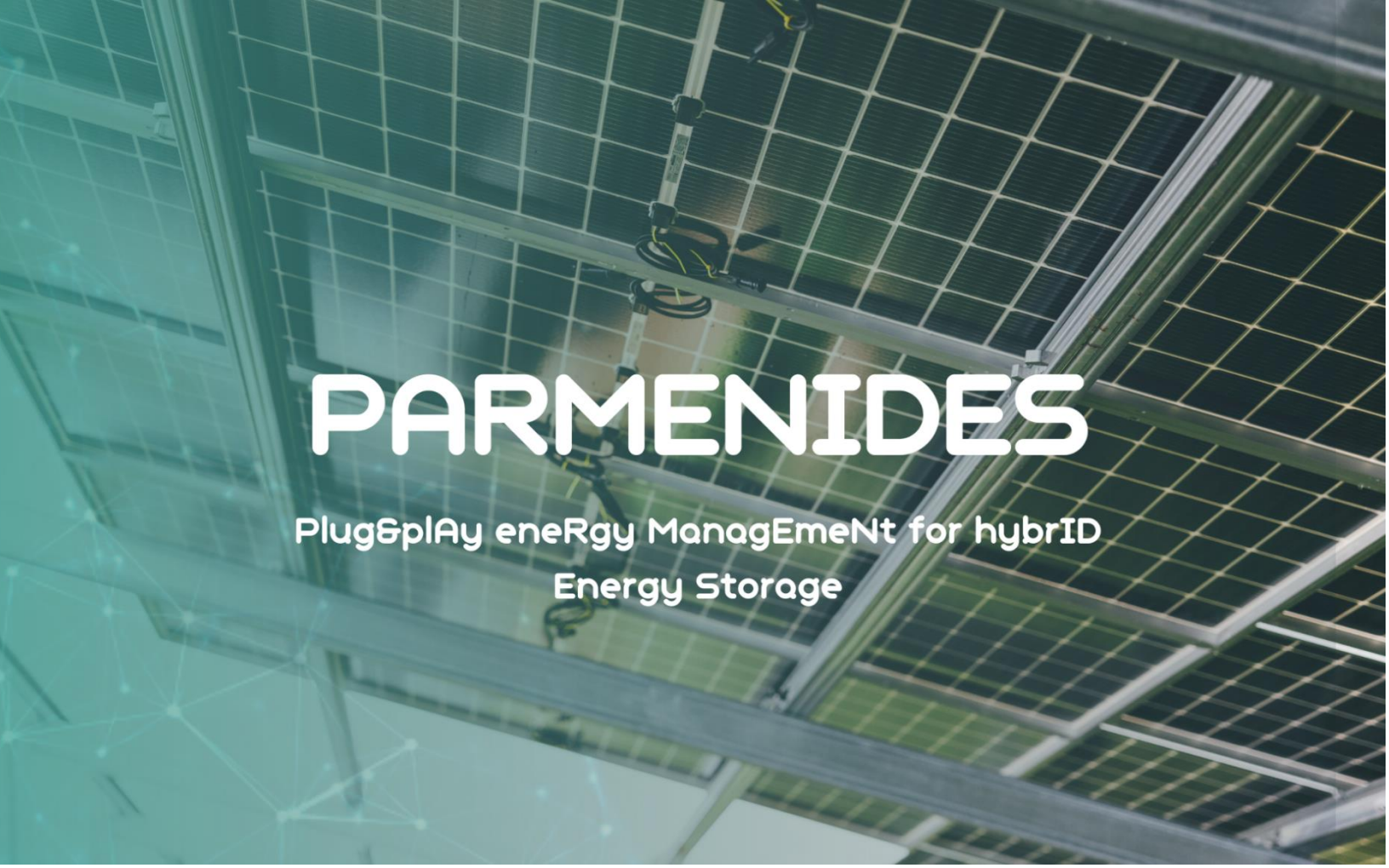


Deliverable D3.3

Cybersecurity and privacy practice and user acceptance criteria

Work Package 3

Disclaimer

Funded by the European Union's Horizon Europe programme under Grant Agreement nº 101096453

Grant agreement	101096453
Type of action	HORIZON-IA HORIZON Innovation Actions
Topic	HORIZON-CL5-2022-D3-01-10 Interoperable solutions for flexibility services using distributed energy storage
Starting date of project	01.01.2023
Project duration	36 months

Work package	WP3 - Architecture design, interoperability, and ontology development
Related task	T3.3 - Trustworthiness (cybersecurity and data privacy)
Deliverable due date	M15 (31.03.2024)
Actual delivery date	M15 (31.03.2024)
Dissemination level	Public
Deliverable responsible	TRIALOG

Document Information

Document Version: 1.0

Revision / Status: Submission

PARMENIDES

All Authors/Partners

Name	Organisation
Léo Cornec	Trialog
Dune Sebilleau	Trialog
Estibaliz Arzoz Fernandez	Trialog
Guillaume Mockly	Trialog
Frédéric Mesureur	Trialog

Document History

Revision	Content/changes	Resp. partner	Date
0.1	Creation of the structure	Trialog	19.02.2024
0.2	First draft of the document	Trialog	08.02.2024
0.3	Completion of section 2 and 3	Trialog	20.02.2024
0.4	Completion of section 1, 4 and 5	Trialog	29.02.2024
0.5	Issuance of the first full version for partners review	Trialog	08.03.2024
	Deliverable review	AIT	19.03.2024
0.6	Second version of the document based on partners feedback	Trialog	27.03.2024
0.7	Deliverable final review	AIT	31.03.2024
1.0	Final version	Trialog	31.03.2024

Document Approval

Final approval	Name	Resp. partner	Date
1.0	Jawad Kazmi	AIT	31.03.2024

PARMENIDES

Executive Summary

This task enabled to assess the status of the pilots and systems in terms of cybersecurity and privacy and prepare for the definition of the Privacy and Security Plan, that will occur in Task 5.2, across the development phase of the PARMENIDES solutions. This includes:

- A technical introduction to the notion of privacy and cybersecurity (definitions, methods, standards)
- A presentation of the PARMENIDES methodology to evaluate the privacy and cybersecurity compliance of the pilots and systems
- The identification of the needs and the definition of the project requirements for cybersecurity and privacy
- The presentation of a dashboard which will be used over the course of the systems development to support and monitor the implementation of cybersecurity and privacy controls

This deliverable will describe the method (see Figure 1) to be used in T5.2 which is the Privacy and Security Plan (PSP). The main goal of the PSP analysis is to guide the solution providers to make a complete and thorough analysis of their systems including:

1. A training part that will be constituted of a series of courses and workshops to provide PSP analysis guidelines and methods. This will be distributed along the development of the systems.
2. A participant's contribution to provide a clear understanding of their systems in terms of vulnerabilities
3. Guidelines to identify threats and countermeasures to put in place

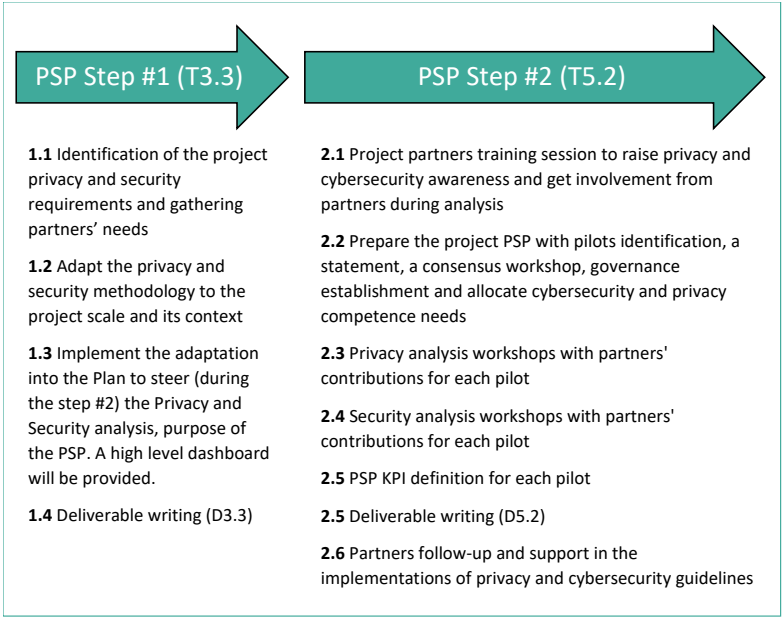


Figure 1: PSP steps within PARMENIDES

PARMENIDES

Table of contents

PARMENIDES

Abbreviations

Acronym	Description
API	Application Programming Interface
CIA	Confidentiality, integrity and availability
CNIL	French national commission on informatics and freedom
CVE	Common Vulnerabilities and Exposures
DFD	Data Flow Diagram
DMP	Data management plan
DPA	Data Protection Authority
DPIA	Data Privacy Impact Assessment
DPO	Data Protection Officer
DSO	Distribution system operator
EC	European commission
EMS	Energy Management System
EU	European Union
GDPR	General Data Protection Regulation
HESS	Hybrid Energy Storage System
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and communication technologies
IEC	International Electrotechnical Commission
IOT	Internet Of Things
ISO	International Organization for Standardization
KPI	Key Performance Indicator
LINDDUN	Linking, Identifying, Non-repudiation, Detecting, Data Disclosure, Unawareness, Non-compliance
NDA	Non-Disclosure Agreement
NIS	Network and Information Security
NISG	Network Information Security Law
NIST	National Institute of Standards and Technology
NISTIR	NIST interagency or internal reports
OWASP	Open Worldwide Application Security Project
PARMENIDES	Plug&plAy eneRgy ManagEmeNt for hybrID Energy Storage
PECO	PARMENIDES Energy Community Ontology
PETS	Privacy-enhancing technologies
PIA	Privacy Impact Assessment
PII	Personal Identifiable Information
POMME	Privacy operationalisation model and method for engineering
PSP	Privacy and Security Plan
RDP	Remote Desktop Protocol
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege
TLS	Transport Layer Security

PARMENIDES

1. Introduction

1.1. PARMENIDES project introduction and summary

The ongoing transition of the energy system is accompanied by digitalization activities, enabling new applications. This results in a fragmentation of existing platforms, protocols, and standards. Therefore, interoperability among various platforms as well as cross-domain interoperability must be ensured.

