



# **iVPP secure data monitoring and governance**

## **AUTHORS:**

**Lucas Pons Bayarri, Mario González Carabayo, Moisés Antón García (ETRA I+D)**



**H2020-LC-SC3-2018-2019-2020 / H2020-LC-SC3-2020-EC-ES-SCC**

**EUROPEAN COMMISSION**

Innovation and Networks Executive Agency

Grant agreement no. 957810

## PROJECT CONTRACTUAL DETAILS

<b>Project title</b>	IntegrATed SolutioNs for the DecarbOnization and Smartification of Islands
<b>Project acronym</b>	IANOS
<b>Grant agreement no.</b>	957810
<b>Project start date</b>	01-10-2020
<b>Project end date</b>	30-09-2024
<b>Duration</b>	48 months
<b>Project Coordinator</b>	João Gonçalo Maciel (EDP) - JoaoGoncalo.Maciel@edp.com

## DOCUMENT DETAILS

<b>Deliverable no.</b>	D4.1
<b>Dissemination level</b>	Public
<b>Work package</b>	WP4 – IANOS Multi-Layer VPP Operational Framework
<b>Task</b>	Task 4.1
<b>Due date</b>	31-03-2022
<b>Actual submission date</b>	31-03-2022
<b>Lead beneficiary</b>	ETRA

<b>Vers.</b>	<b>Date</b>	<b>Beneficiary</b>	<b>Changes</b>
0.1	11.03.2022	ETRA ID	First version to be reviewed
0.2	14.03.2022	NEROA	Peer Review by NEROA
0.3	24.03.2022	CERTH	Peer Review by CERTH
0.4	28.03.2022	ETRA ID	Update based on the Peer Review
1.0	31.03.2022	ETRA ID	Final version



# Executive Summary

This document is part of the deliverables of the IANOS project. It represents D4.1 “iVPP secure data monitoring and governance (v1)”. This deliverable has been elaborated in the framework of Task 4.1 “Cyber-Secure data monitoring and VPP Governance”, that will develop security and privacy environment by design. This deliverable is developed under WP4 that targets the development and delivery of the necessary ICT components that constitute the iVPP platform. These components would entail the interoperable and secure data management platform, forecasting and segmentation algorithms, the Centralized Dispatcher, the intelligent coordination mechanisms for delivering optimal dispatch decisions, along with the Virtual Energy console and the P2P transactive energy layer.

The purpose of the deliverable within the context of IANOS is to show the development of the mechanisms in the IANOS project that assure the secure APIs and communication pipelines that will be developed for sending the required information in-between VPP with field devices and VPP with external systems (namely the IANOS Enterprise Service Bus and the DEP-Fi). Additionally, this deliverable would provide an overview of the status and developments of legislation on the Personal Data Protection (PDP) and Smart Grid (SG) security. Moreover, cyber-security aspects will be highlighted to establish the basis under which the IANOS project will be based. Moreover, this deliverable will also provide an investigation of the IANOS products regarding the incorporation of types of data processing operations which could potentially result in a high risk to the rights and freedoms of natural persons.

The IANOS iVPP framework functionalities and energy services foreseen in the IANOS project, require a successful exchange and operative handling of data and control commands among the different system components and field devices. Both the iVPP secured Enterprise Service Bus (ESB) and the DefPi will be in charge of these data transferring focusing on cyber-security aspects. The required communication protocols and the transformation of data to a common information model will be performed in the beforementioned components. The different components will be connected in the VPP orchestration toolkit using diverse gateways that will adapt the specific data model to the common information model. The model will allow a smooth communication from different field devices, at the same time that intelligent agents and applications in the VPP will not have to worry about the details (connectivity, data models) of these specific devices. This development will progress accordingly considering the ongoing work in the Smart Grid Task Force and its Experts groups

## Disclaimer

This publication reflects the author's view only and the European Commission is not responsible for any use that may be made of the information it contains.

# Table of Contents

List of Figures.....	7
List of Tables .....	8
1 Introduction.....	9
1.1 Objectives and Scope .....	9
1.2 Structure of the deliverable .....	9
1.3 Relation to other tasks and deliverables.....	10
1.4 Abbreviations.....	10
2 Data Privacy Protection .....	11
2.1 General Data protection Legislation and Institutional Setup .....	11
2.1.1. General Data Protection Regulation and institutional setup in EU .....	11
2.1.2 Data protection legislation in Europe and Data Protection Authorities .....	12
2.2 Concepts of data protection.....	13
2.2.1 Established concepts in EU – “By design” and “By default” .....	13
2.3 Responsibilities of actors in data collection, processing, and use .....	13
2.3.1 Data controller, Data processor, and Recipient.....	13
2.3.2. Accountability .....	14
2.3.2.1 Lawfulness, fairness, and transparency .....	15
2.3.2.2. Purpose limitation and storage limitation .....	15
2.3.2.3 Data minimization.....	15
2.3.2.4 Personal data used for research or statistical purposes .....	15
2.3.2.5. Accuracy .....	16
2.3.2.6. Confidentiality and Integrity.....	16

<b>2.4 Obligations for companies.....</b>	<b>16</b>
2.4.1 Documentation on data processing activities.....	17
2.4.2 Data Protection Officer .....	17
<b>2.5 International transfer of personal data .....</b>	<b>18</b>
2.5.1 Adequacy of data protection in third countries.....	18
2.5.2 Harmonization of data protection rules.....	18
<b>2.6 Data Protection Impact Assessment.....</b>	<b>18</b>
2.6.1 Legislative requirements.....	18
2.6.2 Guidelines and implementation .....	19
<b>3. Security of network and infrastructure.....</b>	<b>25</b>
3.1 Directives.....	25
3.2 Utility cybersecurity risks .....	26
<b>4. Data privacy and security in IANOS products.....</b>	<b>28</b>
4.1 DPIA – Pre-assessment questionnaire for IANOS products.....	28
4.1.1 Cases foreseen by the GDPR, DPAs or EDPB.....	28
4.1.2 Relevant occurrence .....	30
4.1.3 Personal data involved and DPIA-related processing activities.....	30
4.1.4 Status of a data controller or a data processor .....	31
4.1.5 New technologies and other criteria .....	31
4.2 Questionnaire results – DPIA Pre-assessment .....	31
4.2.1 Grid Oriented Optimizer.....	31
4.2.2 LCA/LCC Toolkit.....	32
4.2.3 Crowdequity Platform.....	33
4.2.4 TNO Reflex .....	34
4.2.5. System Modeler .....	35
4.2.6 OptiMEMS.....	36

4.2.7 CleanWatts KIPLO .....	37
4.2.8 Aggregation and Classification Intelligence.....	38
4.2.9 Forecasting Engine.....	39
4.2.10 DLT-based Transactive Platform.....	40
4.2.11 Virtual Energy Console.....	41
4.2.12 Enterprise Service Bus .....	41
4.2.13 Non-intrusive characterization of energy flexibility in water heating systems .....	42
4.2.14 FEID-PLUS .....	43
4.2.15 Smart Energy Router .....	44
4.2.16 Hybrid Transformer .....	45
4.2.17 V2G Charging.....	46
<b>5. IANOS Secured Enterprise Service Bus .....</b>	<b>47</b>
5.1 General considerations.....	47
5.2 IANOS Common Architecture.....	49
5.3 Connection guide.....	50
5.3.1 RabbitMQ connection .....	50
5.3.2 Example in Python.....	50
5.3.3 Encrypted MQTT connection .....	51
5.3.4. Connect to the proposed list of topics.....	52
5.3.4 API usage .....	53
5.3.5 Collections allowed .....	54
5.4 Standards and Data models .....	55
5.5 Available data models for IANOS .....	58
5.5.1 Rationale .....	59
5.5.2 Data format for field devices messages .....	59
5.5.3 Measurements and states names .....	61
5.5.4 Data communication for field device messages .....	63

5.5.5 Platform security .....	64
5.6 Secured ESB weather information communication data model .....	64
5.6.1 Rationale .....	64
5.6.2 Data model for weather information messages .....	64
5.6.3 Real time weather messages data model .....	64
5.6.4 Forecasted weather messages data model .....	65
5.6.6 Request API .....	65
5.6.7 Subscribe to real time weather data .....	66
6.Conclusions .....	67
7.References.....	69
8. Annex .....	73
8.1 Grid Oriented Optimizer .....	73
8.2 LCA/LCC Toolkit.....	75
8.3 Crowdequity Platform .....	78
8.4 Reflex TNO .....	80
8.5 System Modeler.....	83
8.6 OptiMEMS .....	86
8.7 CleanWatts KIPLO .....	88
8.8 Aggregation and Classification Intelligence .....	91
8.9 Forecasting Engine .....	93
8.10 DLT-based Transactive Platform.....	95
8.11 Virtual Energy Console .....	98
8.12 Enterprise Service Bus.....	100

8.13 Non-intrusive characterization of energy flexibility in water heating systems.....	102
8.14 FEID-PLUS.....	104
8.15 Smart Energy Router .....	106
8.16 Hybrid Transformer.....	109
8.17 V2G Charging .....	111

## List of Figures

Figure 1: Basic principles related to DPIA in the GDPR [10] .....	20
Figure 2: Generic iterative process for carrying out DPIA [10] .....	22
Figure 3: End-to-end view of DPIA workflow [11] .....	23
Figure 4: Electricity sector interdependencies .....	26
Figure 5: RIVER architecture logo .....	47
Figure 6: CITRIC architecture.....	47
Figure 7: Generic Layout of the IANOS' iVPP modules defined in D4.7 "The iVPP Centralized Dispatcher" .....	49
Figure 8: Deployment for Terceira demonstration site. Based on the architecture defined in D4.7 "The iVPP Centralized Dispatcher" .....	49
Figure 9: Deployment for Ameland demonstration site. Based on the architecture defined in D4.7 "The iVPP Centralized Dispatcher" .....	50
Figure 10: Login request with response using Postman.....	53
Figure 11: Request and response to the messages queue .....	54
Figure 12: Filtered by ID on the route .....	55
Figure 13: Interoperability definition.....	55
Figure 14: Interoperability categories .....	56
Figure 15: Common data exchange format interoperability.....	57
Figure 16: Information exchanges matrix.....	57

## List of Tables

Table 1: Abbreviation list.....	10
Table 2: Questions of Subsection I of the DPIA-PA Questionnaire for products.....	29
Table 3: Questions on Section 2 of the DPIA-PA Questionnaire for products .....	30
Table 4: Questions of Subsection 3 of the DPIA-PA Questionnaire for products.....	30
Table 5: Questions on Section 4 of the DPIA-PA Questionnaire for products .....	31
Table 6: Questions on section 5 of the DPIA-PA Questionnaire for products .....	31
Table 7: CITRIC platform suggests technologies for bulk data ingestion .....	48
Table 8: List of connection to the proposed list of topics .....	52
Table 9: Exchanged Information types.....	58
Table 10: Measurements and states names lists .....	62
Table 11: States names list.....	63
Table 12: Storage specific measurements names lists .....	63
Table 13: Storage specific status names lists .....	63
Table 14: Coordinates Ameland demonstration site .....	66
Table 15: Coordinates Terceira demonstration site.....	66
Table 16: DPIA-PA Questionnaire for Grid Oriented Optimizer .....	75
Table 17: DPIA-PA Questionnaire for the LCA/LCC Toolkit.....	78
Table 18: DPIA-PA Questionnaire for Crowdequity Platform.....	80
Table 19: DPIA-PA Questionnaire for TNO Reflex.....	83
Table 20: PIA-PA Questionnaire System Modeler .....	86
Table 21: DPIA-PA Questionnaire for OptiMEMS.....	88
Table 22: DPIA-PA Questionnaire for KIPLO.....	91
Table 23: DPIA-PA Questionnaire for the Aggregation and Classification Intelligence .....	93
Table 24: DPIA-PA Questionnaire for Forecasting Engine .....	95
Table 25: DPIA-PA Questionnaire for the DLT-based Transactive Platform.....	98
Table 26: DPIA-PA Questionnaire for Virtual Energy Console.....	100
Table 27: DPIA-PA Questionnaire for Enterprise Service Bus.....	102
Table 28: DPIA-PA Questionnaire for Non-Intrusive characterization of energy flexibility in water heating systems .....	104
Table 29: DPIA-PA Questionnaire for FEID-Plus.....	106
Table 30: DPIA-PA Questionnaire for Smart Energy Router .....	109
Table 31: DPIA-PA Questionnaire for Hybrid Transformer.....	111
Table 32: DPIA-PA Questionnaire for V2G charger .....	113

# 1 Introduction

## 1.1 Objectives and Scope

The main objective of this deliverable is to present a description of the development of the iVPP Enterprise Service Bus (ESB) and its background to guarantee a secure communication among the components in the IANOS architecture. Additionally, this deliverable would provide an overview of the status and developments of legislation on the Personal Data Protection (PDP) and Smart Grid (SG) security. Moreover, cyber-security aspects will be highlighted. Moreover, this deliverable will also provide an investigation of the IANOS products regarding the incorporation of types of data processing operations which could potentially result in a high risk for the rights and freedoms of natural persons. The document will provide an overview of the current and future developments in the implementation of required regulations to ensure a safe transfer of data. This would enable the ESB to run seamlessly the data transfer within in-between VPP components with field devices and VPP with external systems. The development of the ESB system will be based on the RIVER architecture, which is based on the CITRIC smart city platform developed by ETRA. This platform will be composed by a plethora of services and modules that support different technologies for the bulk data ingestion (API REST, MWTT, AMPQT, WS DDP, NATS, CoAP, Cron ETL). Nevertheless, this architecture will be adapted and extended to support the functionalities required in IANOS architecture which differs from one pilot demonstration site to the other. In order to perform this adaptation, this deliverable will provide the role of the ESB and the Def-Pi within the rest of the iVPP platform based on the results outperformed in Task 4.4 “Optimized cross-resource VPP coordination for energy service provisions”. This first version will take a deeper look on the horizontal functionalities of the Enterprise Service Bus, whereas the upcoming version of this deliverable regarding Task 4.1 “Cyber-Secure data monitoring and VPP governance” will take a deeper look on the IANOS Def-Pi platform. This deliverable will be used additionally as an introduction to the data models from which the IANOS ecosystem will be benefiting from. This document will also provide a guideline for the connection of the different iVPP components and assets that compose the IANOS layout in Ameland and Terceira that will allow the smooth interconnection to facilitate the communication.

## 1.2 Structure of the deliverable

The deliverable consists of six different chapters that are structured as follows:

- [Chapter 1](#) provides an introduction of the document, presenting the objectives and scope of the deliverable, the structure and the relation with other tasks, deliverables, and work packages in IANOS.
- [Chapter 2](#) provides a framework of the general data protection legislation and institutional setup as an introductory framework on the need of privacy that the IANOS project will be assuring.
- [Chapter 3](#) introduces a theoretical framework of the need for security, emphasizing its important role in the modern society and critical infrastructures in digital technologies and the network.
- [Chapter 4](#) introduces the data privacy and security framework related to IANOS products, as a proof of cyber-security data monitoring role that would be affecting the integrity of data introducing a criterion to conduct a Data Protection Impact Assessment (DPIA) schema.
- [Chapter 5](#) presents the Enterprise Service Bus (ESB) that will facilitate the data information exchange across the different products and assets taking place in the IANOS infrastructure. This chapter will introduce the architecture structure which the project will follow, how it is correlated with the IANOS overall architecture.

- [Chapter 6](#) introduces the conclusion of the information presented in the document.
- [Annex](#) will introduce the responses from the different technology providers regarding the Pre-Assessment to determine whether a Data Protection Impact Assessment is necessary or not. This is directly correlated to the purpose identified in [Chapter 4](#).

## 1.3 Relation to other tasks and deliverables

This deliverable is based on the architecture defined in WP2 “Requirements Engineering & Decarbonization Road mapping”, which is particularly based on the SGAM framework architecture defined in Task 2.5 “System Architecture”. At the same time, this task is highly dependent on Task 2.1 “Islands requirements engineering and use case definitions” in which the different IANOS Use Cases (UC) are presented. The role of the iVPP’s modules and its interactions among them has primarily been defined in T4.4 “Optimized cross-resource VPP coordination for energy service provisions”. This task sets the intercommunication among the different assets established in the two IANOS Lighthouses Islands Ameland (WP5 – Deployment, Use Cases Realization and Monitoring at LH#1) and Terceira (WP6 - Deployment, Use Cases Realization and Monitoring at LH#2) based on the Use Cases definitions (UC), but also among the several modules developed and deployed of the iVPP dedicated tasks in WP4 (from T4-1 to T4.5). Additionally, the deliverable takes into account the security standards defined in T1.4 “Ethics and Cyber Security Management report”.

