turkey. Troya Environment Association has the right to verify the identity before replying.		
BEOF	**BOZI**	**GRADO**	
We must inform consumers of what data we have stored that can be referred to them and for what purpose	We don't collect data.	At any time, the interested people have the right to access their personal data, to request its correction, updating and its cancellation. It is also possible to oppose to the processing and request its limitation. Interested individuals can obtain from the Data Controller access to their personal data, and request information related to how they are stored and processed. The interested parties have the right to claim to the Supervisory Authority - Italian Privacy Authority (https://www.garanteprivacy.it/) if they believe that the processing of personal data is not carried out as foreseen by GDPR.	

VPP4ISLANDS will include all rights defined in subsection 3.2.5. according to each activity. BOZI has been informed about these rights to be respected in relation to their replication case. CIVI has to define the right to be considered.

Question 6: How will you delete these data if you were asked to? How will you check if all data was deleted?

AMU	ALWA	SCHN	BC2050
We will provide the required functions to delete the user's data upon their request. The user data will be separated form consumption/production data using a flow-based methodology. Then, according to the user consent the personal data will be deleted before any process in the platform.	Permanent removal from DBs and File Systems.	As mentioned, real-time values will not be stored in the RTU.	Information stored in blockchain environments cannot be deleted. Nonetheless, the data we are handling are unaffected by GDPR.
BUL	**REGE**	**CU**	**CIVI**
Shred paper documents, delete electronic records if requested or if out of date.	All computer waste of any kind that may contain information, or even obsolete computers themselves, shall be disposed or destroyed according to the following procedure: 1. As a general rule, computer waste must be removed and destroyed by the company in charge of data destruction. 2. Those paper reports that contain more sensitive personal data and are not bulky should be destroyed in a paper shredder. 3. If there is no paper shredding machine or if the reports are very bulky, they must be placed in confidential airtight containers to be delivered to a recycling company that guarantees their destruction by contract.	The targeted data will be erased from the storing location and any other recovery locations as well. Security checks will be performed to ensure that data restoration is not possible.	we will delete data from our cloud through specific commands

	4. All discarded hard disks and other removable media shall be formatted and handed over for re-use to the Security Officer. If they are not to be reused, they shall be formatted, if possible, and placed in the organisation's confidential containers to be handed over to the data destruction company. 5. In the case of obsolete computers, before they are donated, sold or given to other institutions, the security officer should be notified so that the hard disk can be formatted, or a special programme can be used to securely delete all data. If the computer is damaged and the formatting operation cannot be carried out, the hard disks must be disassembled and deposited in the recycling company's container for destruction.		
INAVITAS	**IDEA**	**RDIUP**	**FTK**
We can delete all the data on the server at the end of the project. end of the project.	NA	We use a REST-API and we send “delete” requests and receive an acknowledge	There is nothing to delete
CSIC	**TROYA**	**UEDAS**	**FORM**
Data to test the model stored at IFISC servers will be deleted by the system administrator once the digital twin has been deployed. Once the digital twin becomes operational all data handling, including data deletion, will be carried out by the digital twin itself (WP3, lead by IDEA).	We delete all the electronic files from all the computers and shred the hard copies (such as written surveys / questionnaires)	All documents are deleted or disposed by data officer accordance as PERSONAL DATA STORAGE and DISPOSAL POLICY scope of local GDPR laws.	TIC department.
BEOF	**BOZI**	**GRADO**	

If we chose to delete data, we will do so, and be able to document it has been done	We don't collect data.	Deletion requests may be addressed to the Municipality of Grado, with registered office in Piazza B. Marin in Grado (Go), e-mail: comune.grado@certgov.fvg.it The persons who are responsible for the verification are the DPO and the "Data Controller", who will enact the provisions foreseen by the GDPR for deleting the data.

Based on the right to erasure and to be forgotten, BOZI has to define a secure technique to delete the collected data.