The usage of ontologies provides an opportunity to address cross-platform and cross-domain interoperability. PARMENIDES aims to develop a new ontology by extending existing ontologies to provide a knowledge base, with a focus on the electricity and heating domain for buildings, customers, and energy communities. It will support different use cases, focusing on the utilization of Hybrid Energy Storage Systems (HESS). Besides the representation of storage technologies, information about energy community customers, their behaviours, and components including their relations will be part of the ontology, providing a standardized vocabulary of the domain of energy communities. This further includes technical, economic, regulatory, behavioural, and social constraints to be considered in operation.

To support a number of use cases, a new generation of innovative Energy Management Systems (EMS) will be developed. These systems will be capable of using ontology as a knowledge base. This will enable a very generic software design and ensures the scalability and replicability of the solution.

As a framework for the integration of the EMS, PARMENIDES will define an information and communication architecture, enabling an interoperable, reliable, and secure exchange of data and instructions. The developed EMS will be demonstrated in very diverse pilots in Austria and Sweden. The Austrian pilot will address energy communities with different storage technologies, the Swedish pilot will focus on flexibility from a very short time scale through innovative heat pump control to electrical and thermal batteries and seasonal storage through geothermal borehole heat exchangers.

1.2. Work Package 3 (WP3) introduction

The objectives of this work package are to design an interoperable and secure system architecture to support the use-cases defined in WP2 and develop the required components in WP4. It will rely on existing references (e.g., standards, reports, etc.) and results from previous projects (e.g., InterConnect, BRIDGE, etc.). Furthermore, the PARMENIDES Energy Community Ontology (PECO) will be developed, based on existing ontologies to act as a knowledge base for the new generation of energy management applications (WP4) and to utilize the flexibility of different storage technologies.

1.3. Task 3.3 (T3.3) introduction

The objective of the task 3.3 is to prepare the cybersecurity analysis (T5.2) that will take place throughout the development of the PARMENIDES pilots and systems. This includes three main aspects:

- The definition of cybersecurity and privacy requirements to define the actions to be done within the analysis
- The definition of the PARMENIDES cybersecurity and privacy methodology to ensure pilots and system compliance

- The update of an existing dashboard according to project needs, with the objective of gathering the analysis information, and monitoring the progress

These analyses will enable to get an overview of the status of the solutions developed in PARMENIDES in terms of cybersecurity and privacy. Furthermore, this task enables to tailor the development of the cybersecurity and privacy tool and method to the project needs.

1.4. Objective and structure

The aim of this deliverable is to lay the foundations that will be used to carry out the privacy and cybersecurity analysis (T5.2), while presenting the preliminary work carried out in task T3.3.

The deliverable is structured as follows:

- a technical introduction of privacy and cybersecurity notions with a focus on methods and standards
- a description of the PARMENIDES methodology to assess the project pilots and systems privacy and cybersecurity compliance
- a description of the PARMENIDES requirements
- a presentation of the dashboard to be used with the methodology

This deliverable is a preparatory document and explains the methodology to be applied in task T5.2.

2. Cybersecurity and privacy introduction

This chapter will detail the most relevant elements within the context of privacy and security applied to the project. They will be described from key definitions to main methods that are applied to the Privacy and Security Plan (PSP).

2.1. Definition, context, and scope

First, it is essential to define the context and scope where cybersecurity and privacy will be analysed. It is necessary to understand the scope of the project or product or system of interest, but also the context of the element that will be analysed, from the data that will be used, shared, stored to the main actors or stakeholders that interact within the element/system and exchange data between them or have access to that data.

For a better understanding, a list of most relevant definitions is presented. It will be used along this document and through the PSP definition and risk analysis.

- PII[1] (Personally Identifiable Information): Any information that can be used to identify the PII Principal to whom such information relates or is or might be directly or indirectly linked to a PII Principal.
- Sensitive PII: Category of personally identifiable information (PII), either whose nature is sensitive, such as those that relate to the PII principal's most intimate sphere, or that might have a significant impact on the PII principal. (e.g., health data, political or philosophical orientation, sexual orientation, biometric/genetic data, race, ethnic data).
- Privacy Risk Assessment – PIA (Privacy Impact Assessment) – DPIA (Data Privacy Impact Assessment):
    - Overall process of risk identification, risk analysis and risk evaluation with regard to the processing of PII.
    - Overall process of identifying, analysing, evaluating, consulting, communicating, and planning the treatment of potential privacy impacts with regard to the processing of personally identifiable information, framed within an organisation's broader risk management framework.
- PII Principals: Natural person to whom the personally identifiable information (PII) relates. The synonym Data Subject can also be used.
- Privacy Breach: Situation where PII is processed in violation of one or more relevant privacy safeguarding requirements. A personal data breach means a breach (due to inadequate security or processes) leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.
- Privacy Risk[2]: Effect or uncertainty on privacy.

[1] ISO/IEC 29100-:2011
[2] ISO/IEC 29100:2011

- Privacy Control: Measures that treat privacy risks by reducing the likelihood or consequence of a breach.
- Processing of PII: Operation or set of operations performed upon PII.
- Privacy Impact: Anything that has an effect on the Privacy of a PII principal and/or group of PII Principals.
- Anonymization/De-identification: Processes by which PII is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party.
- Consent: PII principal's freely given, specific and informed agreement to the processing of their PII.

Here below, the definitions are detailed for the main roles, that the GDPR refers to:

- PII Controllers: Privacy stakeholders that determine the purposes and means of processing personally identifiable information (PII) other than natural persons who use data for personal purposes. The term Data Controller is also used in the GDPR.
- PII Processors: Privacy stakeholder that processes personally identifiable information (PII) on behalf and in accordance with the instructions of the PII Controller. The term Data Processor is also used in the GDPR.
- DPO[3]: Data Protection Officer is a new role defined by the GDPR (General Data Protection Regulation) whose primary role is to ensure that his organisation processes the personal data in compliance with the applicable data protection rules. GDPR requires certain organizations to appoint a DPO. The appointment of the DPO must be based on his personal and professional qualities, a good understanding of the organisation and knowledge on data protection.
- DPA[4]: Data Protection Authority are independent public authorities that supervise, through investigative and corrective powers, the application of the data protection law. They provide expert advice on data protection issues and handle complaints lodged against violations of the GDPR and relevant national laws. There is one in each EU Member State.

[3] https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en
[4] https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en

2.2. Privacy requirements

Requirements are the needs that must be satisfied for a proper development, accomplishment or deployment of a system or solution. Regarding Privacy, the requirements should address the privacy needs that the system or solution presents or which have been identified that performs a Privacy Impact Assessment (PIA). When the system or solution is sharing, exchanging, or storing data, the first analysis is to determine and identify:

- Which type of data, is it PII?
- Is there personal data processing?

Privacy will focus on the personal data processing with regard to the Impact on the citizen privacy but also on the organisation/business and ecosystem impact. Standardisation work on privacy provides a wide list of standards to look at and use within privacy analysis:

- The NIST Privacy Framework: It is based in the following steps:
    - Identify: Identify the data processed, understand interests of individuals affected and conduct risk assessment to understand the business environment and identify and prioritize privacy risks.
    - Govern: Develop and implement the organizational governance structure to understand a continuous risk management activity on privacy priorities.
    - Control: Develop and implement appropriate activities to manage data in such a way to also manage privacy risks.
    - Communicate: Apply and develop appropriate activities to provide a reliable understanding and engage in a dialogue on how data is processed and its associated risks.
    - Protect: Data protection measures.
- NISTIR 8062 – An introduction to privacy Engineering and Risk management in Federal Systems.
- PRIPARE – Privacy and security by design methodology Handbook.
- Specifically, ISO/IEC 27570 – Privacy guidelines for Smart Cities is the only reference document that deals with ecosystem practice but focused on privacy.
- ISO/IEC 23894 AI risk management - guidance on how organizations that develop, produce, deploy or use products, systems and services that utilize artificial intelligence (AI) can manage risk specifically related to AI. The guidance also aims to assist organizations to integrate risk management into their AI-related activities and functions.
- ISO/IEC 24028 Trustworthiness – Trustworthiness is a hot topic in standardisation and an important topic to address in technical systems, AI systems. This standard supports in the approach to establish trust AI systems through transparency, explainability, controllability. But also provides typical AI threats, risks together with mitigation measures for these kind of systems. And finally, it approaches to assess and achieve availability, resiliency, reliability, accuracy, safety, security and privacy of AI systems.
- IEC 62443 – This standard has several norms/parts that provide information over the security of industrial automatization and control systems. From this norm, it is taken the definitions of KPIs for Security Levels and Maturity Levels.