## 1.4 Abbreviations

Abbreviation	Definition
AP	Autoriteit Persoonsgegevens
CNPD	Portuguese Data Protection Authority
DPA	Data Protection Authorities
DPO	Data Protection Officer
ECI	European Critical Infrastructure
EDPB	European Data Protection Board
ESB	Enterprise Serviced Bus
GDPIA	Guidelines on Data Protection Impact Assessment
GDPR	General Data Protection Regulation
IED	Intelligent Electronic Device
IoT	Internet of Things
JSON	JavaScript Object Notation
MS	Member States
PDP	Personal Data Protection
P2P	Peer-to-Peer
PLC	Programable Logic Controller
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SG	Smart Grid
SGAM	Smart Grid Architecture Model
SME	Small Medium Enterprises
SMS	Smart Metering System
SSL	Secure Socket Layer
UC	Use Cases
VPP	Virtual Power Plant

Table 1: Abbreviation list

## 2 Data Privacy Protection

### 2.1 General Data protection Legislation and Institutional Setup

#### 2.1.1. General Data Protection Regulation and institutional setup in EU

The General Data Protection Regulation (GDPR) [1] on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, was adopted on 27 April 2016 and entered into force on 25 May 2018. GDPR repealed the Directive 95/46/EC, which used to regulate the protection of individuals with regard to the processing of personal data and on the free movement of such data, and on which grounds the issue was regulated in the national laws of EU MSs.

The main objectives of the GDPR are allowing citizens to have control over their personal data and making the regulatory environment for international corporations easier by harmonizing regulations throughout the EU. According to GDPR, the term 'personal data' is clarified as: "any information relating to an identified or identifiable natural person ('data subject')". An identifiable natural person is someone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. The basic principles of personal data processing are the following:

- Lawfulness, fairness and transparency;
- Purpose limitation;
- Data minimization;
- Accuracy;
- Storage limitation;
- Integrity and confidentiality.

Further, the regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. However, it does not apply to the processing of personal data "by a natural person in the course of a purely personal or household activity" nor "by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security [1].

With regards to the territorial scope of the regulation, it is prescribed that the "Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not", as well as, that the "Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union...". Consequently, the GDPR regulation presents a reform of PDP in the European Union which was created in accordance with technological development and novel ways of processing personal data. As long as citizens are concerned with GDPR, easier access to their data is imposed, and they are informed in a much clearer and more understandable manner how and for which purposes of their data is processed. Furthermore, the Regulation introduces the concept the right to be forgotten. That is to say, the right of a citizen with clear safeguards to ask business or organization to delete their data, when they do not want their personal data to be further processed, provided that there are no legitimate reasons for its retention. In

the event of a personal data breach, the processing manager shall inform the corresponding Data Protection Authority (DPA) on the personal data breach without undue delay, unless it is unlikely that the personal data breach would affect the risk to individuals' rights and freedoms. Furthermore, under certain circumstances, the necessity to alert the data subject in case there is a violation of their personal data is introduced. For certain controllers, the obligation to appoint a Data Protection Officer (DPO) is also introduced. GDPR makes the transfer of personal data simpler within the European Union. It opens possibilities for business competition within the EU member states. Additionally, it also regulates the use of personal data for statistical and research purposes. GDPR also strengthens activities of DPAs of EU MSs by establishing the European Data Protection Board (EDPB), which collects all the MSs' DPAs. This entity has powers to provide guidance and interpretation and it also adopts binding decisions in case several EU countries are concerned under the same case.

### ***2.1.2 Data protection legislation in Europe and Data Protection Authorities***

Current data protection legislation in the examined countries (the Netherlands and Portugal) is protected under the General Data Protection Regulation (GDPR). This legislation took effect on 25<sup>th</sup> May 2018, replacing the EU Data protection Directive (Directive 95/46/EC).

In the Netherlands, the GDPR legislation (Regulation (EU) 2016/679) and the Dutch Implementation replaced additionally the former Dutch Personal Data Protection Act [2]. Although GDPR has introduced a single legal framework in the EU, it includes provisions that allow EU MSs to enact national legislation regarding certain elements of the GDPR in the Netherlands. According to Article 44 of the Act, Articles 15, 16, and 18 of the GDPR do not apply in case personal data is processed by institutions or services for scientific research or statistics, and the required safeguards are put in place to ensure that the personal data can only be used for such purposes. Considering to the Dutch National implementation of Article 89 of the GDPR, Article 45, Articles 15, 16, 18(1)(a), and 20 of the GDPR do not apply in cases where personal data is processed that is included in archives within the meaning of the Public Records Act. The data subject has the right of access to the archived records unless the request for access cannot reasonably be granted because the request is not specified sufficiently. A data subject has the right to add its own understanding of the relevant data to the archived records in cases where incorrect personal data is processed. The AP has published an overview of types of processing activities which require a Data Protection Impact Assessment, which include activities related to: large-scale monitoring, blacklist of personal data concerning criminal convictions, offences, wrongful conduct and payment performance, large-scale processing of health data, partnerships between municipalities, government bodies and other public or private parties when personal or sensitive data is shared, large scale systematic camera surveillance information, systematic and extensive assessment of personal traits by means of automated processing profiling or large-scale automated processing of personal data in order to monitor or influence behaviour [3].

In Portugal, the fundamental right to personal data protection was established in the Constitution of the Portuguese Republic 1976. The first Portuguese Data Protection Act No.10/91 was adopted in 1991, foreseeing the creation of the Portuguese supervisory authority in data protection matters. Prior to the entry into force of the GDPR, the general rule was established as follows: before initiating any personal data processing, the controlled had to notify the Portuguese data protection authority (CNPD) to obtain prior

processing authorisation from the same entity. Portugal has adopted additional data protection obligations besides the GDPR. These sector specific laws are [4]:

- Law No. 12/2005 of 26 January, which contains specific provisions regarding data protection on genetic and health information; and
- Law No. 41/2004 of 18 August, which regulates the protection of personal data in the electronic communications sector and contains specific provisions for telecommunication service providers.

## 2.2 Concepts of data protection

### 2.2.1 Established concepts in EU – “By design” and “By default”

GDPR [1], allows for two basic concepts of data protection – Data protection by design and Data Protection by default, which are the two main pillars of the EU approach to the matter:

- **Protection by design** understands implementation of technical measures at the earliest stages of the design of the processing operation with the aim to secure privacy and data protection.
- **Protection by default** relates measures to ensure that personal data is processed with the highest privacy protection so as to make inaccessible default personal data to an indefinite number of persons.

According to GDPR, to allow the demonstration of its compliance, any controller should adopt internal policies and implement measures that meet the principles of data protection by design and data protection by default. These measures may consist in minimizing the processing of personal data, pseudonymizing personal data, adopting transparency concerning the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features.

## 2.3 Responsibilities of actors in data collection, processing, and use

### 2.3.1 Data controller, Data processor, and Recipient

The **data controller** decides on the purpose and the means of processing data. GDPR precisely defines a data controller as a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided by Union or Member State law [5].

**Data processor** provides the service of data processing for the data controller. This entity means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. This is subject to the definition of the term processing, which is referred to any operation or set of operations which is performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction [5].

The obligations and mutual relations of the controller and processor are defined in a precise manner, within Chapter IV of GDPR [5]. The same applies for the rest of the actors that could participate in the process of data processing. The role of recipient or third party

can also be highlighted from that chapter of the GDPR regulation. The definitions on these actors are given in the following:

- **Representative** is a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27. It represents the controller or processor with regard to their respective obligations under the GDPR Regulation
- **Third party** means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;
- **Recipient** is a natural or legal person, public authority, agency or another body, to which the personal data is revealed, whether it is a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law will not be regarded as recipients. This data processing shall be in compliance with the applicable data protection rules according to the purposes of the processing.

Both in the Netherlands and in Portugal are no additional requirements next to the GDPR. Its provision is applied to the Controller and Processor contracts processes.

### 2.3.2. Accountability

The actors in data processing shall prove their accountability to carry out responsibilities allocated to them with GDPR Regulation. These responsibilities are built on the main principles relating to personal data processing, which are stipulated in Article 5 of GDPR [5]. Considering the importance of this Article, it is entirely cited in the following:

(1) Personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency principles).
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89 (1), not be considered to be incompatible with the initial purposes.
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).
- Accurate.
- where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed are erased or rectified without delay ('accuracy').
- Stored in a form that allows the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 (1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation').
- Data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

The controller shall be responsible for, and be able to demonstrate compliance with, accountability. In fact, the principles prescribed in Article 5 of GDPR are twofold. They essentially concerned about the rights of data subject, but they also identify the deriving responsibilities of actors in data processing in order to safeguard the rights. However, regarding the demonstration of accountability of controllers and processors, their responsibilities should include the obligation to secure integrity and confidentiality of personal data as well as implementation of the other principles.

### ***2.3.2.1 Lawfulness, fairness, and transparency***

It is worth mentioning here that the principle of 'lawfulness, fairness and transparency' is additionally guaranteed within GDPR by Article 6 - Lawfulness of processing.

### ***2.3.2.2. Purpose limitation and storage limitation***

The principles of 'Purpose limitation' and 'Storage limitation' are addressed in GDPR Article 5 [5](1) (b) and (e). They make clear that data can be collected for specified, explicit and legitimate purposes and when the data that it is no longer used for the scope of work of the data controller/data processor, it should ensure that it is removed from the system, unless the data is processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In GDPR, exceptions regarding public interest are further detailed and they should be conducted on the basis of Union or Member State law. In the Netherlands case, the Act does not contain any provisions or exemptions in relation to retention and deletion of personal data [3], whereas in Portugal, this retention period shall correspond to the period fixed by law or regulation necessary for the purpose of processing [4].

### ***2.3.2.3 Data minimization***

Data minimisation implies that the controller/processor must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. First of all, GDPR affirms the requirement to ensure 'data minimisation': is the personal data processing to achieve purposes in the public interest, scientific or historical research or statistical purposes that should be subject to appropriate safeguards for the rights and freedoms of the data subject. Those safeguards should ensure that technical and organisational measures are in place to ensure this principle.

In the Netherlands, the principles of data protection law are set out in the GDPR, which implies that personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which data are processed [3]. In the Portuguese case, data minimisation is established as part of the Data Protection Law that establishes that the processing of personal data for scientific or historical research purposes respects the principle of data minimisation and that it shall include the anonymisation or pseudonymisation of the personal data wherever possible [6].

### ***2.3.2.4 Personal data used for research or statistical purposes***

GDPR does not substantially concern with the processing of anonymous information, including data stored for statistical or research purposes. The act of providing those appropriate measures, such as pseudonymisation, are taken to preserve the rights of data subjects. The reason is that, often, it is not possible to fully identify the purpose of personal data processing for scientific or historical research or statistical purposes at the time of data collection. Therefore, data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose. In the Netherlands case, the processing necessary for scientific,

historical research or statistical purposes is in accordance with Article 89 of the GDPR, provided that the conditions set out in Article 24(b) (c) and (d) of the Act are met [6]. Regarding the Portuguese case, the National implementation of Article 89 of the GDPR covers the processing of personal data for scientific or historical research purposes, which establishes the relevant consent that could cover several areas of research or be given only to certain areas of projects of scientific research [4].

### **2.3.2.5. Accuracy**

Accuracy ensures that the data processed by the controller/processor is updated with the information. To ensure accuracy, every reasonable step should be taken to ensure that personal data which are inaccurate can be rectified or deleted. According to GDPR's Chapter III - Rights of the data subject, Section 3 – Rectification and erasure provides information regarding the application of this principle [5]. It is obvious that the 'accuracy' principle must be applied by controller/processor in order to guarantee the citizen rights [5]. In the Netherlands [3], the principles of data protection law are set out in the GDPR. This means that personal data must be accurate and kept up to date (accuracy). In regard to the Portuguese case [6], the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data.

### **2.3.2.6. Confidentiality and Integrity**

The responsibilities of data controller or data processor along with authorized data recipient to ensure confidentiality and privacy of data during its usage in their scope of work are precisely stipulated in GDPR [5]. In this context, Article 28 - Processor (3) b), Article 32 - Security of processing, Article 38 (5) - Position of the DPO and Article 72 – Confidentiality specifically addresses the obligation of different actors and institutions to preserve integrity and confidentiality of data. In the Dutch case [3], the principles of data protection law are fully set out in the GDPR. So that, personal data processed in a manner that security and protection against unauthorised or unlawful processing and against accidental loss, destruction or damage are considered. The same considerations are applied to Portugal [6].

## **2.4 Obligations for companies**

The EC has issued a useful leaflet [7] to help companies prepare for implementation of GDPR. Based on this material, we try to elaborate some additional points to the previous Chapter 2.3, which are considered relevant for the further analyses and the aim of this Report. This document [7] states that the aim to help those companies that do not handle personal data as a core business activity, such as Small- and Medium-sized Enterprises (SMEs). They normally deal with personal data of their employees or have lists of clients and customers. We find that the aim of the booklet [7] applies to the IANOS end-users and the cases which are analysed in this task of the project. Namely, even though the project partners involved in demonstration of products through UCs cannot in any case be considered as SMEs, they still do not handle personal data as a core business activity and mainly deal with personal data of their employees as well as of eventual contractors, landowners (related to the land acquisition procedures for construction of new investments), job applicants and visitors on sites. The following seven steps are recommended for companies to get ready for GDPR [7]:

1. Check the personal data to be processed, the purpose of collection, and on which legal bases the data are established;
2. Inform customers, employees and other individuals when personal data collection takes place;
3. Keep personal data no longer than it is necessary;
4. Secure the personal data throughout the process;

5. Keep documentation on all data processing activities;
6. Ensure that any sub-contractor(s) adhere to the same rules;
7. Check whether the provisions on Data Protection Officer (DPO) designation and DPIA apply to the company.

### **2.4.1 Documentation on data processing activities**

GDPR introduces obligations for companies to keep records of their processing activities. Companies are advised to prepare a short document explaining what personal data they hold and the reasons behind this, since they might be required to make the documentation available to the national DPA if requested [7]. The provisions of GDPR aim to achieve a record of processing activities under its responsibility. To achieve that purpose, each controller and processor should be obliged to cooperate with the supervisory authority and make those records available. That record shall contain all the following information:

- the name and contact details of the controller.
- where applicable, the joint controller, the controller's representative and the data protection officer (DPO).
- the purposes of the processing.
- a description of the categories of data subjects and of the categories of personal data.
- the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations.
- where possible, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49 [5], the documentation of suitable safeguards.
- if possible, the envisaged time limits for erasure of the different categories of data.
- if possible, a general description of the technical and organisational security measures referred to in Article 32 [5].

To take account of the specific circumstances of micro-, small- and medium-sized enterprises, this Regulation prevents organisations with fewer than 250 employees regarding record-keeping. Additionally, the Union institutions and bodies, MSs and their supervisory authorities are encouraged to take account of the specific needs of micro-, small- and medium-sized enterprises in the application of this Regulation.

### **2.4.2 Data Protection Officer**

GDPR introduces obligations for companies to appoint a Data Protection Officer (DPO), except for SMEs with fewer than 250 employees that do not handle personal data as a core business activity. This figure, whether they are an employee of the controller, should be able to perform their duties and tasks independently. GDPR prescribes the issues of designation of the DPO, his/her position and tasks, within Chapter IV, Section 4, Articles 37 – 39 [5]. The AP (Dutch case) has issued general guidance on DPOs, based on the Guidelines on Data Protection Officers as issued by the EDBP [8]. On behalf the Portuguese case, there are conflicting options of the Portuguese Bar Association, on the conflict of interest arising from the exercise of the DPO's function by lawyers [6]. The GDPR aims to remove any administrative requirements that could be too oppressive for smaller companies. Similarly, many SMEs benefit from the fact that companies are not required to appoint a DPO, unless their business are activities that present specific data protection risks, such as handling sensitive data on a large scale. Nevertheless, even those who are required to appoint a DPO do not have to hire a full-time employee. Instead, they can save money by appointing an ad-hoc qualified consultant as their DPO.

## 2.5 International transfer of personal data

Cross-border processing means running personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State. From the definition, it is obvious that EU understands a regulated and safe transfer only within the borders of EU MSs. In the provisions of GDPR, the international transfer of personal data is often referred to as 'transfer to a third country', while using the common EU-vocabulary for non-EU countries, which have not ratified legally binding agreements with EU on the subject matter.