Question 7: What are you privacy policies ? Did you create a clear privacy notice for your tools ? if yes, provide the main content of this notice

AMU	ALWA	SCHN	BC2050
The structure and the type of the data to provide a privacy policy is already determined in work package 2. In the relevant privacy notice, it is identified who the data controller is in each level and also the contact details for its Data Protection Officer are clearly specified. It is also explained the purposes for which personal data are collected and used in VPP4IBoxes, how the data are used and disclosed in VPP4INodes and in the platform; Also, how long it is kept, and the controller's legal basis for the processing. Already, all partners of VPP4IsLANDs have contributed to provide a privacy notice that is: In a concise, transparent, intelligible, and easily accessible form. The notice is Written in clear and with a plain language and will be delivered to users in a timely manner.	Privacy Policies for tools to be developed/integrated in VPP4ISLANDS still must be completely defined	Privacy policies at Schneider Electric are described in the following website: https://www.se.com/ww/en/about-us/legal/data-privacy.jsp Regarding the contribution for VPP4Islands project, Schneider Electric is not providing tools to be accessed by users of the platform, but RTUs, which are devices to be deployed on the islands. As mentioned, all the relationship with the field installations (buildings, facilities, and so on), should be managed by the partners in charge of the demonstrator of the islands.	NA
BUL	**REGE**	**CU**	**CIVI**

This privacy notice explains how Brunel University London ("we", "our", "us") collects, uses and shares your personal data, and your rights in relation to the personal data we hold. This privacy notice concerns our processing of personal data of prospective students and applicants of Brunel University London ("you", "your"). Brunel University London is the data controller of your personal data and is subject to the General Data Protection Regulation (the "GDPR"). Our Data Protection Policy can be found here. Here the link of the privacy policies: https://www.brunel.ac.uk/About-this-website/Privacy-Policy-and-Copyright-Statement	Data transmission over the network, whether by e-mail, file transfer systems or web applications, is becoming one of the most widely used means of sending data, to the extent that it is replacing physical media. For this reason, they deserve special treatment since, due to their characteristics, they may be more vulnerable than traditional physical media. - All input and output of data by e-mail shall be carried out from a single e-mail account or address controlled by a user specially authorised. Similarly, if data is input or output via network file transfer systems, only one user or administrator shall be authorised to perform such operations. - Copies of all e-mails involving input or output of data shall be kept in protected directories under the control of the above-mentioned controller. A copy of files received or transmitted by network file transfer systems, together with a record of the date and time of the operation and the destination or origin of the file received or sent, shall also be stored in protected directories.	This issue will be determined later as the project proceeds.	We have a privacy policy that complies with the GDPR policy
INAVITAS	**IDEA**	**RDIUP**	**FTK**
We don't need a privacy policy since we don't use any personal data.	NA	We have a privacy policy in our website to be improved	We are not aware of this being relevant for our tools
CSIC	**TROYA**	**UEDAS**	**FORM**

Regarding the data stored temporarily at IFISC, servers are located on access controlled room. Data access on IFISC severs is controlled by ACLs at file level. IFISC has implemented a data protection policy according to which access to given data set is restricted to researchers involved in a specific research. Researchers with access to data must sign an specific agreement according to which they can only use the data for the specific research being carried out, must keep confidentiality, can not disclose any information to a third party and can not copy (any part of) the data by any means to any computer or device outside IFISC servers. Regarding the policies to be implemented once the digital twin is deployed this should be defined at the level of the entire digital twin or above. The modelling engine does not uses personal data and we do not foresee the need for any specific privacy note for the data used by it.	TROYA has Personal Data Protection and Privacy Policy which can be reached at: https://www.troyacevre.org/data-protection-and-privacy-policy/	We have defined our privacy policities under “ISO 27001 standarts” and “Turkish Commercial Laws”. The privacy notice is included in agreement of customers and both participations sign the agreement . The main contents are “protecting customers rights”, “protecting UEDAS rights” and “usage rights of customer data”	We don’t need privacy policies
BEOF	**BOZI**	**GRADO**	
Our team members has been tought the rules of GDPR	We don't need privacy policy .	The privacy notice foresees: 1 .Information on the processing of personal data 2. Identification of the Data Controller (and other subjects) 3. Purpose of the treatment 4. Type of personal data processed 5. Legal basis of the processing 6. Nature of the use of personal data 7. Methods, scope and duration of the processing 8. Scope of communication and dissemination of data 9. Rights of interested parties	

In order to enhance GDPR and regulation compliance, BC2050, CU, FTK, IDEA, and INAVITAS are invited to define a privacy policy as they develop digital tools and applications.