- ISO/IEC 27701 – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – requirements and guidelines.

In the case of Privacy risk analysis, here are the most used methodologies to perform DPIAs:

- ISO/IEC 29134 – Privacy Impact Assessment Guidelines: This standard provides guidelines and recommendations to conduct a PIA; from understanding which are the benefits, objectives, and targets of a DPIA to how to conduct PIA process (e.g., risk assessment, risk treatment).
- CNIL: The CNIL (Commission Nationale de l'Informatique et des Libertés) is the DPA (Data Protection Authority) in France. This organization has provided its methodology called CNIL methodology and a tool for the performance of DPIAs. This methodology is more extended and known in France but has many similarities with the ISO/IEC 29134.
- LINDDUN (Linking, Identifying, Non-repudiation, Detecting, Data Disclosure, Unawareness, and Non-compliance): It is a privacy impact assessment (PIA) method that provides support to the elicitation and mitigation of privacy threats.

There are other types of methodologies oriented to Privacy Engineering or Privacy operationalization, such as:

- ISO/IEC 27561 – Privacy operationalisation model and method for engineering (POMME): It provides support on privacy engineering management.
- ISO/IEC 27556 – User centric framework for the handling of PII based on privacy preferences.
- ISO/IEC 27550 Privacy engineering for system life cycle processes; it is supported by the design process for strategies to take:
    - Data oriented strategies:
        - Minimize: Limit as much as possible the processing of PII (selection before collection, anonymization).
        - Separate: Distribute or isolate personal data as much as possible, to prevent correlation (Logical or physical separation, endpoint processing).
        - Abstract: Limit as much as possible the detail in which personal data is processed while being useful (Aggregation over time (used in smart grids), dynamic location granularity (used in location-based services), k-anonymity).
        - Hide: Prevent PII from becoming public or known (Encryption, mixing, perturbation (differential privacy, statistical disclosure control), unlinking (pseudonymization), attribute-based credentials).
    - Process oriented strategies:
        - Inform: Inform PII principals about the processing of PII (Privacy icons, layered privacy policies, data breach notification).
        - Control: Provide PII principals control about the processing of their PII (Privacy dashboard, consent (also withdrawal)).
        - Enforce: commit to PII processing in a privacy friendly way, and enforce this (sticky policies and privacy rights management, commitment of resources, assignment of responsibilities).

- Demonstrate: Demonstrate that PII is processed in a privacy friendly way (Logging and auditing, privacy impact assessment, design decision documentation).

2.2.1 LINDDUN methodology

It is a methodology for privacy engineering framework that provides support to elicit and mitigate privacy threats in digital systems. In consists in three main steps:

1. Model the system: It needs a good understanding of the system, specifically of the Data Flow Diagram (DFD) of the system which provides the essential information about data transfers and flows. A DFD is a structured, graphical representation of the system that contains four main parts (entities, data stores, processes, and data flows).
2. Elicit threats: Once the system is described, each DFD element is systematically analysed for privacy threats. These threats are categorized into LINDDUN threat categories.
3. Manage threats: the threats are prioritized in relevancy, the most important are treated with mitigation strategies/measures. Some threats identified may be acceptable.

Figure 2 presents the extended steps for LINDDUN methodology, where the problem space is identified versus the solution space:

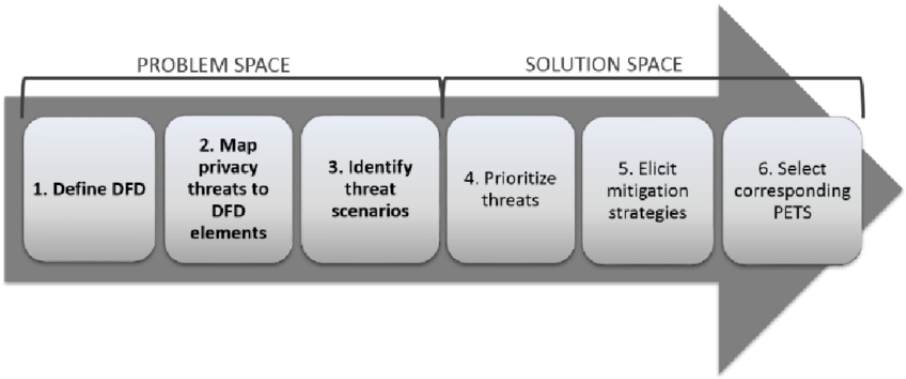


Figure 2: LINDDUN methodology steps

Table 1 represents the 7 categories that LINDDUN method provides to categorize the privacy threats in a system. The categories are linked to different data properties which are classified are Hard privacy (no one

externally can violate the privacy of the user), Security (relative to the confidentiality and security of the system) and Soft privacy (relative to the legal aspects of privacy).

Table 1: LINDDUN threats categories

	Threat	Property		Threat definition
L	Linkability	Hard Privacy	Unlinkability	Hiding the link between two or more actions, identities, and pieces of information associated with entities or users.
I	Identifiability		Anonymity	Hiding the link between a user or an entity identify and an action or a piece of information.
N	Non-repudiation		Plausible deniability	Ability for an entity or user to deny having performed an action that other parties can neither confirm nor contradict.
D	Detectability		Undetectability and unobservability	Hiding the activities of an entity or user.
D	Disclosure of information	Security	Confidentiality	Ability of the system to hide the data content or to control the release of data content.
U	Unawareness	Soft Privacy	Content awareness	User's unconsciousness regarding his own data.
N	Non-Compliance		Policy and consent compliance	Stakeholder as data controller of PII to inform the user, who is a PII principal, on the system privacy policy, or allow the user to specify consents and exercise his rights in compliance with legislation.

2.3. Security requirements

Security requirements are the needs that system must or should address in order to keep an acceptable risk to manage or mitigate the risks presented. Security focuses on the threats and vulnerability of the systems. And its risk and impact are measured for the system. On the other hand, a security attack materialized can lead to a privacy breach, too.

Standardisation work in security:

- ISO/IEC 27001 Information Security management systems-requirements.
- ISO/IEC 27002 Code practice for information security controls.
- ISO/IEC 27005 Information security risk management
- ISO/IEC 27110 Cybersecurity framework development guidelines
- ISO/IEC Security and privacy guidelines for IoT
- ISO/IEC 27403 IoT Security and privacy – Guidelines for IoT – Domotics

Methodologies for security risk analysis:

- NIST Cybersecurity Framework: It is based in the following steps:
  - Identify: the assets to protect through governance, risk assessment and risk management strategy.
  - Protect: the protection of the assets through access control, awareness, training and other processes and procedures.
  - Detect: events, anomalies through a continuous monitoring and detection process.
  - Respond: planning, analysis, communication, mitigation, and improvements.
  - Recover: Recovery planning, improvements, and communications.
- STRIDE: It is oriented towards the identification and categorization of security threats to protect security properties of the system

2.3.1 STRIDE methodology

This methodology analyses threats. It identifies and categorizes security threats that can lead to a cybersecurity breach of the target system.

Table 2: STRIDE threats categories

	Threat	Property violated	Threat definition
S	Spoofing	Authentication	Pretending to be something or someone other than yourself (e.g., illegally accessing and using another user's information, such as username or password).
T	Tampering	Integrity	Modifying something on disk, network, memory or elsewhere, malicious data modification (e.g., disrupt operations, intercept data flow, inject data).
R	Repudiation	Non-repudiation	Claiming that you did not do something or were not responsible; can be honest or false (e.g., user performs an illegal

			operation in a system that lacks the ability to trace the prohibited operation).
I	Information disclosure	Confidentiality	Providing information to someone not authorized to access it (e.g., users read a file that they are not granted access to or an intruder reads data in transfer).
D	Denial of Service	Availability	Exhausting resources needed to provide service (e.g., an attack deny service to valid users). It hinders system availability and reliability.
E	Elevation of privilege	Authorization	Allowing someone to do something they are not authorized to do (e.g., users gain privileged access to compromise or destroy the entire system. The attacker has penetrated the system and becomes part of the trusted system itself).

3. Cybersecurity and privacy analysis - PARMENIDES methodology

The following section aims at describing the methodology applied in PARMENIDES to provide a cybersecurity and privacy analysis of the project demonstrators and systems. This process is based on an existing methodology developed by Trialog and successfully demonstrated in previous EU projects, e.g., InterConnect [1], Energica [2] etc. In the context of each project the Trialog team work on the identification of the project and partners' needs and then adapt and customise the existing methodology to fit the requirements. Indeed, each project has their own cybersecurity and privacy requirements. In parallel, the corresponding developments and features are integrated into the Trialog tool/dashboard.