### 2.5.1 Adequacy of data protection in third countries

Transfers on the basis of an adequacy decision of GDPR [5] specifies that a transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation ensures an adequate level of protection. This type of transfer shall not require any specific authorisation if the previous condition is fulfilled. Furthermore, to assure protection adequacy of data transferred in third countries, GDPR prescribes mechanisms to determine whether a third country offers adequate level of protection [5].

### 2.5.2 Harmonization of data protection rules

One of the main goals of GDPR is to harmonize data protection rules for all companies processing personal data of individuals based in the EU, removing the costly administrative burdens for companies looking to access new markets within the EU regulatory space fragmented with 28 different data protection laws [9]. The primary goals of GDPR were achieved with the Regulation entering into force in May 2018, the considerations should now be focused on how to extend the benefits of GDPR outside the EU.

## 2.6 Data Protection Impact Assessment

### 2.6.1 Legislative requirements

GDPR [5] introduces Data Protection Impact Assessment (DPIA) as a procedure that investigates and discovers types of data processing operations, which are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context, and purposes. Its aim is to evaluate the origin, nature, and severity of that risk. DPIA is able to determine if outcomes of data processing are conflicting with the GDPR legislation. The DPIA replaces the general obligation to notify the processing of personal data to the supervisory authorities from directive 95/46/EC that did not contribute to improving the protection of personal data. The DPIA should be performed in cases of processing operations that involve use of new technologies or are of a new kind and where no DPIA has been carried out before, or where it has turned a necessary condition. In such cases, DPIA is performed prior to the processing and its outcomes are used to take measures for mitigating the risks ensuring compliance with GDPR.

One of the activities that should be discovered and addressed by DPIA is the so-called profiling where personal data are processed for taking decisions regarding specific natural persons following any systematic and extensive evaluation of personal aspects. Also, DPIA is required for systems for monitoring publicly accessible areas on a large scale as defined in Article 35 (3) (c) from GDPR. This legislation provides only a general framework of the cases when conducting DPIA is required. In order to cover more specific cases, the DPAs of MSs should establish a list of types of processing operations for which

DPIA is required. In addition, the DPAs can establish another list of types of processing operations for which DPIA is not required. The EDPB should apply a consistency mechanism in which such lists involve processing activities that are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States or may substantially affect the free movement of personal data within the Union. GDPR also provides a general framework of the contents of the DPIA [5] (Article 35 (7)). Systematic description of the envisaged processing operations and the purposes of the processing are shown. The DPIA should also cover an assessment of the risks to the rights and freedoms of data subjects referred in the description of the processing information and should set security measures and mechanisms to ensure that the protection of personal data accomplishes compliance with security measures, mechanisms taking into account the rights and legitimate interests of data subjects and other persons concerned.

The data controller shall have the responsibility for carrying out a DPIA, while the data processor should assist if requested. This assessment should be used to determine appropriate measures to demonstrate that the processed data complies with Regulation [5]. If a high risk is detected, which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing. DPIA also allows controllers/processors to voluntarily assess the data processing procedure and outcome and individually correct potential conflicts.

As defined in GDPR [5], DPIA indicates that the processing would result in a potential high risk in the absence of measures taken by the controller to mitigate that risk: It would result in a high risk to the rights and freedoms of natural persons and the controller if the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation. If that is the case, the supervisory authority should be consulted prior to the start of processing activities. Whether the supervisory authority concludes that there is an infringement of GDPR by the data, the controller should be provided within a defined period.

## ***2.6.2 Guidelines and implementation***

DPIA is one of the main tools that enables efficient enforcement of the rules prescribed by GDPR [5]. Therefore, its fast, efficient, and proper implementation is of great significance. The most important aspects are where, when and how DPIA should be conducted, how the results of DPIA will be interpreted, and which actions a DPIA will imply. A list of types of processing operations that are subject to the requirement for DPIA in each MSs facilitates the process of determining the need to conduct DPIA. Also, another list of processing operation for which DPIA is not required can be established. The creation of these lists is task for the DPAs. The creation of these lists for data processing in wide area of different purposes will significantly facilitate the performing of DPIA and the enforcement of GDPR, as a central goal. The EDPB should apply consistency mechanism to these lists for the processing operations that are related to more than one MS. In parallel to the creation of the above-mentioned lists, other actions for creation of guidelines, as defined in GDPR, are performed. One of the main aims of these guidelines is to help data controllers to identify where the performing of DPIA is required. In that light, Guidelines on Data Protection Impact Assessment (GDPIA) and determining whether processing is high risk for the purposes of Regulation 2016/679 (GDPIA) [10]. The GDPIA illustrates the basic principles related to DPIA in the GDPR, as shown on Figure 1 [10]:

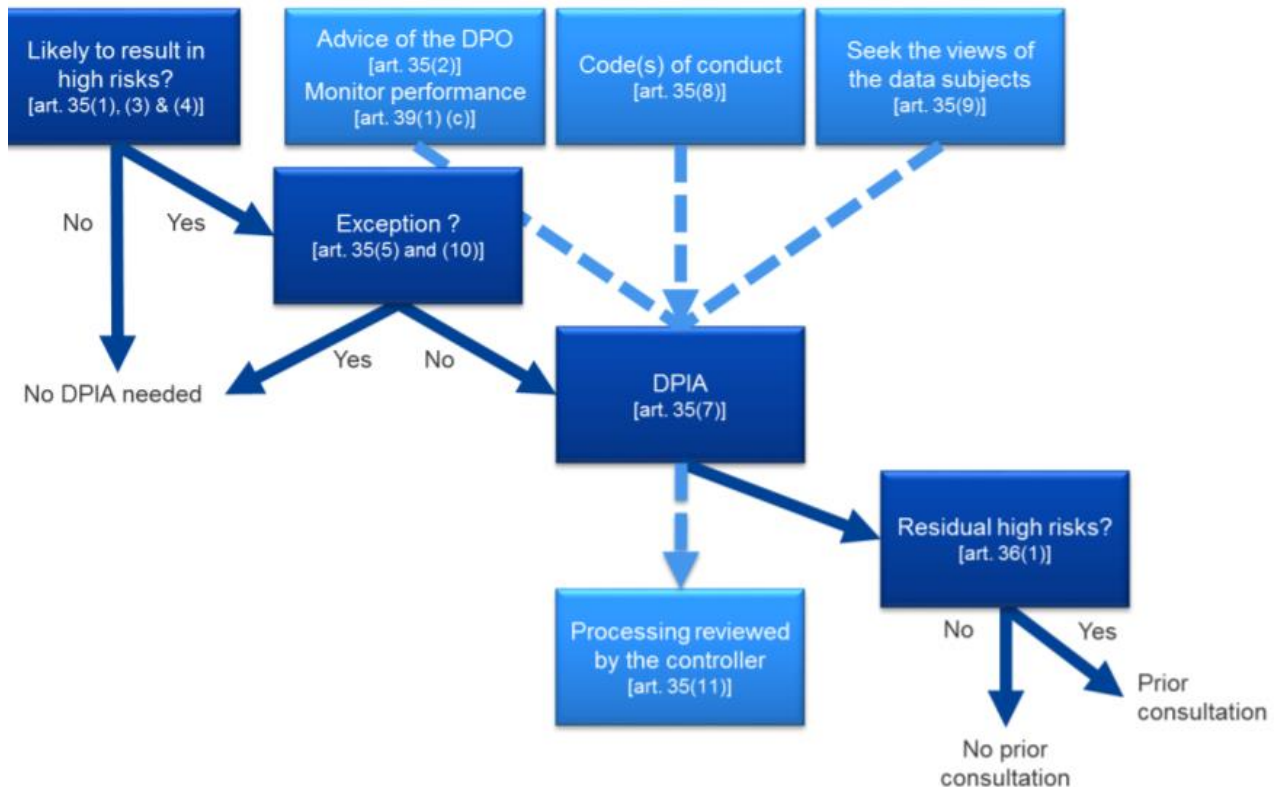


Figure 1: Basic principles related to DPIA in the GDPR [10]

In GDPIA, there is a clarification whether DPIA addresses a single data processing operation or a set of similar processing operations, which could be done for economical and organisational reasons.

Article 35 of GDPR [5] states that single assessment may address a set of similar processing operations that present similar high risks could require a single DPIA to assess multiple processing operations that are similar in terms of the risks presented. Adequate consideration should be given to the specific nature, scope, context and purposes of the data processing. In addition, DPIA should be performed on a certain product by the manufacturer. In case the product is used in the context as defined, no additional DPIA is needed where similar technology is used to collect the same sort of data for the same goals. DPIA can also be useful for assessing the data protection impact of a technology product. Of course, the data controller deploying the product is obliged to perform its own DPIA about the implementation. GDPIA defines the criteria for determining the set of processing operations that require a DPIA due to their inherent high risk, taking into account the particular elements of Articles 35 (1) and 35 (3) (a) to (c), the list to be adopted at the national level under Article 35 (4), recitals (71), (75) and (91) [5]. In that context, the following criteria should be considered [10]:

- Evaluation or scoring, including profiling and predicting;
- Automated decision-making with legal or similar significant effect: processing that aims at taking decisions on data subjects producing legal effects concerning the natural person or which similarly significantly affects the natural person.
- Systematic monitoring: processing used to observe, monitor or control data subjects, including data collected through a systematic monitoring of a publicly accessible area.
- Sensitive data: this includes special categories of data as defined in Article 9 (for example information about individuals' political opinions), as well as personal data relating to criminal convictions or offences.

- Data processed on a large scale.
- Datasets that have been matched or combined.
- Data concerning vulnerable data subjects.
- Innovative use or applying technological or organisational solutions.
- Data transfer across borders outside the European Union.
- When the processing in itself “prevents data subjects from exercising a right or using a service or a contract” (Article 22 and Recital (91)).

GDPIA also provides criteria for determining data processing operations that do not require DPIA [10]:

- Cases where the processing is not likely to result in a high risk to the rights and freedoms of natural persons.
- Cases where the nature, scope, context and purposes of the processing are very similar to the processing for which DPIA have been carried out.
- When the processing operations have been checked by a supervisory authority before May 2018 in specific conditions that have not changed.
- Where a processing operation, pursuant to point (c) or (e) of article 6 (1), has a legal basis in EU or MS law, where the law regulates the specific processing operation and where a DPIA has already been carried out as part of the establishment of that legal basis (Article 35 (10)), except if a MS has stated it to be necessary to carry out a DPIA prior processing activities.

GDPIA provides answer to the question whether the performing of DPIA is needed for existing processing operations: “The requirement to carry out a DPIA applies to existing processing operations likely to result in a high risk to the rights and freedoms of natural persons and for which there has been a change of the risks, taking into account the nature, scope, context and purposes of the processing”. GDPIA provides a path for DPIA to be performed. Additionally, it highlights the need for treating DPIA as an ongoing continuous process especially when the processing information is dynamic and subject to change. It also provides more detailed information on who is obliged to carry out the DPIA. The responsibility of performing DPIA is given to the data controller, and it ought to be supported by the DPO and data processor. GDPIA provides a generic process for carrying out a DPIA [10]. As it is shown on Figure 2, the process of carrying out DPIA. This process starts when the envisaged processing is systematically described. Consequently, it continues with assessment of the necessity and proportionality of the envisaged processing and the identification of the measures that are already taken for ensuring protection of personal data and compliance with GDPR. Then, the assessment of risks for the rights and freedoms of data subjects and envisaging measures is performed. The process is characterized to be iterative, and it shall be documented, monitored, and reviewed.



*Figure 2: Generic iterative process for carrying out DPIA [10]*

Considering the area of Smart Grids (SGs), the Smart Grid Task Force, Expert Group 2 (Regulatory Recommendations for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment) has provided Template for SG and SMS [11]. The first Template for SGs and Smart Metering Systems (SMSs) was submitted to Article 29 Working Party in January 2013. Article 29 Working Party issued its opinions on several occasions and new versions of the Template were prepared. The current version of the Template from September 2018 has been extensively updated due to the adoption of GDPR [5].

The template is destined for Data Controllers that are SG operators that manage or initiate SGs or SMSs, as well as those that introduce changes to existing SG architecture platforms. Since the collection and usage of Personal Data (e.g., household consumption, usage data) is one of the key business enablers for SG operators, the potential risks to the rights and freedoms of natural persons will be properly assessed and mitigated. The rules for collecting Personal Data should be established, in particular with regard to proportionality of collection to the purpose of processing and legal basis [11]. Additionally, it provides detailed systematic procedure for conducting DPIA. For each step, its connection to GDPR and GDPIA and the justification is described. In addition, detailed explanation and supporting tables is provided in Figure 3 [11].

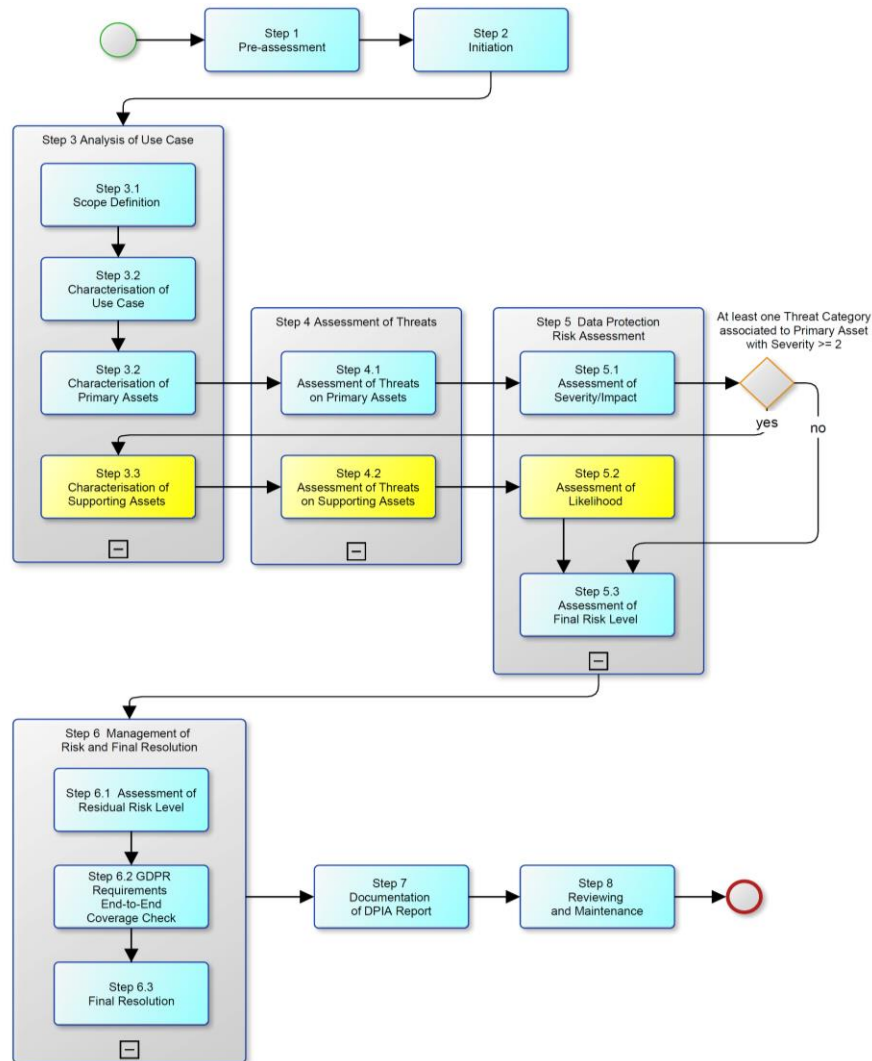


Figure 3: End-to-end view of DPIA workflow [11]

The diagram provides an overview of the complete DPIA workflow. Tasks in yellow are optional. A Primary Asset is a set of one or more pieces of personal data allocated to a specific Actor that shall be properly protected. It should be underlined that the same set of personal data may have different characteristics. An Actor is an entity that communicates and interacts, and it can include people, software systems and field devices. To the DPIA, Actors are logical components of the SG/SMS under assessment on which personal data can reside. Actors rely on various physical components referred to as Supporting Assets. The process starts with **pre-assessment** (which will be conducted for the IANOS products in Section 4. Data privacy and security in IANOS products). Its objective is to determine whether DPIA should be conducted for the observed set of data processing operations. The Template for SGs and SMSs [11] provides a set of questions to facilitate the SG operator to verify whether the criteria for carrying out a DPIA are fulfilled. These questions are based on the following five criteria:

- Cases foreseen by the GDPR, DPAs or EDPB;
- Relevant occurrence;
- Personal data involved and DPIA – related data processing activities;
- Status of data controller or a data processor; and
- New technologies and other criteria.