Question 8: Are our team members aware of the GDPR and security aspects ?

AMU	ALWA	SCHN	BC2050
Yes	Yes, the company DPO is also the VPP4ISLANDS WP2 leader and internal courses on GDPR are organized for compliance of algoWatt SpA to ISO27001 certification.	Data confidentiality and security are a paramount importance to Schneider Electric. Schneider Electric implements appropriate technical and organizational measures to ensure an adequate level of security for the personal data processed in order to prevent accidental or unlawful destruction, loss, alteration, unauthorized disclosure or unauthorized access. Schneider Electric staff undergoes training on information security and data protection. Personnel who may have access to confidential information are bound to confidentiality.	Yes
BUL	**REGE**	**CU**	**CIVI**
Yes	Yes	Yes	Yes
INAVITAS	**IDEA**	**RDIUP**	**FTK**
Yes	NA	Yes, we following webinars and MOOCs about GDPR	Yes
CSIC	**TROYA**	**UEDAS**	**FORM**
No	Yes	Yes they are. There are information in agreements between Participations and us.	Yes
BEOF	**BOZI**	**GRADO**	
Yes, we have a GDPR Plan	NO	Yes, some team members also took part to several specialization courses on GDPR	

To increase the GDPR awareness of the whole consortium, we will arrange meetings in WP6 about the GDPR compliance of the whole solution. CISC, IDEA and BOZI are invited to inform their team about the GDPR purposes and objectives.

Question 9: Do you have an action plan in case of security breaches ? if yes, provide some details about the corrective actions ?

AMU	ALWA	SCHN	BC2050

We must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. The main steps of action are as: 1. Notify the police, 2. Notify other affected businesses and any other necessary parties. 3. Call the police immediately, report your situation and note the potential risk for identity the 4. Analyze the breach and find the risky points 5. Exploit proper security methods to fix the problem 6. Test the upgraded security mechanism 7. Update the system and security consent procedure (if required).	Yes, as described in the Incident Management procedure included in the Integrated Information Management Sytem procedures, implemented within the ISO 27001 certification framework.	Schneider Electric's incident management program is designed to prevent, detect, and remedy incidents, including unauthorized access, disclosure, unavailability, and compromise of personal data. The Schneider Electric Security Operation Center (SOC) and regional security representatives oversee incident analysis and response in accordance with our Incident Management Procedure. Incident management teams identify the root cause of incidents and issue the required notifications to customers.	Based on discussions so far, we are implementing a permission based blockchain which translates into specific persons accessing it, and without the right permission any data retrieval is impossible
BUL	**REGE**	**CU**	**CIVI**
Yes. The Information Security Incident Management Data Breach Procedure (BUL-PROC-16.03) relates to all personal and special categories (sensitive) data held by the University regardless of format. This procedure sets out the action to be followed to ensure a consistent and effective approach is in place for managing data breaches and is aligned to the BUL ISMS information security incident management policy and procedure across the University. The objective of this procedure is to contain	An incident is any event that may occur sporadically and that may pose a danger to the security of the files, understood under its three aspects of confidentiality, integrity and availability of the data. Keeping a record of the incidents that compromise the security of the files is an essential tool for applying the necessary corrective measures, as well as making it possible to prevent possible attacks on that security and to prosecute those responsible for them. - An incident log shall be set up for the purpose of recording any incident that may pose a security risk. - Any user who becomes aware of an incident is responsible for recording it, if	This issue will be determined later as the project proceeds.	**NO**