The name of the Trialog methodology is Privacy and Security Plan (PSP).

Methodology objective: Ensure that security and privacy is adequately managed without dead zone in PARMENIDES demonstrators and system-of-interest and its associated ecosystem.

3.1. Methodology process and organization

The PARMENIDES methodology is divided in two main steps as describe by Figure 3. Firstly, the identification and preparation step. And secondly, the privacy and cybersecurity analysis of pilots and systems.

The 1st step of this process is based on a questionnaire (see Section 7.1) to be answered by the project partners. Feedbacks combined with a review of the project context and needs are necessary to identify the project requirements. Based on these requirements the methodology of the PSP and associated tools are adapted to cover all the needs. In this project the 1st step corresponds to Task 3.3.

The 2nd step of this process is based on the preliminary work done in the 1st step as well as a series of workshops with the task contributors. These sessions will be organised by Trialog to prepare the Privacy and Security Plan. Five main phases constitute the 2nd step of the PSP:

- Training sessions will be performed by Trialog to the task contributors to ensure a sufficient level of knowledge. The following subjects will be covered:
    - Preparing a PSP
    - Privacy analysis
    - Security analysis
    - Privacy and security program KPI
- The most extensive steps (2.2, 2.3 and 2.4) consist of a series of focused workshops for each pilot, gathering Trialog's cybersecurity expert and the pilot leaders. These workshops enable targeted security and privacy analysis to be carried out for each pilot and systems to be developed as part of the project. The number of sessions to organise by pilot will depend on the complexity of their Information and communication technologies (ICT) infrastructure. The participants of the workshop should have a good vision of the overall pilot architecture and use-cases in order to be able to identify threats and breaches at the whole system level.

- The KPIs definition is important as it will ensure an efficient monitoring of the improvements based on the results of the analysis.
- The objective of phase 2.6 is to support the partners in the implementation of the recommendations and to monitor the progress thank to the KPIs.

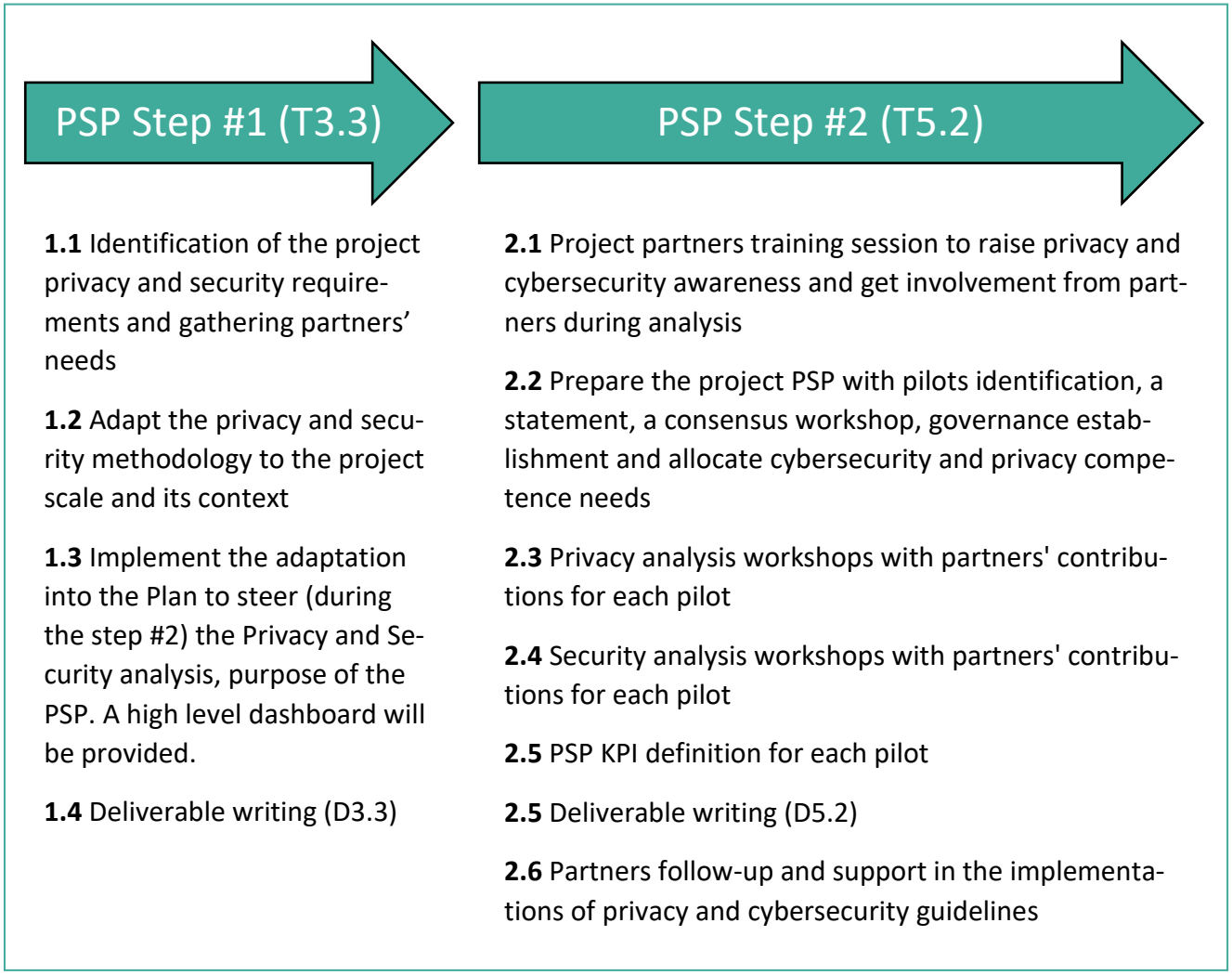


Figure 3: PARMENIDES PSP methodology phases

3.2. Project requirements

The aim of the cybersecurity and privacy requirements (see section 0) is to answer the following questions [3] in order to guide the analysis:

- What is the state of the solutions in terms of cybersecurity and privacy?
- What are the efforts dedicated to cybersecurity and privacy?
- What are the needs from the partners on the cybersecurity and privacy side?
- How are the needs distributed across the pilots and their components?

The cybersecurity and privacy requirements were defined in collaboration with the project contributors, solution providers in order to make sure to get a good understanding of the project needs. A questionnaire was answered to provide the following information:

- Presence of Personally Identifiable Information (PII) data in pilots
- The efforts dedicated towards cybersecurity and privacy
- The cybersecurity and privacy features in place
- Risks analysis performed
- Specific agreement already in place within pilots
- Cybersecurity and privacy level of the participants
- Expectations from this study

3.3. Privacy analysis

The privacy analysis aims to support the solution providers in identifying and assessing the risks for privacy in the developed systems.

It first starts by describing Personal Identifiable Information (PII), as well as the context information. In particular, the frameworks for the Privacy Impact Assessment (PIA) process are investigated, including local regulations.

The potential breaches are then studied, including the categories they fall into, their goal, and the list of stakeholders who may be affected. The threats are investigated and linked to the breaches described earlier. They are categorized according to the LINDDUN categories and associated to their goals and stakeholders.

The impact of each breach is then identified, including the user, operational and overall impact levels, as well as the rationale for each of them. Afterwards, the risk associated with each breach is assessed, by combining the likelihood and impact ratings.

A control strategy is finally defined, including the strategy for the control, its categorization, and requirements. The plan for the management of privacy incidents is also defined.

3.4. Cybersecurity analysis

The security analysis begins with a description of the system, its interfaces, assets, stakeholders, and use-cases. The analysis parameters, including the likelihood, impact and risk scales, the risk map and treatment strategy can be defined.

The next step consists of identifying the threats, starting by defining the attacker profiles, and attaching them to the threats, along with the goal, assets involved, impact and target properties of each threat.

Attack scenarios are then investigated. The events are identified, describing their effect, the identification of possible Common Vulnerabilities and Exposures (CVE), the target properties and the likelihood of the event. They are linked to the attack paths that are defined afterwards, with the related threats, and the likelihood of each attack path.

From there, the global risk level is calculated, by combining the likelihood and impact ratings of each risk. The risks are also linked to the attack paths.

Finally, the treatment plans are elaborated, by defining the strategies used to treat the risks and the possible controls with their goals and implementation process, and attaching them to the risks, with the impact of the treatment.

4. PARMENIDES cybersecurity and privacy requirements

This section of the deliverable summarizes the PARMENIDES requirements and expectations based on partners feedbacks. The definition of the cybersecurity and privacy requirements was conducted for two main reasons: to assess the state of the systems in terms of cybersecurity and privacy in order to be prepare for the Privacy and Security Plan (PSP) analysis that will take place in Task 5.2, and to tailor the development of the PSP tool and dashboard, described in section 0, to the needs of the project.

4.1. Summary of the partners feedback to the questionnaire

As mentioned earlier in this deliverable a questionnaire was sent to the project partners involved in the Swedish and Austrian pilots as well as other project developments. The aim of this questionnaire was mainly to understand the project needs/requirements, partners knowledge level/status and partners expectations.