If the answers to the questions from the pre-assessment provide clear indication that the observed set of data processing operations are not subject to DPIA, then the process does not longer continue.

**Initiation** includes preparatory and organisational activities for conducting DPIA. A creation of a team to conduct DPIA and the identification of the sources are performed. In this step, it is essential to include the DPO and data processor(s) in the team that conducts DPIA.

The third step, **analysis of use cases**, provides a thorough representation of the processes and assets under analysis. This is done through analysis of Use Cases defined. The main aim is to define the scope and boundaries of the DPIA and to provide a comprehensive description of the Primary Assets in scope of the DPIA. Also, where needed the Supporting Assets are also identified in this step.

The fourth step, **assessment of threats**, aims to identify threats on the Primary and Secondary Assets. The threats are defined as risks to the rights and freedoms of individuals.

The fifth step includes **Risk Valuation**, the severity of impact that the threat category would have on the rights and freedoms of individuals, and likelihood of associated threats, are accounted.

In the sixth step, **Assessment of Residual Risk** Level is done by identification and assessment of implemented or planned controls in order to reduce the risk. In addition, in order to ensure that the Threat and Risk analysis has been done properly, a final check is done for verifying that for each Primary Asset, all applicable GDPR requirements are satisfied. The final management decision is taken whether to consider the solution resulting from DPIA to be acceptable or not.

The final two steps include documentation of the DPIA report and review and maintenance of the whole process. The need to review the DPIA, periodically or when new initiatives arise, potentially involving personal data, is also assessed.

### 3. Security of network and infrastructure

The modern society becomes strongly dependent on new information, communication technologies and critical infrastructures. Traditional technologies are becoming more connected to the digital technologies and networks. The increase of digitalization requires a transformation of the energy system into a smarter one so that it can allow consumers to benefit from innovative solutions. Nevertheless, digitalisation is a source of risk due to the increased exposure to cyberattacks and incidents that could potentially have an effect on the security of energy supply and the privacy of consumer data. The EU Security Union Strategy [12] highlights the importance of assuring the European security both physically and digitally in all parts of the society. Applied to the energy sector where IANOS stands, the strategy is to make critical energy infrastructure more resilient against physical, cyber and hybrid threats.

#### 3.1 Directives

The issue of security of networks and infrastructure is included in several European strategic documents, legislation and programmes that aim to create inter-sectoral approaches into ensuring security of infrastructure, assets, and services essential for economy and society:

- [2015 Digital Single Market Strategy](#)

An European Based strategy that is built on three pillars: 1) better access for consumers and business to digital goods and services; 2) creating an environment to guarantee conditions for digital networks and innovative services to flourish 3) maximize the growth potential of the digital economy [13].

- [The EU 2013 Cyber Security Strategy](#)

This strategy sets out the EU's approach on best preventing and responding to cyber disruptions and attacks. A series of actions are detailed to enhance the cyber resilience of IT-systems so that cybercrime is reduced, and the international cybersecurity policies are strengthened [14].

- [NIS directive](#)

The NIS (Network and Information System) Directive [15] aims to increase the overall level of security of networks across the EU. The directive assures that network and information systems (primarily the internet) play an essential role in facilitating the cross-border movement of goods, services and people. The security of network and information systems is therefore essential for the smooth functioning of the internal market. Hence, the transposition of the NIS Directive has the objective to increase the capability of MSs, and therefore of the EU, to build a systematic approach in counteracting the possible threats to networks and information systems. The NIS Directive [15] lays down the basic principles for increasing the cyber security capabilities on national level as well as the principles for organized EU level approach in achieving high level of security of networks and infrastructure.

- [Critical Infrastructure Directive](#)

The Critical Infrastructure Directive [16] was adopted with the objective to establish a framework for identification and designation of European Critical Infrastructures (ECIs) as well as to establish the basis for their protection. The Critical Infrastructure Directive fosters conducting of regular threat assessments and reporting on risks and vulnerabilities to the EC. The approaches of implementation of the Critical Infrastructure Directive vary across EU [17] and the need to a more practical approach in the designation of ECIs has initiated revision of the Directive and the European Programme for Critical Infrastructure Protection [18]. On one hand, the objective is to identify interdependencies

and cross-sectoral relations between ECIs, industry and state actors. On the other hand, the aim is to assess the cross-border interdependencies within a same sector, which is the case for the European transmission system. The research in [19] shows that the electricity and telecommunication sectors are the main cascading initiating sectors. They can cause outages in other sectors, but other critical infrastructure sectors generally do not initiate outages in these sectors. These interdependencies are reflected in Figure 4.

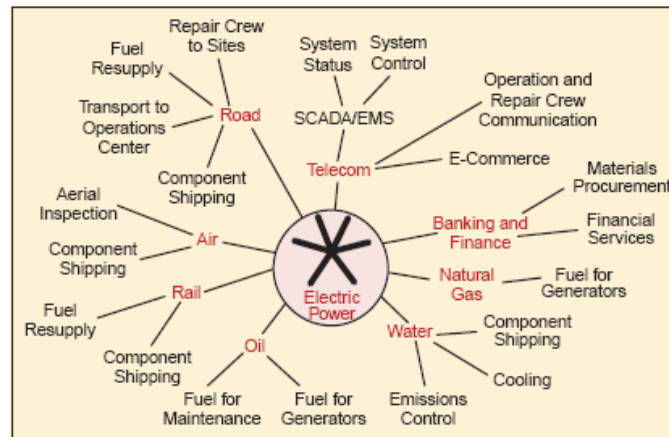


Figure 4: Electricity sector interdependencies

Nevertheless, the energy sector introduces certain particularities that need to be addressed carefully [12]:

- Real-time requirements: Energy systems need to react quickly to standards security measures such as authentication of command, verification of digital signature.
- Cascading effects: the energy infrastructure is strongly interconnected across Europe and beyond EU. The malfunctioning of one country might trigger blackouts or shortages of supply in other areas.
- Combined legacy systems with new technologies: Some of the elements in the energy system were designed and built before cybersecurity considerations were contemplated. Nowadays, there is a need to connect this infrastructure with the most recent state-of-the-art equipment (e.g, smart meters, connected appliances, devices of the Internet of Things (IoT) considering that these assets cannot be exposed to cyber-threats.

### 3.2 Utility cybersecurity risks

The operation of electricity utilities depends on legacy systems and new technologies. The existing electrical infrastructure is controlled with sophisticated control systems and other intelligent components that must be combined with bi-directional communication systems, this information and communication systems represent an overlay to the conventional electricity systems and allow a real-time control operation of both the generation, transmission, and distribution of the electricity in the grids.

In electricity systems, the attacks that the system could suffer could potentially endanger the electricity supply chain and additionally affect other essential services whose systems cannot be disconnected as other Information Technology systems. Furthermore, there is a strong interdependency among sectors and other systems that could enable some threats to become a cross-border issue not only in the EU, but across other neighboring countries [20]. According to those references, the general challenges of energy sector with regards to cybersecurity are listed as follows:

- Grid stability in a cross-border interconnected energy network.

- Protection concepts reflecting current threats and risks.
- Handling of cyber-attacks within the EU.
- Effects by cyber-attacks not fully considered in the design rules of an existing power grid or nuclear facility.
- Introduction of new highly interconnected technologies and services.
- Outsourcing of infrastructures and services.
- Integrity of components used in energy systems.
- Increased interdependency among market players.
- Availability of human resources and their competences.
- Constraints imposed by cyber security measures in contrast to real-time/availability requirements.

Regarding the assets, since they process data, they are exposed to cyber threats as well. The risk is inherited since assets are exposed to threats and have to be considered when developing cyber securities measures. According to [21], these assets that can be somehow related to information systems include:

- Physical infrastructure:(cables, relays, transformers, switches, automation, sensors, FACTS devices, etc.).
- Operational information about electrical assets (status indicators, alerts, events, disturbance information).
- Information system configuration (communication network topology, IP addresses, MAC addresses, user credentials & permissions, configuration files, location data).
- Historical information (data that is stored for further use/or as legislation requirement).
- Trending information (all information related to commercial issues).
- SCADA components operation is based on information and communication technologies. The software includes applications, data bases and web servers as well as operating systems, firmware and device drivers. Services usually consist of user, network and cloud services. Apart from SCADA components (RTUs, IEDs, PLCs), servers, clients, communication network.

As regarding the potential threats [21], critical information systems include several threats coming from intrusions during data transfer among assets, but additionally other software malfunctions and bugs, user errors, field assets (equipment) malfunctioning are part of the problem. Communication equipment malfunctioning, physical attacks and system intrusion abusing data are also considered as potential threats that endanger the integrity of the systems. The list provided by [21] is quite comprehensive and cover a wide range of potential threats.

## 4. Data privacy and security in IANOS products

The main goal of the IANOS project is to demonstrate and replicate the operation of diverse energy streams in EU islands, unlocking their potential to act as Lighthouses (Ameland and Terceira) in decarbonization processes. Large-scale deployment of local renewable energy sources and storage systems will contribute to decarbonising the energy system of the islands as well as reducing greenhouses gas emissions and improving air quality. Towards this objective, the project will develop a set of technological solutions packaged within different products, each one of them providing different functionalities to different actors. The products developed in IANOS encompass innovative approaches of RES generation, usage of novel storage technologies and operation of wholesale and balancing markets. According to the GDPR regulation, the products that are developed by the IANOS project could be subject to DPIA to demonstrate their compliance with GDPR. In this chapter, alongside chapter 8. Annex, an investigation of the of the IANOS products defining the criteria to conduct a DPIA is presented.

### 4.1 DPIA – Pre-assessment questionnaire for IANOS products

The investigation conducted is going to be performed by a DPIA-PA Questionnaire. The objective is to determine if the product/application that is being developed, tested, and demonstrated in the Project requires collection, processing and archiving personal data in a manner that could result in high risk to the rights and freedoms of natural persons. The questionnaire performed for the IANOS project has been based on the questions for the pre-assessment and criteria determining the need to conduct a DPIA from the document “Data Protection Impact Assessment Template for Smart Grid and Smart Metering system” [22]. The DPIA Questionnaire is organised in five different subsections:

- Cases foreseen by the GDPR, DPAs or European Data Protection Board
- Relevant occurrence.
- Personal data involved and DPIA-related Data Processing activities.
- Status of a data controller or a data processor; and
- New technologies and other criteria.

#### 4.1.1 Cases foreseen by the GDPR, DPAs or EDPB

This subsection will describe the first part of the DPIA-PA Questionnaire proposed, in which the cases where the execution of the DPIA is needed, foreseen by GDPR, DPAs and EDPB are investigated. The questions for this part are show in Table 2. The GDPR (Article 35 (3)) lists three particular cases where DPIA is required [5]:

- A systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions that produce legal effects concerning the natural person or similarly significantly affect the natural person are based;
- Processing on a large scale of special categories of data referred to in Article 9 (1) of GDPR, or of personal data relating to criminal convictions and offences referred to in Article 10 of GDPR;
- A systematic monitoring of a publicly accessible area on a large scale.

1	Profiling: Consumers	a	Are you designing a Smart Grid application or system that allows for consumer profiling or another similar activity?
		b	Is your application using data (names, addresses, contact and other descriptor/identifier) for individual consumers that are natural persons?

		c	Do you collect data for energy consumption (demand information and time stamps) for households? Is the data for consumption in some way related to consumers' name, address or other identifiers?
		d	In the application, do you create profiles of types of consumers (natural persons)?
		e	In the application, do you collect any data for time of use/hours of operation for particular equipment in households or comfort indicators in households (temperature/humidity/lighting)? Is the data in some way related to owners' name, address or other identifiers?
2	Profiling: Generation and Storage	a	Do you collect data (names and addresses) from data subjects (natural persons) that are owners of generation/storage facilities?
		b	In the application, do you collect data for power and energy production/demand from data subjects (natural persons) that are owners of generation/storage facilities? Is the data in some way related to owners' name, address or other identifiers?
		c	In the application, do you create profiles of types of generators/storage owned by natural persons?
		d	In the application, do you collect any data for time of use/hours of operation for particular generation/storage facility owned by a natural person? Do you collect data on available storage capacity of a storage facility owned by natural person? Is the data in some way related to owners' name, address or other identifiers?
3	Profiling: data from natural persons	a	If you collect any data from natural persons in the application, what is the frequency of measurement and transmission of data? Please provide response for all types of data collected.
		b	In the application, do you perform remote readings for billing purposes or network planning from natural persons?
		c	In the application, do you collect/send any billing data and information on consumers' payment method from/to natural persons?
		d	Is your application providing online information to consumers/owners of generation or storage facilities that are natural persons? Please describe.
4	Large Scale Data Personal processing	a	Is your application processing <b>personal data</b> [5] on a large scale? (large-scale processing operations which aim to process a considerable amount of <b>personal data</b> at regional, national or supranational level and which could affect a large number of data subjects)
5	International transfer of personal data	a	In case of international transfer of personal data to a third country, what mechanisms are in place to ensure adequacy of data protection?
		b	For your application, do you envisage any contracts with clauses for data transfer from data controllers in EU to data controllers in third countries?
6	Smart Grid operations that prevent users from using a service	a	Will the outcome of use of the Smart Grid application lead to preventing consumers from using a service (e.g. disconnection)?
		b	In the application, do you perform remote switching of equipment/facilities owned by natural persons? Please explain the purpose of the remote switching.
		c	If the use of the Smart Grid application leads to preventing consumers from using a service, do you make a contract with the consumer? Please describe what the contract includes.
7	Processing of special categories of personal data	a	In the application, are you processing special categories of data defined in Art. 9 or Art. 10 of the GDPR [5]?
8	Applications for which the need to conduct DPIA is determined by authorities	a	Is the Smart Grid application or system under design listed by the national Data Protection Authority in your country or by the European Data Protection guidelines as one that requires DPIA?
		b	Is the Smart Grid application or system under design listed by the national Data Protection Authority in your country or by the European Data Protection guidelines as one that does not require DPIA?

Table 2: Questions of Subsection I of the DPIA-PA Questionnaire for products

The first case is mostly concerned for Smart Grid application. Consequently, the first three questions of the questionnaire are related to the profiling of: consumption and

generation of natural persons. Additionally, information related to the frequency of data collection and association with personal data is also inquired. The fourth question is dedicated to figure out if processing data on a large-scale mode is going to be done. If the answer is positive, a DPIA should be carried out for the examined product before it conducts a data processing process. Moreover, question five is related to the international transferring of personal data in order to guarantee the protection of personal data. Question six examines the possibility that some operations could influence exercising natural person's rights. Question number seven and eight examine the requirement from GDPR Article 35 to establish the kind of processing operations requiring a DPIA assessment to establish list of the kind of processing operations for which DPIA is not required. If the processing operations performed by the product are listed on one of these lists, it would indicate that a DPIA should be performed.

### 4.1.2 Relevant occurrence

The second subsection of the DPIA-PA questionnaire is related to the principle of relevant occurrence of the DPIA procedure. When a new system is developed, in order to apply the compliance principle of data protection by design, a DPIA should be executed from the start through the design and its implementation. The products analysed in the document are in their initial design phase. In such case, the DPIA serves as a tool to discover the use of personal data and to indicate if there is a need to perform the beforementioned analysis. Moreover, the procedure is intended to allow product developers to uncover potential risk and implement personal data protection measures if there is a need. The same procedure is applied for existing products. DPIA is performed for already developed products if a significant unexpected breach of personal data or other needs to review the DPIA process has occurred. Consequently, this second subsection is intended to address the introduction of new processes and new types of information that could require performing a DPIA.

1	Introducing a new business process (If an existing product is revised or upgraded for the purposes of the project)	a	Are you designing a new business process within the Smart Grid situation or are you making significant changes to an existing Smart Grid situation?
		b	Are there new types of information introduced and processed in the new business process?
		c	Is the new business process connected to collection and processing of personal data? Description

Table 3: Questions on Section 2 of the DPIA-PA Questionnaire for products

### 4.1.3 Personal data involved and DPIA-related processing activities

Additional explanation for personal data is provided in GDPIA [10] and for the scope of Smart Grids in [11]. Principally, processing of personal data should be performed only when it is necessary for operational purposes. This third subsection is intended to collect and process personal data by the product. These questions will analyse whether personal data is processed and if there is potential risk to impact the rights and freedoms of natural persons. A positive answer to these questions would imply performing a DPIA and implementing adequate "by design" PDP measures for the product.