any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches. When a breach is ongoing, every effort must be made to contain the breach. Containment is most likely to be necessary in cases where a breach is caused by a cybersecurity incident, such as phishing. Recovery takes place after the breach event has ended. This phase includes learning lessons from the breach and putting measures in place to try to avoid any similar breaches occurring in the future. In the case of simple email breaches (where an email containing personal data has been sent to the wrong individual), recovery will most often consist of requesting that the person or people who received the email in error, delete the email. Containment and recovery measures should be organised by the Data Protection Office (DPO) / Cyber and Information Security Manager (CISM). Notify the DPO of the breach before trying to recover from it. (For more information, please see: https://www.brunel.ac.uk/	the incident log is automated, or for notifying the Security Officer or immediate superior in writing, if the log is kept manually. - The knowledge and failure of a user to notify or log an incident shall be considered as a breach of the security by that user. - The notification or registration of an incident shall contain at least the following information: type of incident, date and time of occurrence, person making the notification, person to whom it is communicated, possible effects, detailed description of the incident		

about/documents/pdf/breach.pdf)			
INAVITAS	**IDEA**	**RDIUP**	**FTK**
Yes. We have a regular back up process.	NO	Yes, we are defining a corrective action in case of Cyber-attack by informing early all users and modifying token access to our Modules.	As a small organization, we have basic monitoring in place. Our Admin will shutdown services on detection. Once issues are resolved we go back online. All persons affected are informed immediately and leaks are disclosed where applicable.
CSIC	**TROYA**	**UEDAS**	**FORM**
IFISC servers storing data are not directly accessible outside IFISC VLAN. IFISC servers are continously monitored and periodically updated with the lastest security patches available. IFISC computer technicians will inmediate take action in case of a security thread to any server	Yes, we have a Data Breach action plan. For the full text can be supplied if requested. Some details are stated below: • Communications will be sent to the press, internal teams, and externally affected parties is necessary. • Assistance /advice of the legal advisor will be requested to draft messages /letters to ensure the optimal message is delivered at the right time. • All the stakeholders will be informed throughout the investigation, notification, containment, and recovery phases of a data breach. • Effective coordination with the stakeholders with be ensured. • An investigation team will be appointed according to the technical nature of the investigation and systems, networks, and data types. • If necessary, an outside expert team will be invited to deal with the matter. • When the issues identified, immediate action will	There is an Information Security Breach Procedure within the scope of ISO 27001. n case of a security breach, necessary actions will be taken according to the content of the breach.	Not needed

	be taken to contain them without disrupting the investigation or damaging any evidence. • The goal of containment is to stop the incident or the malware from spreading. At this step, the goal is not to remove or eradicate it. • When the problem is fully identified and understood, affected partied will be identified and notified. • Before and during notification process, a legal review will be asked if necessary. • The goal is to fully reverse the damage or remove the malware from the affected systems; it is not to fully recover those systems back into production. • Necessary processes such as upgrade and patch software, reinstall base operating system, set up and migrate to new hardware will be carried out. • Once the damage is eradicated, data can be restored • Steps include testing the restored and hardened systems, deploying them into production, monitoring systems for signs of incident reoccurrence, validating that the systems are fully recovered, and removing any unneeded containment measures. • Meetings will be held with staff to discuss the experience and exchange opinions. • The meeting should include a list of identified probable causes of any identifiable errors and recommendations. • A report will be prepared which includes the problem, timeline, actions taken and the results.		
BEOF	**BOZI**	**GRADO**	
We have an action plan in	We don't need a security plan.	Security breaches will be handled following	

case of security breaches		the procedures in use in the IT department.

As IDEA, CU and CIVI are developing digital modules in Box-Node and cloud levels, they have to define a security plan and corrective actions to avoid breaches risks.

Question 10: which measures you have in place or implement to ensure that no one will leak, hack, or misplace users' data ?