The following questions were asked to the partners:

- Is the system handling Personally Identifiable Information (PII)? Sensitive data?
- Apart from tasks specifically dedicated to cybersecurity issues, what efforts are dedicated for implementing cybersecurity and privacy measures in the work to come?
- What cybersecurity and privacy features are already in place in your pilot?
- Have you already performed a risks analysis for your system or pilot?
- Are there specific agreements in place within the existing pilots?
- Are the participants experimented or trained on cybersecurity or privacy issues?
- What your minimal expectations could be for a cybersecurity and privacy analysis tool for your system or pilot?

The following sections summarize the answers received.

Is the system handling Personally Identifiable Information (PII)? Sensitive data?

According to the partners, Personally Identifiable Information (PII) will be handled by the two pilots and in general by the system. However, it will not include Sensitive data [3] (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs; trade-union membership; genetic data, biometric data processed solely to identify a human being; health-related data; data concerning a person's sex life or sexual orientation). Project system will include critical data not only from the customers but from the DSO as well.

Customer PII will be: name of the customer, address, number, metering point, installed photovoltaic power, consumption including consumption pattern, related measuring data etc.
DSO critical data are: grid topologies as transformer station, technical data of grid assets, switching states, connection points of assets etc.

Apart from tasks specifically dedicated to cybersecurity issues, what efforts are dedicated for implementing cybersecurity and privacy measures in the work to come?

Generally, the partners have already worked on the subject of privacy by setting up contracts about privacy and consent with customers and third parties. In addition, in the system development case they aim to include these considerations by-design or to make sure that third-party components are. Some of them are also considering the Network Information Security Law (NISG) with audit logs as well as data encryption and anonymisation.

What cybersecurity and privacy features are already in place in your pilot?

Here are the main features raised by the partners within this survey:

- Audit Logs
- Encrypted communication between systems
- Use of containers with Docker for services
- Database anonymization
- Database access only possible for services running on the Remote Desktop Protocol (RDP)
- Integration by-design
- Grid assets and communication in the low voltage grid protected by the grid operator directly
- User consent of the data management policy
- All back-end components are installed on private machines in the protected cloud with remote access authenticated via public-private keys
- Front-ends and public Application Programming Interfaces (APIs) are exposed on specific ports via proxy servers installed on public machines. Access to APIs and front ends occurs exclusively via the Hypertext Transfer Protocol Secure (HTTPS) protocol, offering Transport Layer Security (TLS) 1.2 encryption in transit
- Use of ISO/IEC 27001 to guarantee the confidentiality, integrity and availability (CIA) of information 'in use'
- All interoperability layers support the secure transport of information in compliance with Open Worldwide Application Security Project (OWASP) requirements
- The EMS includes an identity and access management system, for strong authentication, such as multi-factor authentication, authorization and single sign-on, administration and management of policies and roles. Appropriate measures are used for the management of digital identities (e.g. certificates) and for machine-to-machine communication (e.g. TLS)

Have you already performed a risks analysis for your system or pilot?

Some partners have already performed a risk analysis through EU projects or subcontracting. The methodologies used were STRIDE, NIST SP 800-115 standards and GDPR analysis.

Are there specific agreements in place within the existing pilots?

Here are the existing agreements in place within the existing pilots:

- some partners have set up contracts among them to ensure privacy through anonymise data
- contracts between pilot site tenant and research institute
- Non-Disclosure Agreement (NDA) among some partners

- Privacy statement and declaration of consent by customers

Are the participants experimented or trained on cybersecurity or privacy issues?

The participants' level of knowledge is fairly heterogeneous. Some have no knowledge of these subjects, while others have received training on GDPR and privacy.

What your minimal expectations could be for a cybersecurity and privacy analysis tool for your system or pilot?

Here are the partners' main expectations:

- privacy and cybersecurity context and training
- privacy and cybersecurity status
- best practices guidelines
- simulation of attack
- include NIS2 [4] requirements in the process

4.2. Project requirements and implementation

This section starts by presenting a summary of the PARMENIDES participants answers to a questionnaire sent to them to understand their needs in addition of the projects ones. The following sub-sections describe one identified requirements and the way it is plan to be implemented into the project.

4.2.1 Analysis of system security & privacy

Definition of the requirement

The main requirement identified corresponds to obtaining an overview of the systems' security and vulnerabilities.

This analysis should provide a one-shot broad analysis of all aspects of cybersecurity and privacy within the pilots and cover the different points that were pointed out by respondents or identified as relevant by Trialog. The method allows to monitor progress in implementing measures thanks to the use of KPI.

This one-shot analysis should enable the solution providers to get a deep understanding of cybersecurity and privacy principles, based on relevant reference architectures, ISO standards (including Management standards & Management systems standards [5], 20889 [6], 27xxx series [7] [8] [9] [10] [11] [12] [13], 29100 [14], 29134 [15], 31000 [16], 31700 [17]), IEC standards 62443 series [18], NIST guidelines (NISTIR 7628 [19] and 8062 [20]) and privacy [21] and security frameworks, EC recommendations on cybersecurity in the energy sector (SWD (2019) 1240 final), LINDDUN privacy threat model [22], STRIDE Threat modelling, MITRE Knowledge bases and the CNIL Privacy Impact Assessment Methodology [23].

Since some participants could focus their efforts on cybersecurity and privacy into a few narrow areas, such as one system entry point, or the data encryption, it is especially important that this analysis covers all aspects of cybersecurity and privacy and provide an analysis of the complete system.

Implementation in PARMENIDES

The main goal of the PSP analysis is to guide the solution providers to make a complete and thorough analysis of their systems including:

- A training part that will be constituted of a series of courses and workshops to provide PSP analysis guidelines and methods. This will be distributed along the development of the systems.
- A participants' contribution to provide a clear understanding of their systems in terms of vulnerabilities.
- Guidelines to identify threats and countermeasures to put in place.

4.2.2 Training sessions

Definition of the requirement

As pointed out by some participants, it is important for the project to provide training and awareness on cybersecurity and privacy.

Implementation in PARMENIDES

To respond to this need, the first stage of the PSP is to conduct training and awareness workshops, to ensure that the entire group is at a sufficient level of knowledge, to understand the challenges, to provide relevant information and to be able to capitalize on the work carried out after the task.

4.2.3 Action plan for improvement

Definition of the requirement

The analysis of the system through the PSP tool should end with the establishment of an improvement report, that highlights the parts of the system where improvements are required, and indicates how the system should be modified to achieve a sufficient level of security. This report can be considered as a plan to follow. This has been highlighted as relevant by some of the respondents.

The report should provide:

- An overview of the analysis of the cybersecurity and privacy in the system
- An understanding of the weaknesses of the system
- A highlight of the main risks
- Suggestions and guidelines for system improvements

Implementation in PARMENIDES

The output of the PSP will be a written report, delivered to the pilot after completion of the PSP process and supported by the PSP dashboard. This report will provide information on:

- How the PSP has been prepared
- The characterization of the system
- Privacy analysis results
- Cybersecurity analysis results
- Privacy and Cybersecurity KPI results

The report will therefore provide the needed overview and analysis of the systems, enabling solution providers to implement improvements accordingly. In particular, it will highlight the areas of the systems that will need to be secured in priority by highlighting the scale and likelihood of the most significant risks. However, the choice of the most relevant solution to implement will be done by the solution developers.

4.2.4 Evidence of Compliance

Definition of the requirement

The PSP should provide evidence that the system respects the privacy and cybersecurity principles that constitutes the coordinated security and privacy-by-design practice on which is based the PSP tool.

The evidence of compliance aims to prove that the systems have implemented the necessary measures to ensure the security of their systems.

The evidence of compliance should therefore entail:

- A proof of the full analysis of the system in terms of cybersecurity and privacy, aiming to detect any weaknesses.
- Normalized testing following privacy and security standards to prove the compliance of the system to said standards.
- A focus on NIS2 requirements [4]

Implementation in PARMENIDES

The PSP tool will not be able to provide any standardized certifications, as it doesn't have access to the systems for testing, only to the declarations of the PSP participants. A set of KPIs will moreover enable to give indications on the maturity and security levels of all systems involved.

Results of the PSP can be presented as proof that a risk-based approach has been taken to manage cybersecurity and privacy, which is a NIS2 requirement. The PSP itself is not enough to ensure NIS2 compliance as the directive also covers personnel training, incident reporting and coordination with cybersecurity agencies, and is evaluated for a company/organisation and not a system/pilot.

With this in mind, the PARMENIDES partners will be asked during the preliminary workshops to provide a description of their cybersecurity incident management process as an input to the PSP.

4.2.5 Definition of access plan for data to be shared

Definition of the requirement

The data present in the pilots should be analysed in order to characterize and protect them adequately.

The analysis of the data should include:

- The sensitiveness of the data
- The impact in case of leak
- The access rights for partners of the project
- The appropriate level of dissemination

Some data indeed require a special focus, either because of their relevance to the system's security, or because they include personal information from participants of the project or persons and entities interacting with its systems.