1	a	Does the design/change require your application to collect and process any personal data? Explain if it is affirmative.
	b	Is the purpose or scope of the process/application capable to have an impact on the rights and freedoms of natural persons? Explain if it is affirmative.

Table 4: Questions of Subsection 3 of the DPIA-PA Questionnaire for products

#### 4.1.4 Status of a data controller or a data processor

In the process of DPIA-PA, it is important to determine who will be data controller and data processor for the examined application (Table 5). It is important to highlight that these roles exist only when personal data is processed. In fact, the data controller determines the purposes, conditions, and means of operating Smart Grid applications or systems which have impact on personal data, according to the GDPR. In addition, if there are other entities that act as data processors, they have to be determined in a precise manner.

1		a	Who will have the role of Data Controller and Data Processor [5] for your product/application during the development and testing/implementation of the product within the project? (it may be too early to have an explicit answer to this question, but you may have an idea of the possible roles in future)
		b	Do you plan to define Data Protection (contractual) requirements between you as developer and the possible future Processor/Controller?

Table 5: Questions on Section 4 of the DPIA-PA Questionnaire for products

#### 4.1.5 New technologies and other criteria

This section of the DPIA-PA Questionnaire will introduce new technologies, especially the technologies identified in [11] (smart metering environment, cloud processing and internet of things) is investigated. The introduction of novel technologies is expected for the IANOS products, but that does not necessarily imply performing of DPIA. Adding new technologies to developing products may also require conducting of DPIA.

1		a	In your application, do you plan to implement new technologies (smart meter environment, cloud processing, Internet of things)?
		b	Does the design/change of the product/application contain any other criterion that may affect rights and freedoms of natural persons?

Table 6: Questions on section 5 of the DPIA-PA Questionnaire for products

## 4.2 Questionnaire results – DPIA Pre-assessment

The DPIA-PA Questionnaire described in the previous section has been applied to the different IANOS products. The responses to each one of these questionnaires were provided by the IANOS product leaders, which are presented in 8. Annex8. Annex. This section summarises the responses to the DPIA-PA Questionnaire and presents the findings from the DPIA-PA procedure. The aim is to identify if there are products which DPIA should be performed. These questionnaires are the responses given for each of the technology responsible. It is worth mentioning that this section is still open to some of the IANOS products that could be add some additional information in these questionnaires. This will be further completed at the second version of the deliverable D4.2 "IVPP secure data monitoring and governance" that is planned to be submitted in month 32.

#### 4.2.1 Grid Oriented Optimizer

The Grid-oriented Optimizer component belongs to the Island Energy Planning and Transition Suite (IEPT) of IANOS. This tool is a grid modelling and simulation tool, able to support long-term planning, while evaluating several energy management and operational strategies. The tool is able to account for multiple RES and storage integration scenarios as well as fostering decarbonization of current energy mixture. It also can promote energy networks synergetic operation.

The responses to the DPIA-PA Questionnaire for the Grid-Oriented Optimizer product provided by CERTH is presented in 8.1 Grid Oriented Optimizer. From the aspect of the cases foreseen by GDPR, DPAs or EDPB (Topic I), Grid Oriented Optimizer does not allow for consumer profiling for both generation and consumption, which was confirmed by the responses in 8.1 Grid Oriented Optimizer. The product allows consumer profiling, estimating on design specification for related energy systems. It is envisaged that the Grid Oriented Optimizer shall create prosumers and major production profiles, based on design data conducting simulations and not based on actual data compilation. The relevance of the eight questions from Topic I should be discussed considering the following: 1) types of processing operations for which DPIA assessment is required, 2) the list of operations for which DPIA is not required which is not mandatory. These lists have practical significance only in the cases when personal data is processed. Additionally, 8.1 Grid Oriented Optimizer it also shows the answers related to the second topic. As the product is in the design phase, it represents a novel solution. Therefore, it introduces new business processes and new types of information. Consequently, the response of the Grid Oriented Optimizer, the existence of these lists is not entirely relevant as the whole product does not envisage processing of personal data. The product conducts simulations to carry out its purposes. As it can be observed from the responses in 8.1 Grid Oriented Optimizer, the Grid Oriented Optimizer tool, does not incorporate personal data processing. Regarding Topic III, it directly addresses processing of personal data, the impact it might have on rights and freedoms of natural persons. Although the conclusion that the use of personal data is not considered for this product, it is already derived from previous topics. As far as Topic IV of DPIA-PA is regarded, it is intended to determine who will play the role of data controller and data processor for the product. It is essential to note that these roles exist only when personal data is processed. For the scope of the product, there is no entity that should take the role of data controller in this product. However, the answer presented in Topic V, it should not be considered under a future scenario, upon possible commercialization of the Grid Oriented Optimizer, and introduction of new functionalities that would process personal data.

As a consequence of the answers to the questions on the previous Topics, it is shown that there is no need to develop procedures for detection of personal data breach because the product does not process personal data. The overall analyses of the responses to the DPIA-PA Questionnaire prove that conducting a DPIA is not necessary, considering the design features of the Grid Oriented Optimizer, and its usage in the scope of the IANOS project. The rationale behind this conclusion is primarily since the functionalities of the product, no personal data is envisaged to be collected and processed at any stage of product demonstration and application.

#### **4.2.2 LCA/LCC Toolkit**

The LCA/LCC Toolkit component belongs to the Island Energy Planning and Transition Suite (IEPT) of IANOS. This tool will perform environmental and cost assessment of the proposed implemented RE technologies in the islands as well as of the storage devices. The Lifecycle Assessment (LCA) evaluates parameters such as: Energy savings due to the implementation of the IANOS interventions; Reduced fossil fuel consumption; Reduced Greenhouse Gas Emissions; Primary Energy Demand and Consumption. On the other hand, the Lifecycle Cost (LCC) assessment evaluates the direct, indirect, internal, and external costs of the implemented technologies at all stages during a project's lifetime (capital, operation and maintenance and end-of-life costs).

The responses to the DPIA-PA Questionnaire for the LCA/LCC Toolkit product provided by CERTH is presented in Annex 8.2 LCA/LCC Toolkit.

From the aspect of the cases foreseen by GDPR, DPAs or EDPB (Topic I), LCA/LCC Toolkit does not allow for consumer profiling, but they could be created for both generation and storage, which was confirmed by the responses in 8.2 LCA/LCC Toolkit. The product collects information monitored on asset basis (e.g., building, power plant, transformers) which is not related to any owners personal data. It is envisaged that the LCA/LCC Toolkit shall provide information not related to any consumer's personal data and identity. The relevance of the eight questions from Topic I should be discussed considering the following: 1) types of processing operations for which DPIA assessment is required, 2) the list of operations for which DPIA is not required which is not mandatory. These lists have practical significance only in the cases when personal data is processed. Additionally, Annex 8.2 LCA/LCC Toolkit it also shows the answers related to the second topic. As the product is in the design phase, it represents a novel solution therefore introduces new business processes and new types of information. Consequently, the response of the LCA/LCC Toolkit the existence of these lists is not entirely relevant as the whole product does not envisage processing of personal data. As it can be observed from the responses in Annex 8.2 LCA/LCC Toolkit, LCA/LCC Toolkit does not incorporate personal data processing. Regarding Topic III, it directly addresses processing of personal data, the impact it might have on rights and freedoms of natural persons. Although the conclusion that the use of personal data is not considered for this product is already derived from previous topics.

As far as Topic IV of DPIA-PA is regarded, it is intended to determine who will play the role of data controller and data processor for the product. It is essential to note that these roles exist only when personal data is processed. For the scope of the product, there is no entity that should take the role of data controller in this product. However, the answer presented in Topic V should be considered under a future scenario, upon possible commercialization of the LCA/LCC Toolkit and introduction of new functionalities that would process personal data. Because of the answers to the questions on the previous Topics, it is shown that there is no need to develop procedures for detection of personal data breach because the product does not process personal data.

The overall analyses of the responses to the DPIA-PA Questionnaire prove that conducting a DPIA is not necessary, considering the design features of the LCA/LCC Toolkit and its usage in the scope of the IANOS project. The rationale behind this conclusion is primarily based on the fact that due to the functionalities of the product, no personal data is envisaged to be collected and processed at any stage of product demonstration and application.

### **4.2.3 Crowdequity Platform**

The Crowdequity Platform will provide all the stakeholders, such as project investors and islanders, the opportunity to fund future projects in exchange for shares to the project or register their future projects to receive funding. The component will make the members of the community shareholders of the renewable energy assets, aligning with the community and Islander-centric approach that IANOS adopts.

The responses to the DPIA-PA Questionnaire for the Crowdequity Platform product provided by CERTH is presented in Annex 8.3 Crowdequity Platform.

From the aspect of the cases foreseen by GDPR, DPAs or EDPB (Topic I), Crowdequity Platform does not allow for consumer profiling for both generation and consumption, which was confirmed by the responses in Annex 8.3 Crowdequity Platform. Nevertheless, the product is planned to collect and use data for individual consumers that are natural persons. It is envisaged that the Crowdequity Platform shall provide fundraising

campaigns for future renewable energy installations. For that purpose, the application would process personal data on a large scale. The relevance of the eight questions from Topic I should be discussed considering the following: 1) types of processing operations for which DPIA assessment is required, 2) the list of operations for which DPIA is not required which is not mandatory. These lists have practical significance only in the cases when personal data is processed. Additionally, Annex 8.3 Crowdequity Platform it also shows the answers related to the second topic. As the product is in the design phase, it represents a novel solution therefore introduces new business processes and new types of information. Consequently, the response of the Crowdequity Platform, the existence of these lists is entirely relevant. Nevertheless, it is not explicitly listed. As it can be observed from the responses in Annex 8.3 Crowdequity Platform, Crowdequity Platform is planned to incorporate personal data processing. Regarding Topic III, it directly addresses processing of personal data, the impact it might have on rights and freedoms of natural persons. The users of the platform will be able to create user profiles that contain personal information. As far as Topic IV of DPIA-PA is regarded, it is intended to determine who will play the role of data controller and data processor for the product. It is essential to note that these roles exist only when personal data is processed. For the scope of the product, there is not yet an entity that should take the role of data controller in this product, since the project is at an early stage to define this role. However, the answer presented in Topic V should be considered under a future scenario upon possible commercialization of the Crowdequity Platform and introduction of new functionalities that would process personal data. As a consequence of the answers to the questions on the previous Topics, it is shown that there is need to develop procedures for detection of personal data breach because the product processes personal data.

The overall analyses of the responses to the DPIA-PA Questionnaire prove that conducting a DPIA would be necessary, considering the design features of the Crowdequity Platform and its usage in the scope out of the IANOS UC.

#### **4.2.4 TNO Reflex**

Reflex is a software solution that empowers aggregators to create a powerful Virtual Power Plant (VPP). This tool can use the flexibility of large quantities of small devices effectively for multiple purposes. The overall purpose is to enable the flexibility of DER assets to be used in energy markets and ancillary services markets. Consequently, the value of flexibility can be stacked and the profits of using the flexibility are increased. This tool calculates the flexibility of an specific cluster, planning the energy production and consumption for every device for the coming 48 hours with a precision of 15-minutes intervals. The responses to the DPIA-PA Questionnaire for the TNO Reflex product provided by TNO is presented in Annex 8.4 Reflex TNO

From the aspect of the cases foreseen by GDPR, DPAs or EDPB (Topic I), TNO Reflex does not allow for consumer profiling for both generation and consumption, which was confirmed by the responses in Annex 8.4 . The product collects information collected is yet unclear and subject to research in the IANOS project. It is envisaged that the TNO Reflex shall provide energy measurements in which they are registered under a unique ID that from perspective is not related to the owner, household or natural person processed in the application. The relevance of the eight questions from Topic I should be discussed considering the following: 1) types of processing operations for which DPIA assessment is required, 2) the list of operations for which DPIA is not required which is not mandatory. These lists have practical significance only in the cases when personal data is processed. Additionally, Annex 8.4 Reflex TNO8.4 it also shows the answers related to the second topic. As the product is in the design phase, it represents a novel solution therefore introduces new business processes and new types of information.

Consequently, the response of the TNO Reflex, the existence of these lists is not entirely relevant as the whole product does not envisage processing of personal data. As it can be observed from the responses in 8.4 Reflex TNO, TNO Reflex does not incorporate personal data processing. Regarding Topic III, it directly addresses processing of personal data, the impact it might have on rights and freedoms of natural persons. Although the conclusion that the use of personal data is not envisaged for this product is already derived from previous topics.

As far as Topic IV of DPIA-PA is regarded, it is intended to determine who will play the role of data controller and data processor for the product. It is essential to note that these roles exist only when personal data is processed. For the scope of the product, there is no entity that should take the role of data controller in this product at this stage. Reflex will have both roles. However, the answer presented in Topic V should be considered [under a future scenario], upon possible commercialization of the TNO Reflex and introduction of new functionalities that would process personal data.

As a consequence of the answers to the questions on the previous Topics, it is shown that there is no need to develop procedures for detection of personal data breach because the product does not process personal data. The overall analyses of the responses to the DPIA-PA Questionnaire prove that conducting a DPIA is not necessary, considering the design features of the TNO Reflex and its usage in the scope of the IANOS project. The rationale behind this conclusion is primarily based on the fact that due to the functionalities of the product, no personal data is considered to be collected and processed at any stage of product demonstration and application.

#### **4.2.5. System Modeler**

The Energy System Simulator (ESSIM) is a discrete time simulation tool and collection of models that calculates energy flows in assets and the effects thereof, in an interconnected hybrid energy system over a period of time. With the help of the energy flows ESSIM calculates, one can get insights into how well the assets in a network are dimensioned, if there is overloading in any given transport asset (like pipe, cables, etc.) and what the effect of storage is in any part of the network.

From the aspect of the cases foreseen by GDPR, DPAs or EDPB (Topic I), the System Modeler does not allow for consumer profiling for both generation and consumption, which was confirmed by the responses in Annex 8.5 System Modeler. The product collects information from publicly available sources or general specification. Moreover, identifiers are used for the households which information is extracted from. Energy demand profiles are generic based on standards for the entire Netherlands Pilot Site. It is envisaged that the System Modeler shall provide information based on aggregate data which is based on standards profiles from technical specifications and weather forecasts. The relevance of the eight question from Topic I should be discussed considering the following: 1) types of processing operations for which DPIA assessment is required, 2) the list of operations for which DPIA is not required which is not mandatory. These lists have practical significance only in the cases when personal data is processed. Additionally, Annex 8.5 System Modeler it also shows the answers related to the second topic. As the product is in the design phase, it represents a novel solution therefore introduces new business processes and new types of information. Consequently, the response of the System Modeler, the existence of these lists is not entirely relevant as the whole product does not envisage processing of personal data. As it can be observed from the responses in Annex 8.5 System Modeler, System Modeler does not incorporate personal data processing. As long as Topic III is regarded, it directly addresses processing of personal data, the impact

it might have on rights and freedoms of natural persons. Although the conclusion that the use of personal data is not envisaged for this product is already derived from previous topics.

As far as Topic IV of DPIA-PA is regarded, it is intended to determine who will play the role of data controller and data processor for the product. It is essential to note that these roles exist only when personal data is processed. For the scope of the product, there is no entity that should take the role of data controller in this product for the life of the project. However, the answer presented in Topic V should be considered (under a future scenario), upon possible commercialization of the System Modeler and introduction of new functionalities that would not need to process personal data.

As a consequence of the answers to the questions on the previous Topics, it is shown that there is no need to develop procedures for detection of personal data breach because the product does not process personal data. The overall analyses of the responses to the DPIA-PA Questionnaire prove that conducting a DPIA is not necessary, considering the design features of the System Modeler and its usage in the scope of the IANOS project. The rationale behind this conclusion is primarily based on the fact that due to the functionalities of the product, no personal data is envisaged to be collected and processed at any stage of product demonstration and application.

#### 4.2.6 OptiMEMS

OptiMEMS is a tool used to monitor multi-source networks energy systems, where advanced energy management strategies are deployed. Except from the optimal scheduling of the small- and large-scale assets of the grid, the decision tool is responsible for the maintenance of the power balance within the grid, the self-consumption and grid services provision in emergency cases. The main objective of the tool is the minimization of the overall daily cost by optimizing the flexibility of the energy portfolio and extracting the optimal set points regarding the supply/demand/storage.