AMU	ALWA	SCHN	BC2050
The basic measures are as follows: 1. Consulting with legal security counsels 2. Securing gathered Data and processing Systems a. Determining the scope of breach b. Securing the relevant system/equipment c. Removing the breached data form the Internet 3. Notifying the relevant parties a. Determining obligation b. Notifying law enforcement c. Notifying users 4. Correct Vulnerabilities to Prevent Future Breaches	Information Asset Management procedures (including access to specific shared assets) are included in the Integrated Information Management System framework, implemented within the ISO 27001 certification framework.	The RTU includes cybersecurity features like Role-Based Access Control (RBAC), secured access through HTTPS and SSH, security events logging or blocking connections of specific ports & interfaces, that would difficult non-authorized users to access the content of the RTU.	Same as above question 9.
BUL	**REGE**	**CU**	**CIVI**
The Information Security Risk Management Policy (BUL-POL-IRM01) is essential to ensure that information, in whatever format, is provided the correct level of protection commensurate with its sensitivity and criticality to BUL business and operations. All staff undergo annual roll dependent compliance training for: - Data protection.	The security of the personal data in the files involves not only the confidentiality of the data but also the integrity and availability of the data. In order to guarantee these two fundamental aspects of security, it is necessary to have backup and recovery processes in place which, in the event of a computer system failure, allow the data to be recovered and, if necessary, reconstructed. There shall be a person, either the administrator, data	Only authorised people will gain access to data on the system and high security measures will be used.	we have no sensitive data

- Environmental sustainability. - Health and safety. - Information security.	processor or another specifically designated user, who shall be responsible for obtaining a regular backup copy of the files, for backup purposes and possible recovery in the event of failure. These copies shall be made at least weekly, except in the event that no update of the data has taken place. In the event of a system failure with total or partial loss of the data, there shall be a procedure, computerised or manual, which, on the basis of the last backup copy and the record of the operations carried out since the time of the copy, reconstructs the data to the state in which they were at the time of the failure. At least every six months the data controller shall verify the correct definition and operation of the backup and recovery procedures.		
INAVITAS	**IDEA**	**RDIUP**	**FTK**
Our data is unlabelled , we don't use any personal user data.	The system will live in a closed network within the VPP4I Platform	RDIUP deploys F2A, JWT and tokenization techniques.	We do not store user data in VPP4I. So nothing can be leaked.
CSIC	**TROYA**	**UEDAS**	**FORM**
At the physical level, IFISC servers are kept on a access controlled room. At the logical level, data access is controlled via ACLs at file level. As stated before following IFISC data protection policy, access to a data set is granted only to researchers involved on a specific research. Researchers with access to data must sign an specific agreement	TROYA take all necessary measures and show the necessary care to keep confidential information strictly private and confidential, and to prevent all or any part of confidential information from entering the public domain or unauthorized use or disclosure to a third party. All teams are fully trained regarding Personal Data Protection and Privacy Policy. Only Data Protection officer only has the password for the	Our company carries out information systems with an understanding of ISO27001 quality standard certificate. Within this scope, data is stored on the system, which is defined with special authorities for personnel such as data officers, and to which they can only login with their own user	Backup copy of data, once a month, TIC department.

according to which they can only use the data for the specific research being carried out, must keep confidentiality, can not disclose any information to a third party and can not copy (any part of) the data by any means to any computer or device outside IFISC servers.	data storage hard disk. All the hard copies (questionnaires / interviews) are kept under locked cabinet	names, and passwords. In order to prevent leaking of user data, procurement processes of applications such as DLP, Data Classification, DB Firewall, etc. have been started. Necessary measures will be taken with the applications taken.	
BEOF	**BOZI**	**GRADO**	
We have a data security plan that we follow, and we monitor if data leaks are taking place.	We use NDA for information exchange and we limit the sharing of critical information.	There are several layers of security in place, among which: • A perimetric firewall is active on all inwards and outwards connections. • A VPN is used to allow remote working. • IP restriction (VLAN) are enforced on the local area network. • Automated differential backups, with a retention period exceeding 6 months, are in place on dedicated local NAS, in a different building than the server. • Bare-metal recovery procedures are also available by means of VM backups. • All-important data are not only backed up, but also printed in hard copy. • Furthermore, there is also an insurance in place.	