Implementation in PARMENIDES

Most of the needs for this requirement, including the analysis of the data sensitiveness, access rights and dissemination levels are covered by the Data Management Plan, and will be updated through the course of the project. Moreover, the data sensitiveness and the privacy impacts will be taken into account in the PSP analysis, and therefore included in the risk analysis of the system.

4.2.6 Simulation of attacks

Definition of the requirement

In order to understand the actual weaknesses of their system, it would be useful for some solution providers to simulate attacks on their system. This was indicated as relevant by two of the respondents.

An attack simulation would entail first an analysis of the potential attacks, including answering the following questions:

- Who could attack?
- What would be the motivation?
- What components of the system would be impacted?
- What would be the impact in terms of cybersecurity and privacy?
- What is the likelihood of such an attack?

This enables to have an idea of all kinds of attacks that could potentially occur, and to focus on the most important ones, which are causing the most risk to the security.

Then, an implementation part is required to simulate the attacks on the system, with a person playing the attacker role, and trying to play out the attack.

Implementation in PARMENIDES

The analysis of potential attacks is included in the scope of the methodology to be applied during the project. The participants will get training to understand the possible attacks that can occur, and they will be supported through the workshops. However, no real simulation of attacks will be carried out as it is not included in the defined scope.

5. Project dashboard for cybersecurity and privacy

The Task 3.3 of PARMENIDES aims to prepare the Task 5.2, that will be focused on the definition and implementation of the Privacy and Security Plan (PSP) by all solution providers. Trialog will train and support technical partners to do so, using a methodology defined across the European projects Sender [24], Maesha [25], InterConnect [26] and Energica [2] as well as a dashboard described in this section. In the context of PARMENIDES, the Trialog Team adapted the tool to meet the needs of the project, in particular by setting up a KPIs system to monitor pilots progress in implementing recommendations during the support phase.

5.1. Purpose of the tool

The dashboard for cybersecurity and privacy is developed by Trialog to support the future activities of Task 5.2, enabling to gather all information and results regarding the PSP activities that will be defined by the solution providers in each pilot, as well as monitor the progression of the plan itself.

The dashboard tool purpose is to help and support users within the creation of a PSP and the performance of the actions planned in that plan, such as privacy and security risk analysis. The tool remains as a guide to help the user in the creation of a PSP and its risk analysis planned within the PSP, with questions, explanations, and examples in each question, as necessary.

The dashboard has been developed in previous projects and completed within task 3.3, based on Trialog's expertise and knowledge on cybersecurity and privacy frameworks, such as ISO standards (including Management standards & Management systems standards [5], 20889 [6], 27xxx series [7] [8] [9] [10] [11] [12] [13], 29100 [14], 29134 [15], 31000 [16], 31700 [17]), IEC standards 62443 series [18], NIST guidelines (NISTIR 7628 [19] and 8062 [20]) and privacy [21] and security frameworks, EC recommendations on cybersecurity in the energy sector (SWD (2019) 1240 final), LINDDUN privacy threat model [22], STRIDE Threat modelling, MITRE Knowledge bases and the CNIL Privacy Impact Assessment Methodology [23].

5.2. Dashboard presentation

The dashboard for cybersecurity and privacy consists in a series of questionnaires on organisational as well as privacy and cybersecurity aspects. A dashboard overview enables to summarize the main information and high-level indicators, as well as the PSP activities integration within the project life cycle.

The PSP Dashboard has been developed taking into account the requirements elaborated in part 4.2:

- The support and explanations provided by the tool will enable to perform the analysis of system security & vulnerability, while taking into account the different backgrounds and expertise of the different participants.
- The information gathered through the questionnaires will enable to provide reports to the participants providing an overview of the cybersecurity and privacy state and highlighting the areas of the systems in need of improvements.
- The dashboard will enable to show the progress of the analysis to the participants and its completeness.

- The data management plan, which defines the access plan for sharing data, is one of the foundations of the PSP, and will be considered across the analysis.
- The reports provided at the end of the analysis, based on the information gathered in the questionnaires, will include the analysis of potential attacks, and highlight the most relevant ones for simulations.

5.2.1 The Dashboard

The tool is divided in different parts according to each main actions of the plan and the plan itself, as in Figure 4.

1. “Identify Resources”: In the lifecycle of a project, such as a development, implementation, and deployment of a technical system, the first stage is the specification and requirements. In the case of the tool, through a questionnaire, the user will identify the resources needed, human and equipment or software, if necessary.
2. “Preparing a PSP”: Once the resources for the project PSP are identified, the preparation to define the PSP starts. The plan gathers the actions scheduled to manage privacy and security in the system to analyze. From the governance team to the actions, agreements and other information about data management, privacy and security risk analysis, privacy engineering and engagement activities.
3. “Privacy analysis”: This part will support the user to create the Privacy Impact Assessment (PIA) through a questionnaire with specifications and examples in order to better understand each question.
4. “Security Analysis”: This part will support the user to create the Security Risk Analysis of the target system through a questionnaire with specifications and examples to better understand each question.
5. “Manage KPIs”: And the last part provides an evaluation of the results to assign levels of security before and after the measures taken. It is important because it helps in the continuous improvement of the PSP, which is a dynamic “file” or “project”. It needs to be updated as well as the analysis of privacy and security needs to be continuous in different stages of the lifecycle of a project.

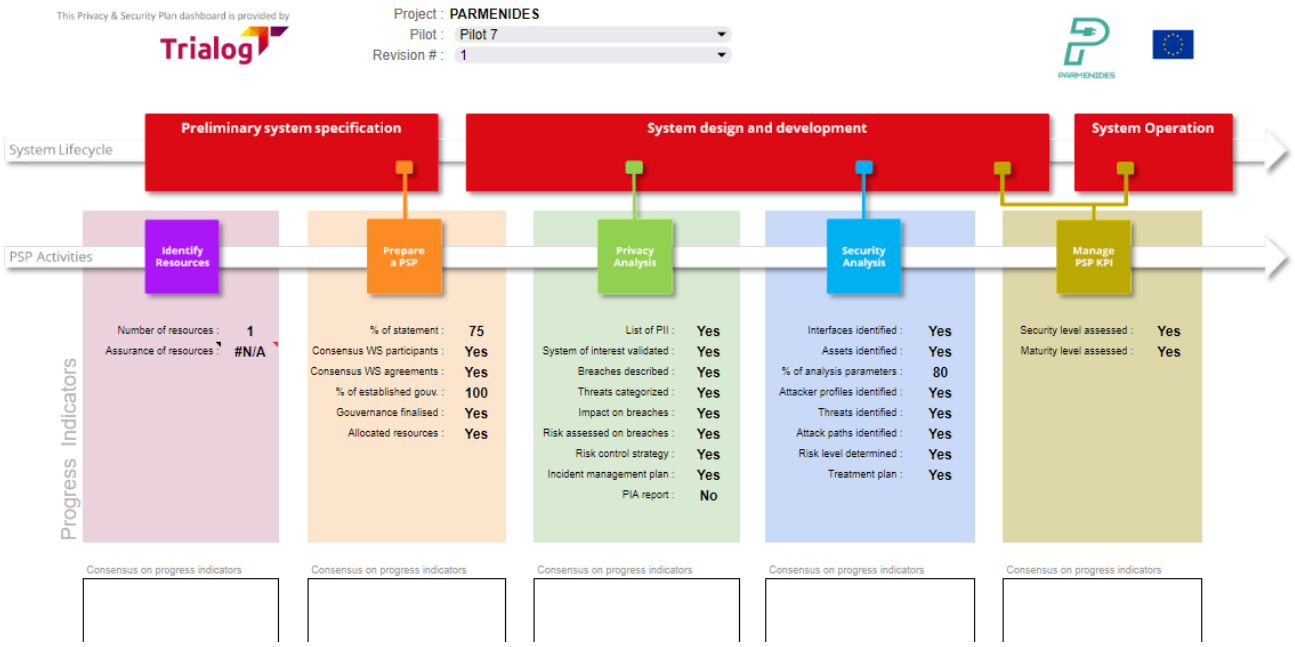


Figure 4: Dashboard overview

This dashboard is mainly used to provide the progression status in the implementation of each activity of the PSP.