The responses to the DPIA-PA Questionnaire for the OptiMEMS product provided by CERTH is presented in Annex 8.6 OptiMEMS. From the aspect of the cases foreseen by GDPR, DPAs or EDPB (Topic I), OptiMEMS does not allow for consumer profiling for both generation and consumption, which was confirmed by the responses in Annex 8.6 OptiMEMS. The product collects information regarding the energy consumption, the user preferences and energy generation and storage data related to each infrastructure and asset individually. It is envisaged that the OptiMEMS shall provide online information related to the infrastructure ID. This data is encrypted, and only authorized users are capable of accessing the actual information. The relevance of the eight questions from Topic I should be discussed considering the following: 1) types of processing operations for which DPIA assessment is required, 2) the list of operations for which DPIA is not required which is not mandatory. These lists have practical significance only in the cases when personal data is processed. Additionally, Annex 8.6 OptiMEMS it also shows the answers related to the second topic. As the product is in the design phase, it represents a novel solution. Therefore, it introduces new business processes and new types of information. Consequently, the response of the OptiMEMS the existence of these lists is relevant as the whole product envisages processing of personal data in an encrypted manner, in which only authorized users are capable of accessing the actual data. Regarding Topic III, it directly addresses processing of personal data, the impact it might have on rights and freedoms of natural persons. As far as Topic IV of DPIA-PA is regarded, it is intended to determine who will play the role of data controller and data processor for the product. It is essential to note that these roles exist only when personal data is processed. For the scope of the product, there is not yet entity defined that should take

the role of data controller in this product. However, the answer presented in Topic V should be considered under a future scenario, upon possible commercialization of the OptiMEMS and introduction of new functionalities that would process personal data.

Because of the answers to the questions on the previous Topics, it is shown that there is need to develop procedures for detection of personal data breach.

The overall analyses of the responses to the DPIA-PA Questionnaire prove that conducting a DPIA would be necessary if the future implementation of the product actually would deal with personal data. It should be highlighted that, at the current status, the data is treated in an encrypted manner. The rationale behind this conclusion is primarily based on the fact that due to the functionalities of the product.

#### **4.2.7 CleanWatts KIPLO**

Kiplo Core Platform purpose is to help utilities, aggregators and users in the management of their energy assets and associated flexibility. By monitoring and managing accurate real-time data from demand and supply side, it allows the optimization of available energy resources using Demand Response activities, flexibility management, connection with upstream markets and the possibility to enable P2P energy markets. Kiplo Core Platform is constantly updating the inputs to dynamically optimise the global operation of the Virtual Power Plant (VPP). Additionally, external advanced services (load and RES forecasting, clustering, and storage optimization) and manage novel types of equipment (e.g. flywheels, hybrid transformer, heat storage) are easily integrable.

The responses to the DPIA-PA Questionnaire for the KIPLO product provided by CleanWatts is presented in Annex 8.7 CleanWatts KIPLO. From the aspect of the cases foreseen by GDPR, DPAs or EDPB (Topic I), KIPLO does not allow for consumer profiling for both generation and consumption, which was confirmed by the responses in Annex 8.7 CleanWatts KIPLO. The product collects information regarding pilot sites ID, not stores personal data. It is envisaged that the KIPLO shall provide remote switching of equipment owned by natural persons, in order to participate on Energy Markets according to each Use Case main objective. The relevance of the eight questions from Topic I should be discussed considering the following: 1) types of processing operations for which DPIA assessment is required, 2) the list of operations for which DPIA is not required which is not mandatory. These lists have practical significance only in the cases when personal data is processed. Additionally, Annex 8.7 CleanWatts KIPLO it also shows the answers related to the second topic. As the product is in the design phase, it represents a novel solution therefore, it introduces new business processes and new types of information. Consequently, the response of the KIPLO to the existence of these lists is not entirely relevant as the whole product does not envisage processing of personal data. As it can be observed from the responses in Annex 8.7 CleanWatts KIPLO, KIPLO incorporates personal data processing under the structure of identifiers. Regarding Topic III, it directly addresses processing of personal data, the impact it might have on rights and freedoms of natural persons. Although the conclusion that the use of personal data is not envisaged for this product is already derived from previous topics. As far as Topic IV of DPIA-PA is regarded, it is intended to determine who will play the role of data controller and data processor for the product. It is essential to note that these roles exist only when personal data is processed. For the scope of the product, there is a plan to define Data Protection and a Data Processor for the application if in the future is considered relevant. However, the answer presented in Topic V should be considered under a future scenario, upon possible commercialization of the KIPLO and introduction of new functionalities that would process personal data. Because of the answers to the questions on the

previous Topics, it is shown that there could be potential development procedures for detection of personal data breach because the product does process personal data. Nevertheless, this is done in the pilot under a pilot-ID. The overall analyses of the responses to the DPIA-PA Questionnaire prove that conducting a DPIA could be necessary, considering the design features of the KIPLO and its usage out of the scope of the IANOS project. The rationale behind this conclusion is primarily since due to the functionalities of the product, no personal data is considered to be collected and processed at any stage of product demonstration and application.

#### ***4.2.8 Aggregation and Classification Intelligence***

The classification is a data mining process, where the most valuable information is extracted. It can be a useful tool to support the operator's portfolio characterization based on the relevant objectives and strategies. In general, the classification will assist and provide support to the operator either for formulating market strategies or for exploiting the results for a demand-side management approach. More specifically, regarding the demand-side management approach, the classification will examine typical consumption patterns and individual profiles of the users included within IANOS to identify the most appropriate set of households for demand response schemes. The cluster analysis will reveal information regarding the patterns of the typical electricity use such as the start of the peak times or peak intensity and will assist to better target the users in reducing the peak-loads and shifting some of the peak time demand to times of lower usage, thereby reducing the need for additional generation and transmission network capacity. Additionally, the classification will contribute to the decision making regarding the energy markets such as the day-ahead and intra-day markets. Finally, the classification process could be an important tool for providing insight information for balancing services provision. In both cases, the aim of the classification is to detect and identify the groups of possible flexibility resources.

The responses to the DPIA-PA Questionnaire for the Aggregation and Classification Intelligence product provided by CERTH is presented in Annex 8.8 Aggregation and Classification Intelligence. From the aspect of the cases foreseen by GDPR, DPAs or EDPB (Topic I), Aggregation and Classification Intelligence does not allow for consumer profiling for both generation and consumption, which was confirmed by the responses in Annex 8.8 Aggregation and Classification Intelligence. The product collects information regarding the energy consumption, the user preferences and energy generation and storage data related to each infrastructure and asset individually. It is envisaged that the Aggregation and Classification Intelligence shall provide online information related to the infrastructure ID. This data is encrypted, and only authorized users are capable of accessing the actual information. The relevance of the eight questions from Topic I should be discussed considering the following: 1) types of processing operations for which DPIA assessment is required, 2) the list of operations for which DPIA is not required which is not mandatory. These lists have practical significance only in the cases when personal data is processed. Additionally, Annex 8.8 Aggregation and Classification Intelligence it also shows the answers related to the second topic. As the product is in the design phase, it represents a novel solution therefore introduces new business processes and new types of information. Consequently, the response of the Aggregation and Classification Intelligence the existence of these lists is relevant as the whole product envisages processing of personal data. As it can be observed from the responses in Annex 8.8 Aggregation and Classification Intelligence, Aggregation and Classification Intelligence incorporates personal data processing encrypted manner, in which only authorized users are capable of accessing actual information. Regarding Topic III, it directly addresses processing of personal data, the impact it might have on rights and freedoms of natural

persons. As far as Topic IV of DPIA-PA is regarded, it is intended to determine who will play the role of data controller and data processor for the product. It is essential to note that these roles exist only when personal data is processed. For the scope of the product, there is not yet entity defined that should take the role of data controller in this product. However, the answer presented in Topic V should be considered under a future scenario, upon possible commercialization of the Aggregation and Classification Intelligence and introduction of new functionalities that would process personal data. Because of the answers to the questions on the previous Topics, it is shown that there is need to develop procedures for detection of personal data breach.

The overall analyses of the responses to the DPIA-PA Questionnaire prove that conducting a DPIA would be necessary if the future implementation of the product would deal with personal data. It should be highlighted that, at the status, the data is treated in an encrypted manner. The rationale behind this conclusion is primarily based on the fact that due to the functionalities of the product.

#### **4.2.9 Forecasting Engine**

This component will provide inputs to the decision support system by developing forecasting mechanisms for both consumption and generation purposes. It will contribute to the optimal scheduling and planning of the grid assets. The forecast horizon will be extended from a short (short-term) to a daily level (day-ahead) utilizing historical consumption/generation data and external information (temperature, humidity, wind speed etc.) as well. Eventually regarding the development and the training of the models, various techniques will be deployed and examined, including statistical and advanced machine learning techniques, such as ensemble methods and deep learning.

The responses to the DPIA-PA Questionnaire for the Forecasting Engine provided by CERTH is presented in Annex 8.9 Forecasting Engine.

From the aspect of the cases foreseen by GDPR, DPAs or EDPB (Topic I), Forecasting Engine does not allow for consumer profiling for both generation and consumption, which was confirmed by the responses in Annex 8.9 Forecasting Engine. The product collects information regarding the energy consumption, the user preferences and energy generation and storage data related to each infrastructure and asset individually. It is envisaged that the Forecasting Engine shall provide online information related to the infrastructure ID. This data is encrypted, and only authorized users are capable of accessing the actual information. The relevance of the eight questions from Topic I should be discussed considering the following: 1) types of processing operations for which DPIA assessment is required, 2) the list of operations for which DPIA is not required which is not mandatory. These lists have practical significance only in the cases when personal data is processed. Additionally, Annex 8.9 Forecasting Engine it also shows the answers related to the second topic. As the product is in the design phase, it represents a novel solution therefore introduces new business processes and new types of information. Consequently, the response of the Forecasting Engine the existence of these lists is relevant as the whole product envisages processing of personal data. As it can be observed from the responses in Annex 8.9 Forecasting Engine, Forecasting Engine incorporates personal data processing encrypted manner, in which only authorized users are capable of accessing actual information. Regarding Topic III, it directly addresses processing of personal data, the impact it might have on rights and freedoms of natural persons. As far as Topic IV of DPIA-PA is regarded, it is intended to determine who will play the role of data controller and data processor for the product. It is essential to note that these roles exist only when personal data is processed. For the scope of the product, there is not yet entity defined that should take the role of data controller in this product. However, the answer presented in Topic V should be considered under a future scenario,

upon possible commercialization of the Forecasting Engine and introduction of new functionalities that would process personal data.

Because of the answers to the questions on the previous Topics, it is shown that there is need to develop procedures for detection of personal data breach. The overall analyses of the responses to the DPIA-PA Questionnaire prove that conducting a DPIA would be necessary if the future implementation of the product actually would deal with personal data. It should be highlighted that, at the current status, the data is treated in an encrypted manner. The rationale behind this conclusion is primarily based on the fact that due to the functionalities of the product.

#### **4.2.10 DLT-based Transactive Platform**

The DLT-based Transactive Platform aims to develop a P2P market so that prosumers in a local network are enabled to directly trade energy with each other, by avoiding RES curtailment and future grid transport costs. This system is based on blockchain technology that guarantees the transparency and security of the transaction, which remains permanently recorded in the platform, allowing all parties to audit the results.

The responses to the DPIA-PA Questionnaire for the DLT-based Transactive Platform provided by ENG is presented in Annex 8.10 DLT-based Transactive Platform.

From the aspect of the cases foreseen by GDPR, DPAs or EDPB (Topic I), DLT-based Transactive Platform does not allow for consumer profiling for both generation and consumption, which was confirmed by the responses in Annex 8.10 DLT-based Transactive Platform. The product collects information aggregated consumption and production data. It is envisaged that the DLT-based Transactive Platform shall provide via dashboard, details on value and energy transactions. The relevance of the eight questions from Topic I should be discussed considering the following: 1) types of processing operations for which DPIA assessment is required, 2) the list of operations for which DPIA is not required which is not mandatory. These lists have practical significance only in the cases when personal data is processed. Additionally, in Annex 8.10 DLT-based Transactive Platform also shows the answers related to the second topic. As the product is in the design phase, it represents a novel solution therefore introduces new business processes and new types of information. Consequently, the response of the DLT-based Transactive Platform, the existence of these lists is not entirely relevant as the whole product does not envisage processing of personal data. As it can be observed from the responses in Annex 8.10 DLT-based Transactive Platform, DLT-based Transactive Platform does not incorporate personal data processing. Regarding Topic III, it directly addresses processing of personal data, the impact it might have on rights and freedoms of natural persons. Although the conclusion that the use of personal data is not envisaged for this product is already derived from previous topics. As far as Topic IV of DPIA-PA is regarded, it is intended to determine who will play the role of data controller and data processor for the product. It is essential to note that these roles exist only when personal data is processed. For the scope of the product, there is no entity that should take the role of data controller in this product at the timebeing of the project, since they will be testing with simulated data.

As a consequence of the answers to the questions on the previous Topics, it is shown that there is no need to develop procedures for detection of personal data breach because the product does not process personal data. The overall analyses of the responses to the DPIA-PA Questionnaire prove that conducting a DPIA is not necessary, considering the design features of the product and its usage in the scope of the IANOS project. The rationale behind this conclusion is primarily based on the fact that due to the

functionalities of the product, no personal data is envisaged to be collected and processed at any stage of product demonstration and application.

#### **4.2.11 Virtual Energy Console**

The Virtual Energy Console is an interoperable user-friendly monitoring console (UI - User Interface) to effectively assess energy flows to properly manage, visualize and dispatch their energy assets. The Virtual Energy Console will be specially designed according to the requirements of IANOS project. The dashboard will allow the VPP operator to easily access different dataset and important information in line with IANOS KPIs such as generation mix of the VPP portfolio, penetration of RES in the system and historical data.

The responses to the DPIA-PA Questionnaire for the Virtual Energy Console provided by CleanWatts is presented in Annex 8.11 Virtual Energy Console. From the aspect of the cases foreseen by GDPR, DPAs or EDPB (Topic I), Virtual Energy Console does not allow for consumer profiling for both generation and consumption, which was confirmed by the responses in Annex 8.11 Virtual Energy Console. It is envisaged that the Virtual Energy Console shall provide an interoperable user-friendly monitoring console to assess energy flows to manage, visualize and dispatch their energy assets. The relevance of the eight questions from Topic I should be discussed considering the following: 1) types of processing operations for which DPIA assessment is required, 2) the list of operations for which DPIA is not required which is not mandatory. These lists have practical significance only in the cases when personal data is processed. Additionally, Annex 8.11 Virtual Energy Console also shows the answers related to the second topic. As the product is in the design phase, it represents a novel solution therefore introduces new business processes and new types of information. Consequently, the response of the Virtual Energy Console, regarding the existence of these lists is not entirely relevant as the whole product does not envisage processing of personal data. As it can be observed from the responses in Annex 8.11 Virtual Energy Console, the Virtual Energy Console does not incorporate personal data processing. Regarding Topic III, it directly addresses processing of personal data, the impact it might have on rights and freedoms of natural persons. Although the conclusion that the use of personal data is not considered for this product is already derived from previous topics. As far as Topic IV of DPIA-PA is regarded, it is intended to determine who will play the role of data controller and data processor for the product. It is essential to note that these roles exist only when personal data is processed. For the scope of the product, there is no entity that should take the role of data controller in this product. However, the answer presented in Topic V should be considered under a future scenario, upon possible commercialization of the Virtual Energy Console and introduction of new functionalities that would process personal data. Because of the answers to the questions on the previous Topics, it is shown that there is no need to develop procedures for detection of personal data breach because the product does not process personal data.

The overall analyses of the responses to the DPIA-PA Questionnaire prove that conducting a DPIA is not necessary, considering the design features of the product and its usage in the scope of the IANOS project. The rationale behind this conclusion is primarily based on the fact that due to the functionalities of the product, no personal data is envisaged to be collected and processed at any stage of product demonstration and application.

#### **4.2.12 Enterprise Service Bus**

The iVPP secured enterprise service bus (ESB) will be the component that will play this data transfer role, with a special focus on cyber-security aspects. Interoperability is seen

as the key enabler of smart grid. A prominent definition describes interoperability as “the ability of two or more devices from the same vendor, or different vendors, to exchange information and use that information for correct cooperation”. In other words, two or more systems (devices or components) are interoperable, if these “two or more” systems are able to perform cooperatively a specific function by using information which is exchanged.