At this stage, the questionnaire showcases that the project as a whole proposes appropriate plans and solutions to comply with GDPR, standards and regulations. Based on this survey, we noticed that the GDPR understating, awareness and compliance are satisfied. Moreover, to evaluate objectively the GDPR and regulation conformity of VPP4ISLANS, we decided to use the SWOT technique where we highlighted the strengths, weakness, opportunities and threats related to the GDPR and security issues. This assessment helps us increasing awareness and choose the suitable actions to improve the security of our solutions early by design.

Table 3: SWOT Analysis

STRENGTHS	WEAKNESSES

- VPP4ISLANDS develops solutions in WP5 that will enhance security and privacy (CPU classification, blockchain, SAPL) - Almost of our partners are aware about the importance of GDPR guidelines - Technical WP leader are integrating GDPR and security early by design - WP5 is providing disruptive solutions to increase security of data exchange.	- Same partners did not assign yet a DPO - Some digital provider partners don't have a privacy policy - Some partners' teams are not informed about the principles of GDPR
OPPORTUNITIES	**THREATS**
- Being a GDPR compliant will facilitate the exploitation and the replication of our solutions. - Raising of demand on secure and digital trust technologies - Increase needs of GDPR compliance software	- Not considering GDPR by demo Islands can complicate the building of energy communities - Not acquiring consents can also slowdown the implementation of our innovations especially in leading Islands

6. Best practices:

The application of the GDPR and privacy framework Template may be strengthened and its output maximized with the adoption of a set of ten good practices.

Table 4: **key Best practices**

Guidance and frameworks should be performed at an **early stage** (preferably during the design of new applications or systems);	DMP should **be adjusted** during a project (especially when Risks to Privacy and Personal Data are changing);
The verification and implementation of regulations must be carried out by a **multidisciplinary team** of experts who have both knowledge of the project/program and access to relevant expertise concerning Privacy and Personal Data;	GDPR verification should be **future oriented** i.e. should support the identification of Risks to Privacy and Personal Data before the usage of new applications or implementation of new programs;
It is better that GDPR verification be subject to **formal or informal control process** performed by external/independent persons	**The check-list** (questionnaire) should be short, clear and comprehensive
It is recommended to **involve relevant internal and external stakeholders** in the process, including the data subjects – where appropriate;	It is not advised to consider the verification as an ad-hoc or random or exercise, or to use it as **a static document**.

It is important to adopt quantified **KPI**s and define **corrective actions** in case of leakages or cyber-attacks.	It is recommended to be a part of an incentive **system of motivating**, sanctioning and controlling;

7. Conclusion

This deliverable D5.6 evaluated the data privacy and security requirements derived from European and international regulation, standards and policies relevant for the VPP4ISLANDS digital solution. The main techniques (SAPL, Blockchain, JWT, CPU classification etc ..) provided by our consortium mainly in WP5 will ensure security and anonymization of data (see section 4). In order to evaluate the GDPR and security compliance of our solutions, we defined a survey composed on 10 questions and arrange internal discussions. The questionnaire shown that VPP4ISLANDS is aware about GDPR requirements. Moreover, we suggest recommendations and 10 best practices to enhance the GDPR compliance.

When developing the VPP4ISLANDS solutions, it is crucial to take into account that it would involve multiple stakeholders each with different goals and motivations. Therefore, privacy and data protection should be considered from the design phase. There exist several solutions that implement the regulatory requirements and standards concerning data privacy in systems. In order to enhance the GDPR and regulation compliance, all partners are keen to consider the best practices and recommendations provided in sections 5 and 6. Some of the discussed solutions are already available (e.g. SAPL, CPU anonymization, JWT etc …) to be implemented for use in a real-world scenario. This will depend on finding the appropriate balance between privacy and utility. VPP4ISLANDS will keep verifying the GDPR and security compliance mainly in WP6 where the different solutions will be put together.