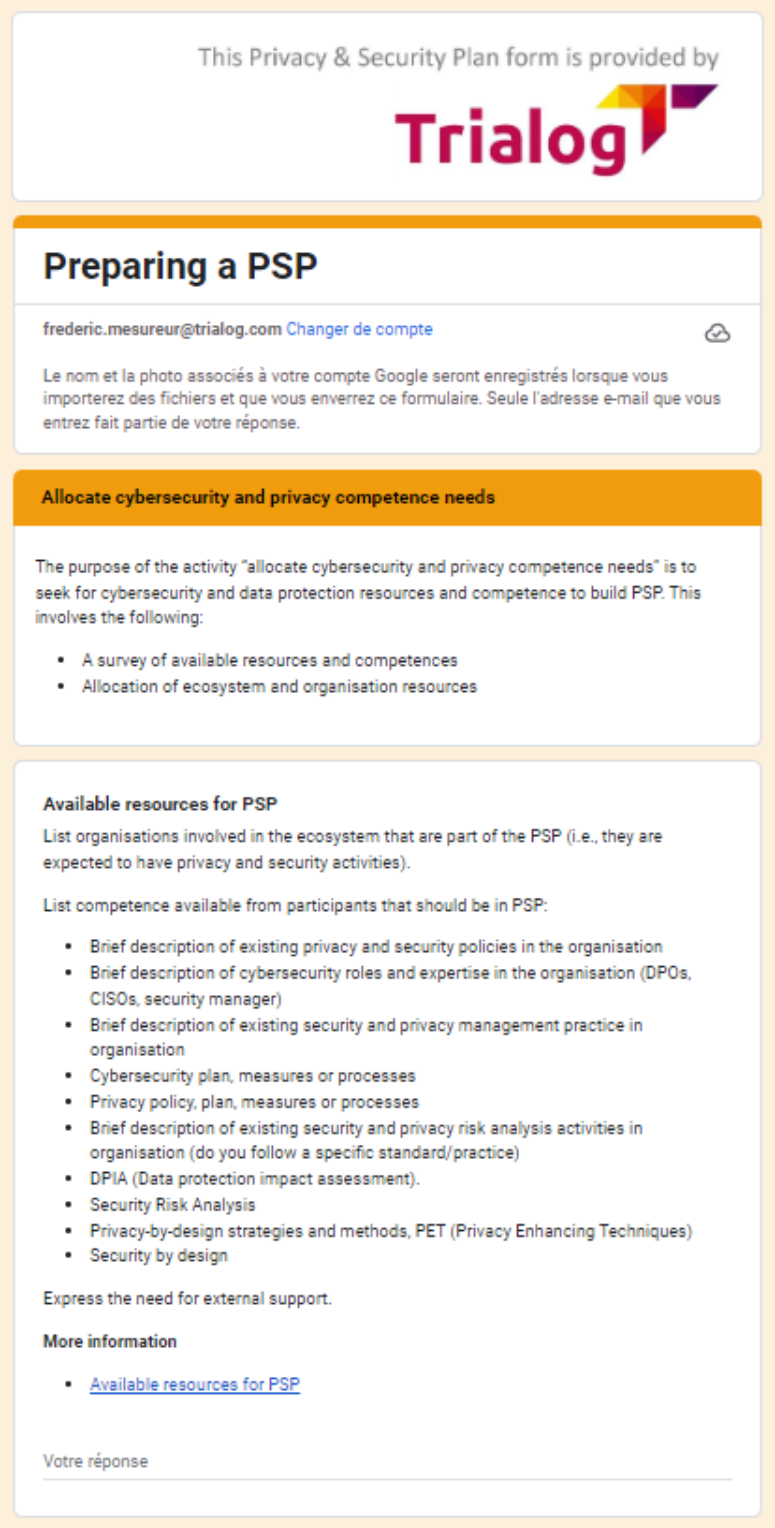
5.2.2 The questionnaires

The questionnaires use in the PSP come as a tooled solution and a complement to the workshops, enabling participants, assisted by Trialog, to fill in all useful information, and facilitates linking the different parameters together. Three questionnaires are designed to focus on the three main aspects of this PSP:

- Organisational information
- Privacy concerns
- Cybersecurity concerns

The questions presented are link to the training previously dispensed. In order to support the user in filling the information, each question is accompanied by the following explanations (see Figure 5 and Figure 6):

- A description of the question
- An example of a possible answer
- A reference to the part of the course related to the question
- An explanation of the use and reason for the question



This Privacy & Security Plan form is provided by

Trialog

Preparing a PSP

frederic.mesureur@trialog.com Changer de compte

Le nom et la photo associés à votre compte Google seront enregistrés lorsque vous importerez des fichiers et que vous enverrez ce formulaire. Seule l'adresse e-mail que vous entrez fait partie de votre réponse.

Allocate cybersecurity and privacy competence needs

The purpose of the activity "allocate cybersecurity and privacy competence needs" is to seek for cybersecurity and data protection resources and competence to build PSP. This involves the following:

- A survey of available resources and competences
- Allocation of ecosystem and organisation resources

Available resources for PSP

List organisations involved in the ecosystem that are part of the PSP (i.e., they are expected to have privacy and security activities).

List competence available from participants that should be in PSP:

- Brief description of existing privacy and security policies in the organisation
- Brief description of cybersecurity roles and expertise in the organisation (DPOs, CISOs, security manager)
- Brief description of existing security and privacy management practice in organisation
- Cybersecurity plan, measures or processes
- Privacy policy, plan, measures or processes
- Brief description of existing security and privacy risk analysis activities in organisation (do you follow a specific standard/practice)
- DPIA (Data protection impact assessment).
- Security Risk Analysis
- Privacy-by-design strategies and methods, PET (Privacy Enhancing Techniques)
- Security by design

Express the need for external support.

More information

- Available resources for PSP

Votre réponse

Figure 5: PSP user help (part1)

AVAILABLE RESOURCE(S) FOR PSP?

List organisations involved in the ecosystem that are part of the PSP (i.e., they are expected to have privacy and security activities)

List competence available from participants that should be in PSP

- Brief description of existing privacy and security policies in the organisation
- Brief description of cybersecurity roles and expertise in the organisation (DPOs, CISOs, security manager)
- Brief description of existing security and privacy management practice in organisation
- Cybersecurity plan, measures or processes
- Privacy policy, plan, measures or processes
- Brief description of existing security and privacy risk analysis activities in organisation (do you follow a specific standard/practice)
- DPIA (Data protection impact assessment).
- Security Risk Analysis
- Privacy-by-design strategies and methods, PET (Privacy Enhancing Techniques)
- Security by design

Express the need for external support

EXAMPLE

None

RATIONALE FOR QUESTION

Identify resources that can be allocated to PSP definition and implementation.

PREREQUISTE

Definition of system and assessment of need completed and governance for PSP established.

PREREQUISTE DESCRIPTION

None

REFERENCE TO THE COURSE

Module A (preparing a PSP)

Slide: 37 and 38

Figure 6: PSP user help (part2)

6. Conclusion

The work done in Task 3.3 prepares and lays the necessary foundations for the PARMENIDES cybersecurity and privacy analysis. The review of the partners status and expectations, shows that they have various levels of maturity and expertise in the analysis of their systems and development of cybersecurity and privacy features.

This task enabled to assess the status of the pilots and systems in terms of cybersecurity and privacy and prepare for the definition of the Privacy and Security Plan, that will occur in Task 5.2, across the development phase of the PARMENIDES solutions.

A series of requirements, defined in collaboration with solution providers, enabled to tailor the PSP methodology and dashboard to their need. The PSP dashboard aims to support the solution providers, throughout the PSP analysis that will take place in Task 5.2, to achieve a sufficient and homogeneous level of cybersecurity in the project.

References

[1] Interconnect project, Grant agreement No 857237, “The Semantic Interoperability Framework,” in *Sustainable Places*, Brussels, 2022.

[2] H2020 Project , “Energica website,” [Online]. Available: http://energica-h2020.eu/fr/.

[3] European Commission, “What personal data is considered sensitive?,” [Online]. Available: https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en#:~:text=personal%20data%20revealing%20racial%20or,sex%20life%20or%20.

[4] NIS2 Directive, “NIS2 Requirements,” [Online]. Available: https://nis2directive.eu/nis2-requirements/.

[5] ISO, “Management system standards,” ISO, [Online]. Available: https://www.iso.org/management-system-standards.html. [Accessed 06 01 2023].

[6] ISO, “ISO/IEC 20889:2018 Privacy enhancing data de-identification terminology and classification of techniques,” 2018. [Online]. Available: https://www.iso.org/standard/69373.html. [Accessed 06 01 2023].

[7] ISO, “ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines,” 2019. [Online]. Available: https://www.iso.org/standard/71670.html. [Accessed 06 01 2023].

[8] ISO, “ISO/IEC TS 27570:2021 Privacy protection — Privacy guidelines for smart cities,” 2021. [Online]. Available: https://www.iso.org/standard/71678.html. [Accessed 06 01 2023].

[9] ISO, “ISO/IEC 27556:2022 Information security, cybersecurity and privacy protection — User-centric privacy preferences management framework,” 2022. [Online]. Available: https://www.iso.org/standard/71674.html. [Accessed 06 01 2023].

[10] ISO, “ISO/IEC TR 27550:2019 Information technology — Security techniques — Privacy engineering for system life cycle processes,” 2019. [Online]. Available: https://www.iso.org/standard/72024.html. [Accessed 06 01 2023].

[11] ISO, “ISO/IEC CD 27561.2 Information technology — Security techniques — Privacy operationalisation model and method for engineering (POMME),” ISO, [Online]. Available: https://www.iso.org/standard/80394.html. [Accessed 06 01 2023].

[12] ISO, “ISO/IEC 27400:2022 Cybersecurity — IoT security and privacy — Guidelines,” 2022. [Online]. Available: https://www.iso.org/standard/44373.html. [Accessed 06 01 2023].

[13] ISO, “ISO/IEC 27559:2022 Information security, cybersecurity and privacy protection – Privacy enhancing data de-identification framework,” 2022. [Online]. Available: https://www.iso.org/standard/71677.html. [Accessed 06 01 2023].