The responses to the DPIA-PA Questionnaire for the Enterprise Service Bus provided by ETRA is presented in Annex 8.12 Enterprise Service Bus. From the aspect of the cases foreseen by GDPR, DPAs or EDPB (Topic I), the ESB does not allow for consumer profiling for both generation and consumption, which was confirmed by the responses in Annex 8.12 Enterprise Service Bus. The product acts as a conductor of the information that needs to flow from one application to another. The relevance of the eight questions from Topic I should be discussed considering the following: 1) types of processing operations for which DPIA assessment is required, 2) the list of operations for which DPIA is not required which is not mandatory. These lists have practical significance only in the cases when personal data is processed. Additionally, Annex 8.12 Enterprise Service Bus, also shows the answers related to the second topic. As the product is in the design phase, it represents a novel solution therefore introduces new business processes and new types of information. Consequently, the response of the ESB regarding the existence of these lists is not entirely relevant as the whole product does not envisage processing of personal data. As it can be observed from the responses in Annex 8.12 Enterprise Service Bus, the ESB does not incorporate personal data processing. Regarding Topic III, it directly addresses processing of personal data, the impact it might have on rights and freedoms of natural persons. Although the conclusion that the use of personal data is not considered for this product is already derived from previous topics. As far as Topic IV of DPIA-PA is regarded, it is intended to determine who will play the role of data controller and data processor for the product. It is essential to note that these roles exist only when personal data is processed. For the scope of the product, there is no entity that should take the role of data controller in this product. However, the answer presented in Topic V should be considered under a future scenario, upon possible commercialization of the product and introduction of new functionalities that would process personal data.

Because of the answers to the questions on the previous Topics, it is shown that there is no need to develop procedures for detection of personal data breach because the product does not process personal data. The overall analyses of the responses to the DPIA-PA Questionnaire prove that conducting a DPIA is not necessary, considering the design features of the product and its usage in the scope of the IANOS project. The rationale behind this conclusion is primarily based on the fact that due to the functionalities of the product, no personal data is considered to be collected and processed at any stage of product demonstration and application.

#### ***4.2.13 Non-intrusive characterization of energy flexibility in water heating systems***

The non-intrusive characterization and use of energy flexibility in water heating systems is made of a set of sensors coupled and installed to a classical water heater with no need to change or modify it. The information from the operation of the water heaters is collected and then passed through a microcontroller. Then it is communicated wirelessly to the servers of UNINOVA and through them to the iVPP. High level instructions will be provided from the iVPP which will be passed to UNINOVA's servers. From there the instructions will be delivered to the individual microcontrollers which will control the water heaters.

The responses to the DPIA-PA Questionnaire for the Non-intrusive characterization of energy flexibility in water heating systems provided by UNINOVA is presented in Annex 8.13 Non-intrusive characterization of energy flexibility in water heating systems

From the aspect of the cases foreseen by GDPR, DPAs or EDPB (Topic I), Non-intrusive characterization of energy flexibility in water heating systems does not allow for consumer profiling for both generation and consumption, which was confirmed by the responses in Annex 8.13 Non-intrusive characterization of energy flexibility in water heating systems. The product collects information regarding hot water consumption profile, which is not related to owner's name, address or other identifiers. It is envisaged that this product does not collect the overall energy consumption, only hot water consumption. The relevance of the eight questions from Topic I should be discussed considering the following: 1) types of processing operations for which DPIA assessment is required, 2) the list of operations for which DPIA is not required which is not mandatory. These lists have practical significance only in the cases when personal data is processed. Additionally, Annex 8.13 Non-intrusive characterization of energy flexibility in water heating systems, also shows the answers related to the second topic. As the product is in the design phase, it represents a novel solution therefore introduces new business processes and new types of information. Consequently, the response of the product, the existence of these lists is not entirely relevant as the whole product does not envisage processing of personal data. As it can be observed from the responses in Annex 8.13 Non-intrusive characterization of energy flexibility in water heating systems, this product does not incorporate personal data processing. Regarding Topic III, it directly addresses processing of personal data, the impact it might have on rights and freedoms of natural persons. Although the conclusion that the use of personal data is not envisaged for this product is already derived from previous topics. As far as Topic IV of DPIA-PA is regarded, it is intended to determine who will play the role of data controller and data processor for the product. It is essential to note that these roles exist only when personal data is processed. For the scope of the product, there is no entity that should take the role of data controller in this product. However, the answer presented in Topic V should be considered under a future scenario, upon possible commercialization of the product and introduction of new functionalities that would process personal data. As a consequence of the answers to the questions on the previous Topics, it is shown that there is no need to develop procedures for detection of personal data breach because the product does not process personal data.

The overall analyses of the responses to the DPIA-PA Questionnaire prove that conducting a DPIA is not necessary, considering the design features of the non-intrusive characterization of energy flexibility in water heating systems and its usage in the scope of the IANOS project. The rationale behind this conclusion is primarily based on the fact that due to the functionalities of the product, no personal data is envisaged to be collected and processed at any stage of product demonstration and application.

#### **4.2.14 FEID-PLUS**

The FEID-Plus is a fog-enabled computing device equipped with special functions to control I/O, phase width modulation and analogic signals. It employs enough processing capacity for applying distributed computing such as information capturing and storing, algorithms execution and control over the installation.

The responses to the DPIA-PA Questionnaire for the FEID-Plus provided by CERTH is presented in Annex 8.14 FEID-PLUS. From the aspect of the cases foreseen by GDPR, DPAs or EDPB (Topic I), FEID-Plus does allow for consumer profiling but not for both

generation and consumption, which was confirmed by the responses in Annex 8.14 FEID-PLUS. The product collects information regarding the energy consumption, the user preferences and energy generation and storage data related to each infrastructure and asset individually. It is envisaged that the FEID-Plus shall provide online information related to the infrastructure ID. This data is encrypted, and only authorized users are capable of accessing the actual information. The relevance of the eight questions from Topic I should be discussed considering the following: 1) types of processing operations for which DPIA assessment is required, 2) the list of operations for which DPIA is not required which is not mandatory. These lists have practical significance only in the cases when personal data is processed. Additionally, in Annex 8.14 FEID-PLUS also shows the answers related to the second topic. As the product is in the design phase, it represents a novel solution therefore introduces new business processes and new types of information. Consequently, the response of the FEID-Plus, the existence of these lists is relevant as the whole product envisages processing of personal data. As it can be observed from the responses in Annex 8.14 FEID-PLUS, FEID-Plus incorporates personal data processing in an encrypted manner, in which only authorized users are capable of accessing actual information. Regarding Topic III, it directly addresses processing of personal data, the impact it might have on rights and freedoms of natural persons. As far as Topic IV of DPIA-PA is regarded, it is intended to determine who will play the role of data controller and data processor for the product. It is essential to note that these roles exist only when personal data is processed. For the scope of the product, there is not yet entity defined that should take the role of data controller in this product. However, the answer presented in Topic V should be considered under a future scenario, upon possible commercialization of the FEID-Plus and introduction of new functionalities that would process personal data such as the communication with smart meters. Because of the answers to the questions on the previous Topics, it is shown that there is need to develop procedures for detection of personal data breach.

The overall analyses of the responses to the DPIA-PA Questionnaire prove that conducting a DPIA would be necessary if the future implementation of the product actually would deal with personal data. It should be highlighted that, at the current status, the data is treated in an encrypted manner. The rationale behind this conclusion is primarily based on the fact that due to the functionalities of the product.

#### **4.2.15 Smart Energy Router**

The Energy Router will be enhanced with flexibility algorithms that will consider flexibility on the user side (either on equipment either on storage capabilities) in order to provide ancillary services to the island grid. These algorithms will be implemented on the energy router controller and will command/control the energy flux to (and from) the grid and to (and from) the storage devices.

The responses to the DPIA-PA Questionnaire for the Smart Energy Router provided by UNINOVA is presented in Annex 8.15 Smart Energy Router. From the aspect of the cases foreseen by GDPR, DPAs or EDPB (Topic I), Smart Energy Router does allow for consumer profiling, but it is not considered for both generation and consumption, which was confirmed by the responses in Annex 8.15 Smart Energy Router. The product collects information regarding the PV panels and batteries. It is envisaged that the Smart Energy Router shall provide information of the PV production and energy storage. The relevance of the eight questions from Topic I should be discussed considering the following: 1) types of processing operations for which DPIA assessment is required, 2) the list of operations for which DPIA is not required which is not mandatory. These lists have practical significance only in the cases when personal data is processed. Additionally, Annex 8.15

Smart Energy Router it also shows the answers related to the second topic. As the product is in the design phase, it represents a novel solution therefore introduces new business processes and new types of information. Consequently, the response of the Smart Energy Router, the existence of these lists is considered as the Smart Energy Router processes information for the generation and storage of personal data. As it can be observed from the responses in Annex 8.15 Smart Energy Router, the Smart Energy Router incorporates personal data processing. Regarding Topic III, it directly addresses processing of personal data, the impact it might have on rights and freedoms of natural persons. Although the conclusion that the use of personal data is considered for this product is already derived from previous topics. As far as Topic IV of DPIA-PA is regarded, it is intended to determine who will play the role of data controller and data processor for the product. It is essential to note that these roles exist only when personal data is processed. For the scope of the product, there is no entity that should take the role of data controller in this product. This role is addressed by the Data Management Structure defined. However, the answer presented in Topic V should be considered under a future scenario, upon possible commercialization of the Smart Energy Router and introduction of new functionalities that would process personal data.

Because of the answers to the questions on the previous Topics, it is shown that there is need to develop procedures for detection of personal data breach. The overall analyses of the responses to the DPIA-PA Questionnaire prove that conducting a DPIA would be necessary out of the IANOS UC context, considering the design features of the Smart Energy Router.

#### **4.2.16 Hybrid Transformer**

A Hybrid Transformer will be developed the power electronic block for voltage regulation. It will introduce new windings to the transformer (and associated magnetic circuit) and the mechanical layout along with prototype laboratory validation and installation in EDA distribution grid (Terceira). The responses to the DPIA-PA Questionnaire for the FEID-Plus provided by EFACEC is presented in Annex 8.16 Hybrid Transformer.

From the aspect of the cases foreseen by GDPR, DPAs or EDPB (Topic I), the Hybrid Transformer does not allow for consumer profiling for both generation and consumption, which was confirmed by the responses in Annex 8.16 Hybrid Transformer. The product does not collect any type of information. It is envisaged that the Hybrid Transformer neither provides but not personal data. The relevance of the eight questions from Topic I should be discussed considering the following: 1) types of processing operations for which DPIA assessment is required, 2) the list of operations for which DPIA is not required which is not mandatory. These lists have practical significance only in the cases when personal data is processed. Additionally, Annex 8.16 Hybrid Transformer it also shows the answers related to the second topic. As the product is in the design phase, it represents a novel solution therefore introduces new business processes and new types of information. Consequently, the response of the Hybrid Transformer regarding the existence of these lists is not entirely relevant as the whole product does not envisage processing of personal data. As it can be observed from the responses in Annex 8.16 Hybrid Transformer, Hybrid Transformer does not incorporate personal data processing. Regarding Topic III, it directly addresses processing of personal data, the impact it might have on rights and freedoms of natural persons. Although the conclusion that the use of personal data is not envisaged for this product is already derived from previous topics.

As far as Topic IV of DPIA-PA is regarded, it is intended to determine who will play the role of data controller and data processor for the product. It is essential to note that these roles exist only when personal data is processed. For the scope of the product, there is no entity that should take the role of data controller in this product. However, the answer

presented in Topic V should be considered under a future scenario, upon possible commercialization of the Hybrid Transformer and introduction of new functionalities that would process personal data. Consequently, the answers to the questions on the previous Topics, it is shown that there is no need to develop procedures for detection of personal data breach because the product does not process personal data.

The overall analyses of the responses to the DPIA-PA Questionnaire prove that conducting a DPIA is not necessary, considering the design features of the product and its usage in the scope of the IANOS project. The rationale behind this conclusion is primarily since due to the functionalities of the product, no personal data is envisaged to be collected and processed at any stage of product demonstration and application.

#### **4.2.17 V2G Charging**

The V2G Charging system will further develop its smart chargers providing control algorithms for ancillary services and grid support (i.e. dynamic charging profile scheduling to avoid grid constraints, voltage support/regulation, grid frequency regulation in coordination with the system's automatic generation control).

The responses to the DPIA-PA Questionnaire for the V2G charger provided by EFAEM is presented in Annex 8.17 V2G Charging. From the aspect of the cases foreseen by GDPR, DPAs or EDPB (Topic I), V2G charger does not allow for consumer profiling for both generation and consumption, which was confirmed by the responses in Annex 8.17 V2G Charging. The product does not directly collect information from users. Since this product developed in IANOS would consist of an algorithm implemented to the EV Chargers to allow scheduling to avoid grid constraints, voltage support/regulation and grid frequency regulation. The relevance of the eight questions from Topic I should be discussed considering the following: 1) types of processing operations for which DPIA assessment is required, 2) the list of operations for which DPIA is not required which is not mandatory. These lists have practical significance only in the cases when personal data is processed. Additionally, Annex 8.17 V2G Charging also shows the answers related to the second topic. As the product is in the design phase, it represents a novel solution therefore introduces new business processes and new types of information. Consequently, the response of the V2G charger the existence of these lists is not entirely relevant as the whole product does not envisage processing of personal data. As it can be observed from the responses in Annex 8.17 V2G Charging, V2G Chargers does not incorporate personal data processing. Regarding Topic III, it directly addresses processing of personal data, the impact it might have on rights and freedoms of natural persons. Although the conclusion that the use of personal data is not considered for this product is already derived from previous topics.

As far as Topic IV of DPIA-PA is regarded, it is intended to determine who will play the role of data controller and data processor for the product. It is essential to note that these roles exist only when personal data is processed. For the scope of the product, there is no entity decided yet that should take the role of data controller in this product. However, the answer presented in Topic V should be considered [under a future scenario], upon possible commercialization of the V2G Charger and introduction of new functionalities that would process personal data. Because of the answers to the questions on the previous Topics, it is shown that there is no need to develop procedures for detection of personal data breach because the product does not process personal data. The overall analyses of the responses to the DPIA-PA Questionnaire prove that conducting a DPIA is not necessary, considering the design features of the product and its usage in the scope of the IANOS project. The rationale behind this conclusion is primarily based on the fact that due to the functionalities of the product, no personal data is considered to be collected and processed at any stage of product demonstration and application.

## 5. IANOS Secured Enterprise Service Bus

### 5.1 General considerations

ivPP ESB will be based on the CITRIC smart city platform that follows the RIVER © architecture created by ETRA. RIVER is a Reactive, Interoperable, Visible, Elastic and Resilient architecture oriented to microservices and events.



Figure 5: RIVER architecture logo

It is an open architecture with capacity to grow its service network, reactive because it is event-driven, interoperable because it is supported by standard protocols and agnostic models of data, visible because it is monitored in its operation, elastic because it can be scaled out and independently in each of its services and resilient because it is orchestrated and monitored to be fault tolerant. CITRIC's microservices distribution fully complies with UNE178104:2017 in its orientation towards functional layer.

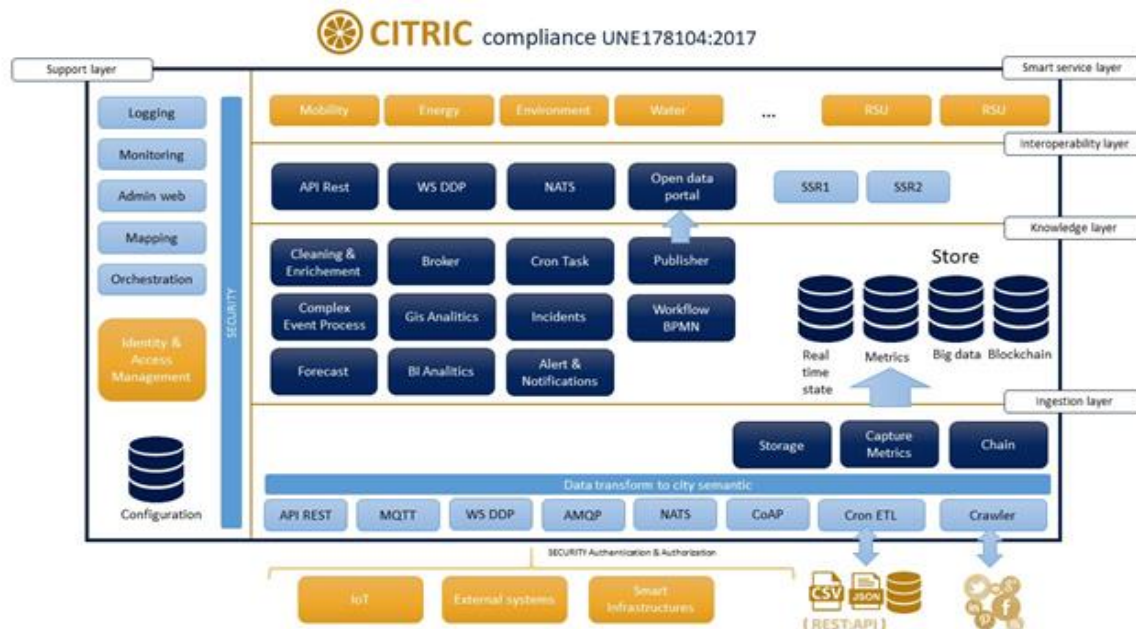


Figure 6: CITRIC architecture

All microservices are scaled out using replicas and load balancers based on the particular needs of each installation. CITRIC can be deployed over Docker Swarm nodes or over Kubernetes cluster based depending on the dimension of the system. Besides the in-premise installation, it can easily be deployed in the Google, AWS, or Azure clouds. CITRIC is composed by a plethora of services and modules that interact among each other and provide services. All of them are containerized, making it possible to deploy and update any architecture component in just a few minutes. The CITRIC platform supports the following technologies for the bulk Data ingestion.