[14] ISO, “ISO/IEC 29100:2011 Information technology — Security techniques — Privacy framework,” 2011. [Online]. Available: https://www.iso.org/standard/45123.html. [Accessed 06 01 2023].

[15] ISO, “ISO/IEC 29134:2017 Information technology — Security techniques — Guidelines for privacy impact assessment,” ISO, 2017. [Online]. Available: https://www.iso.org/standard/62289.html. [Accessed 06 01 2023].

[16] ISO, “ISO 31000:2018 (en) Risk management — Guidelines,” 2018. [Online]. Available: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en. [Accessed 06 01 2023].

[17] ISO, “ISO 31700-1 Consumer protection — Privacy by design for consumer goods and services — Part 1: High-level requirements,” 2023. [Online]. Available: https://www.iso.org/standard/84977.html. [Accessed 06 01 2023].

[18] ISA, “ISA/IEC 62443 Series of Standards,” 2022. [Online]. Available: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards. [Accessed 06 01 2023].

[19] NIST, “NISTIR 7628 Rev. 1 Guidelines for Smart Grid Cybersecurity,” 2014. [Online]. Available: https://csrc.nist.gov/publications/detail/nistir/7628/rev-1/final. [Accessed 06 01 2023].

[20] NIST, “NISTIR 8062 An Introduction to Privacy Engineering and Risk Management in Federal System,” NIST, 2017. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf. [Accessed 06 01 2023].

[21] NIST, “Privacy Framework,” 2022. [Online]. Available: https://www.nist.gov/privacy-framework. [Accessed 06 01 2023].

[22] Lindunn, “LINDDUN privacy engineering,” 2020. [Online]. Available: https://www.linddun.org/. [Accessed 06 01 2023].

[23] CNIL, “Privacy impact assessment (PIA),” 02 2018. [Online]. Available: https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf. [Accessed 06 01 2023].

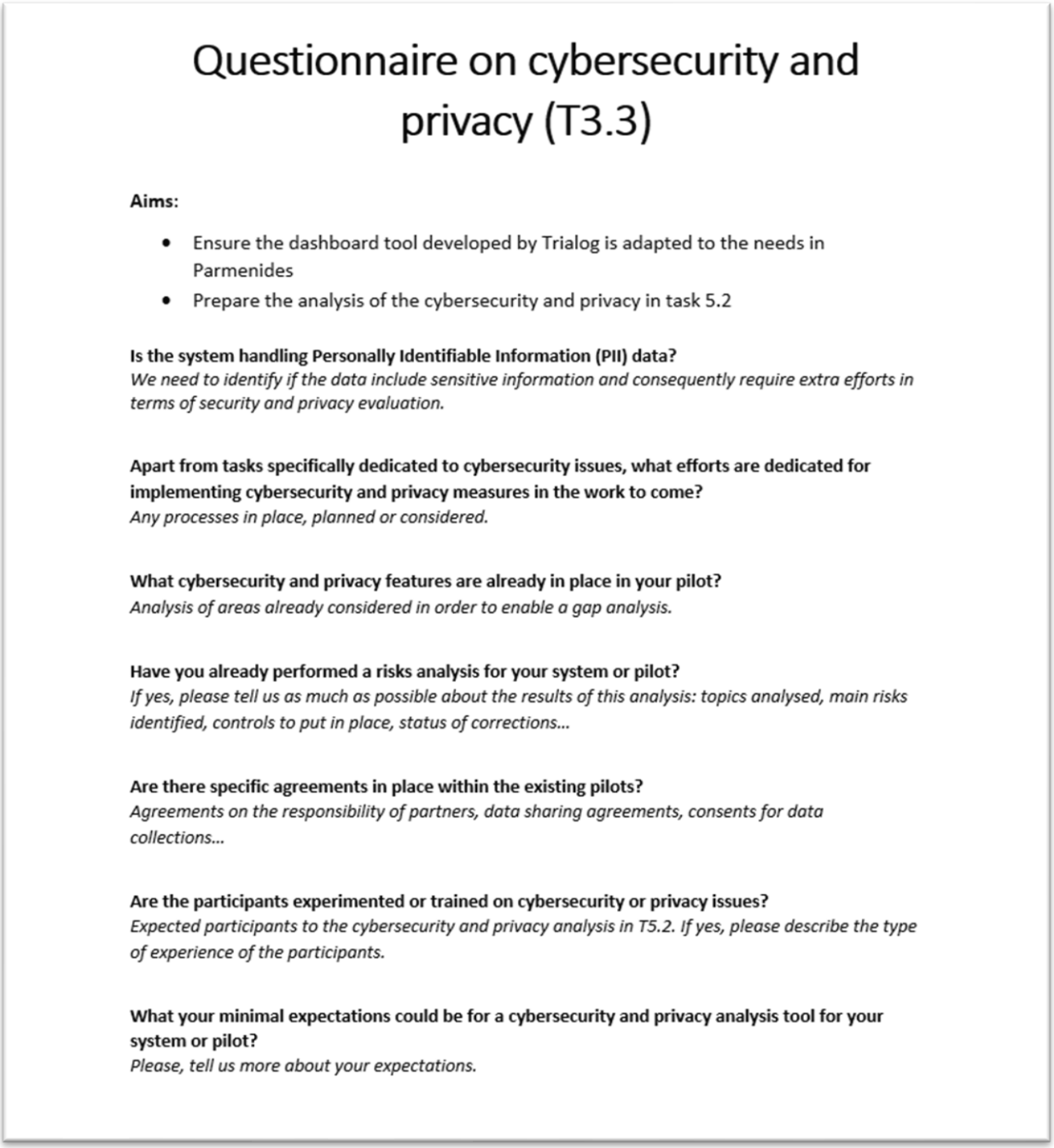
[24] European project Sender (GA n°957755), “Deliverable 4.2: Security and Privacy protection action plan and results,” 2022.

[25] European project Maesha (GA n°957843), “Deliverable D7.3: Security and privacy protection actions plan and results,” 2022.

[26] Interconnect European project Grant agreement No 857237, “Deliverable 2.1: Secure interoperable IoT smart home/building and smart energy system reference architecture,” 2020.

7. Annex

7.1. Annex A: Questionnaire



Questionnaire on cybersecurity and privacy (T3.3)

Aims:

- Ensure the dashboard tool developed by Trialog is adapted to the needs in Parmenides
- Prepare the analysis of the cybersecurity and privacy in task 5.2

Is the system handling Personally Identifiable Information (PII) data?
We need to identify if the data include sensitive information and consequently require extra efforts in terms of security and privacy evaluation.

Apart from tasks specifically dedicated to cybersecurity issues, what efforts are dedicated for implementing cybersecurity and privacy measures in the work to come?
Any processes in place, planned or considered.

What cybersecurity and privacy features are already in place in your pilot?
Analysis of areas already considered in order to enable a gap analysis.

Have you already performed a risks analysis for your system or pilot?
If yes, please tell us as much as possible about the results of this analysis: topics analysed, main risks identified, controls to put in place, status of corrections…

Are there specific agreements in place within the existing pilots?
Agreements on the responsibility of partners, data sharing agreements, consents for data collections…

Are the participants experimented or trained on cybersecurity or privacy issues?
Expected participants to the cybersecurity and privacy analysis in T5.2. If yes, please describe the type of experience of the participants.

What your minimal expectations could be for a cybersecurity and privacy analysis tool for your system or pilot?
Please, tell us more about your expectations.

Figure 7: Questionnaire use during task T3.3 to gather partners feedback

7.2. Annex B: Summary of the answers to the cybersecurity and privacy questionnaire

Table 3: Summary of questionnaire partners answers

Question	AIT	ENS	MAPS	KTH
Use of PII	Yes	Yes	Yes	Yes
Use of sensitive data	No	No	No	No
Efforts for Cybersecurity and Privacy	Effort during the solution development	Unknown	Efforts during the software design and development are done	Use of a BMS with cybersecurity and privacy compliance
Features for Cybersecurity and Privacy	Audit logs, data encryption, docker container, database anonymization, data only accessible from services on RDP	Grid assets and communication in the low voltage grid are protected via grid operator specific cybersecurity and privacy	ISO/IEC 27001, back-end components on private machines, use of cloud best practices, inc. identity management system, compliance with OWASP requirements related to TLS	BMS from Schneider Electric including extensive functionality
Risk analysis	Yes	Yes	Yes	No
Specific agreements	NDA with ENS for using anonymized customer data	Customer will be informed and agreed on a privacy statement and declaration of consent NDA with MAPS, AIT & Siemens for sharing anonymized customer data	No	Yes, agreement between KTH Live-in Lab and its tenants
Participants experience	Yes (GDPR, privacy, PII, etc)	Unknown	Only on GDPR	No
Expectations for PSP				
Privacy and cybersecurity training	X			X
Privacy and cybersecurity analysis	X		X	X
Action plan for improvement	X	X	X	X
Evidence of Compliance	X	X		X
Definition of access plan for data to be shared	X	X	X	X
Simulation of attack	X		X	

7.3. List of Figures

7.4. List of Tables

PARMENIDES

PARMENIDES

PlugGplAy eneRgy ManagEmeNt for hybrID Energy Storage