Technology	Description	
<b>API REST</b>	CITRIC has a robust secure and protected HTTPs Rest API with <i>rate limit</i> control to prevent attacks and allows a lot of flexibility for data ingestion through it. Besides authentication, API security allows to <i>authorize</i> only a certain set of data to each authenticated user. The implementation of this API has been done with Express.	Express JS

MQTT	The MQTT protocol is widely used by lightweight devices (IoT) and supported by CITRIC. To do this, CITRIC uses RabbitMQ as the MQTT ingestion service.	
AMQP	It is possible to ingest data directly with AMQP protocol to ingest directly over queues that are consumed by microservices, which transform and store information in the platform storage system.	
WS DDP	It is possible to connect to the platform using websockets (e.g. from web browsers). The protocol over WS implemented is Distributed Data Protocol (DDP). A number of methods are implemented over this protocol that provide a very efficient way to do mass ingestion.	
NATS	NATS is the underlying broker on the platform and is responsible for managing the entire microservices communication network. It acts as an enterprise service bus (ESB); communication through it makes use of topics that are mapped to services. CITRIC offers a set of topics that allow you to interact directly with storage microservices with their corresponding level of security.	
CoAP	CoAP is a lightweight protocol similar to MQTT but communicating over UDP. It is normally used by moving devices that jeopardize the quality of communication. CITRIC offers this ingestion service to integrate data coming from moving vehicles that interact with the platform. This microservice is natively developed by ETRA.	
Cron ETL	This service is responsible for ingesting data offered in external files, databases or web services. The process can be triggered in a time-basis or by modifying or creating new ready-to-load files on the platform. As an ETL tool, CITRIC uses Node-Red, an interactive tool to design workflows to ingest data with possible transformation.	
EFI S2	EFI is developed specifically as a standard for communication methods between smart devices and Demand-Side Management (DSM) solutions. This S2 protocol could be used for the ingestion of data to the ESB	

Table 7: CITRIC platform suggests technologies for bulk data ingestion

Different processes can be applied to the ingested data (this is configurable):

- **Transformation:** Any ingestion process previously goes through a transformation process to normalize the data before entering it into the platform. Transformation schemas are pre-configured for each source in the configuration database and are particular to each platform deployment as they must be tailored to particular data sources and how they are stored in the storage service and then served to the higher layers.
- **Security:** Every ingestion process is authenticated and authorized by a layer of security in each microservice. Each credential per token or user/password has an authorization scheme to access a subset of platform data at three levels of security: read, write, and only public attributes.
- **Storage:** If data persistence is needed, this microservice handles the storage of data when it is injected or modified. It manages the real-time database supported by MongoDB and the big data database, supported in our case by an ElasticSearch cluster.
- **Message brokering:** the information received is routed to pre-configured endpoints, allowing for a scalable architecture

The CITRIC architecture will be adapted and extended to support the functionalities required in IANOS. CITRIC platform plus the required additions will compose the iVPP ESB.

## 5.2 IANOS Common Architecture

Based on the high-level architecture, and the different use cases at the pilots' islands, a proposal of the multiple controllers interfering with each other has been proposed in task 4.4 "Optimized cross-resource VPP coordination for energy service provision". This task presented a generic approach of the different components presented in WP4 "IANOS Multi-Layer VPP Operational Framework". It is worth mentioning that the IANOS Secure Enterprise Service Bus acts as an enabler of the secure data transfer within in-between VPP and the external devices. The ESB reduces the integration effort required due to its properties in different data ingestion. Further details are given in Deliverable 4.7 "The iVPP Centralized Dispatcher". Nevertheless, the figures reflecting the common, and the specified architecture for both Lighthouse Islands are presented below:

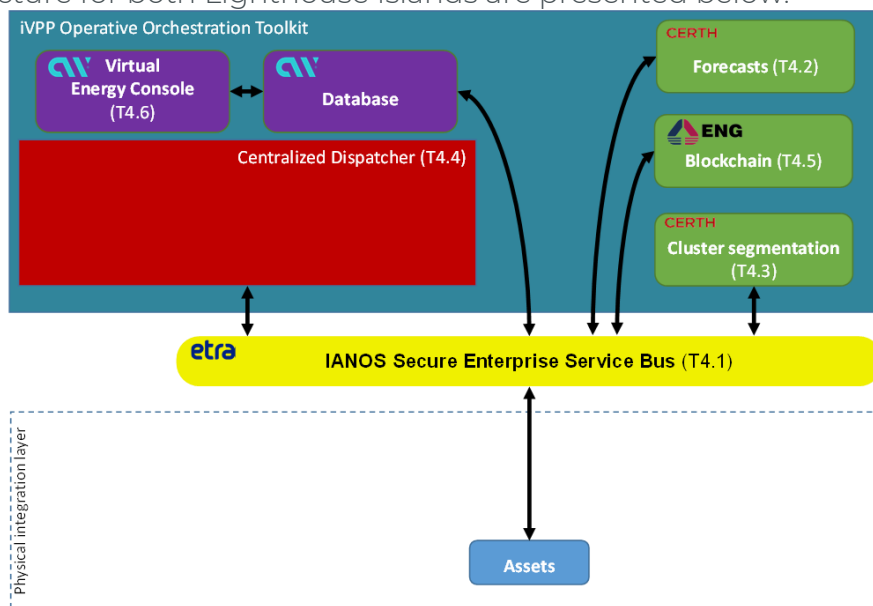


Figure 7: Generic Layout of the IANOS' iVPP modules defined in D4.7 "The iVPP Centralized Dispatcher"

As detailed in deliverable 4.7, based on the Use Cases defined and architecture define, each different lighthouse Island presents a different layout:

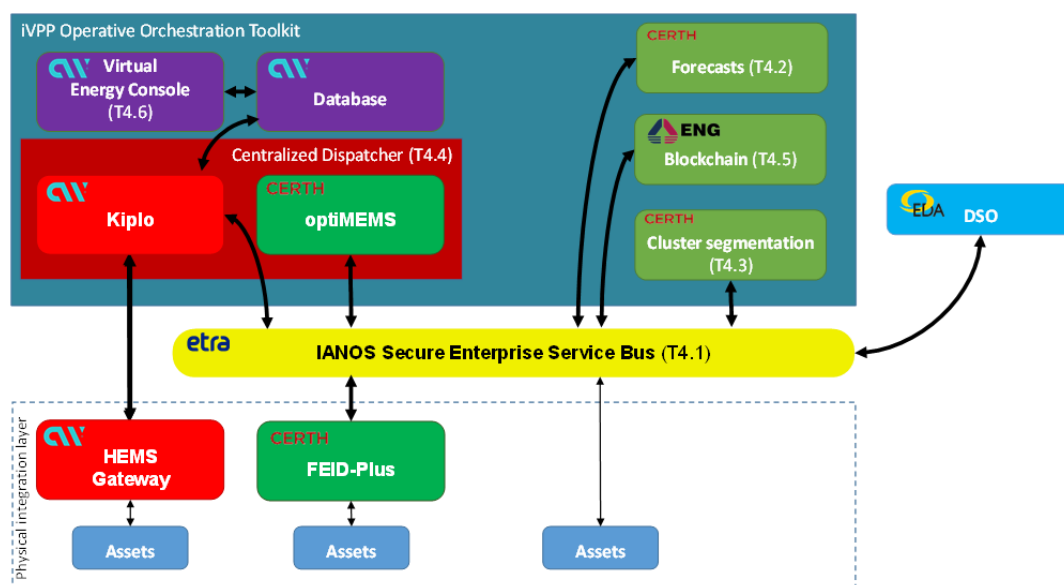


Figure 8: Deployment for Terceira demonstration site. Based on the architecture defined in D4.7 "The iVPP Centralized Dispatcher"

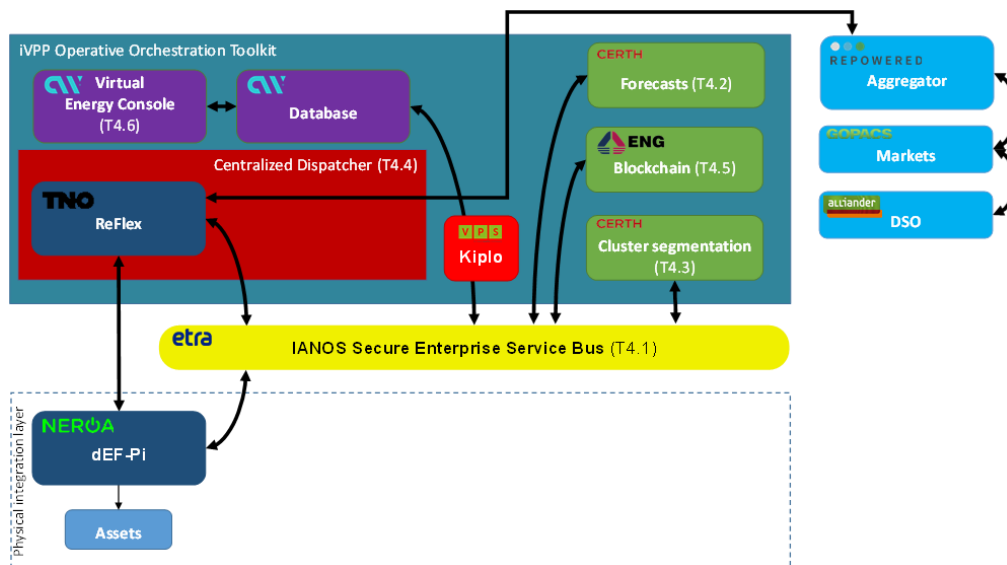


Figure 9: Deployment for Ameland demonstration site. Based on the architecture defined in D4.7 "The iVPP Centralized Dispatcher"

As it can be stated in the figures shown, the role of the ESB in both pilot demonstration sites is slightly different. As it can be seen, in both cases, the ESB acts as the communication pipeline between most of the modules integrated in the demonstration sites. Nevertheless, a difference between both demonstration sites must be stated, since in Ameland (Figure 9), the Assets do not directly communicate with the ESB. The information flows through the Platform dEF-Pi, which is directly connected to both the ESB and the Centralized Dispatcher. In the other case, in Terceira (Figure 8), the ESB acts as the main communication flow between the assets.

## 5.3 Connection guide

This section will be used as an introductory guide to explain the steps to carry out the connection that the different iVPP modules and assets should follow to perform the ESB connection.

### 5.3.1 RabbitMQ connection

With the user and password provided you will be able to publish and subscribe to queues in the virtual-host IANOS using the mqtt protocol. The configuration you must use is the following:

- url: mqtt://etra-id.com
- port: 1884
- virtual-host: ianos
- queue (for the initial tests): messages
- credentials: with the fields 'username' and 'password' as provided
- payload: with the field id and the desired data

### 5.3.2 Example in Python

Here you can see examples for publisher and subscriber using the open-source library paho-mqtt. However, you can publish or subscribe for every message in the topic or just the ones that matches your selection. For example you can publish in ianos/messages/mykey to make sure you only read the messages published there by subscribing to this same messages.

Publish:



```
1 import paho.mqtt.publish as publish
2 import string
3 import random
4
5 #Example of a autogenerated ID
6 def generate_random_ID(length):
7     return ''.join(random.choice(string.ascii_letters +
8                             string.digits) for _ in range(length))
9
10 def publisher(auth, data):
11     publish.single("ianos/messages/1", json.dumps(data),
12                   hostname="mqtt://etra-id.com", port=1884, auth=auth)
13
14 if __name__ == "__main__":
15     auth = {
16         "username": "ianos:username",
17         "password": "yourPassword"
18     }
19     data = {
20         "_id": generate_random_ID(17),
21         "data": "test",
22         "more_data": "more_test"
23     }
24     publisher(auth, data)
```

Subscribe:

```
1 import paho.mqtt.subscribe as subscribe
2
3 def on_message_print(client, userdata, message):
4     print("%s %s" % (message.topic, message.payload))
5
6 def subscriber(auth):
7     subscribe.callback(on_message_print, "ianos/messages/#",
8                       hostname="mqtt://etra-id.com",
9                       port=1884, client_id="PythonJJ", auth=auth)
10
11 if __name__ == "__main__":
12     auth = {
13         "username": "ianos:username",
14         "password": "yourPassword"
15     }
16     subscriber(auth);
```

### 5.3.3 Encrypted MQTT connection

If you want to use the encrypted communication to the same mqtt service, you can use the implemented tls protocol by utilizing the port 8883 and adding the Certificate Authority certificate that should have been provided with the credentials. This way, both examples above should look like the next example.

```

1 publish.single("ianos/messages/xxxx",
2               json.dumps(data),
3               hostname=server, port=8883,
4               auth=auth,
5               tls={"ca_certs": "ca_certificate.pem"})
6
7 subscribe.callback(on_message_print,
8                   "ianos/messages/xxxx",
9                   hostname=server,
10                  port=8883,
11                  client_id="PythonJJ45",
12                  auth=auth,
13                  tls={"ca_certs": "ca_certificate.pem"})

```

### 5.3.4. Connect to the proposed list of topics

As a first approach, we suggested a list of topics to publish and subscribe to. Being the following:

Topic	Definition
<b>ianos/ameland/asset/+:</b>	used by field assets to inform about their current measurements. Normally control processes subscribe to these topics.
<b>ianos/ameland/command/+</b>	used by control processes to send control commands to assets in the field. Normally field devices subscribe to the corresponding topic.
<b>ianos/ameland/message/+</b>	used by services to listen for specific messages that may come from other service (inter-process communication).
<b>ianos/ameland/currentWeather/+</b>	used to periodically broadcast current weather of defined locations in the island.
<b>ianos/terceira/asset/+</b>	used by field assets to inform about their current measurements. Normally control processes subscribe to these topics.
<b>ianos/terceira/command/+</b>	used by control processes to send control commands to assets in the field. Normally field devices subscribe to the corresponding topic.
<b>ianos/terceira/message/+:</b>	used by services to listen for specific messages that may come from other service (inter-process communication).
<b>ianos/terceira/currentWeather/+</b>	used to periodically broadcast current weather of defined locations in the island.

Table 8: List of connection to the proposed list of topics

This '+' represents one level on the sub-tree. For example, if you subscribe via mqtt to 'ianos/ameland/asset/+', you will receive all the messages sent to 'ianos/ameland/asset/anything', being anything any string without the '/'. Also, you can subscribe to 'ianos/ameland/#' so you will receive any message under this route, or in

other words, all the topics that start with this route. One consideration, you could publish messages to anything under the IANOS virtual host, but only these queues are binded and stored to the database, so take care with the routes used in the mqtt protocol. Also, the string written in the position of the + in the routes above, will be used as the id in the database, so if you want to update the sensor, you will only have to send the updated measures to this sensor, and any non-included parameter will be considered as non-changed. Last thing, we are currently working on including a schema validation process for the messages, so those which don't follow the correct schema won't be written in the database that is accessed through the API explained later, but there is no way to check JSON schemes in the own mqtt process. Will be up to the client implementation to validate messages received through mqtt subscriptions.

### 5.3.4 API usage

The base route for accessing the database is: <https://citric-api.tec.etra-id.com/api/v2>

**Important:** Use JSON format for the communications with the API, otherwise there could be unexpected issues. Every message published in `ianos/messages` will also be consumed by a service and written in a database so they can be accessed at any time. For using it, you will have to first login, here is an example of how it works in the Figure 10. Keep in mind that the body params must be 'user' and 'password', any others will be responded with fail status.

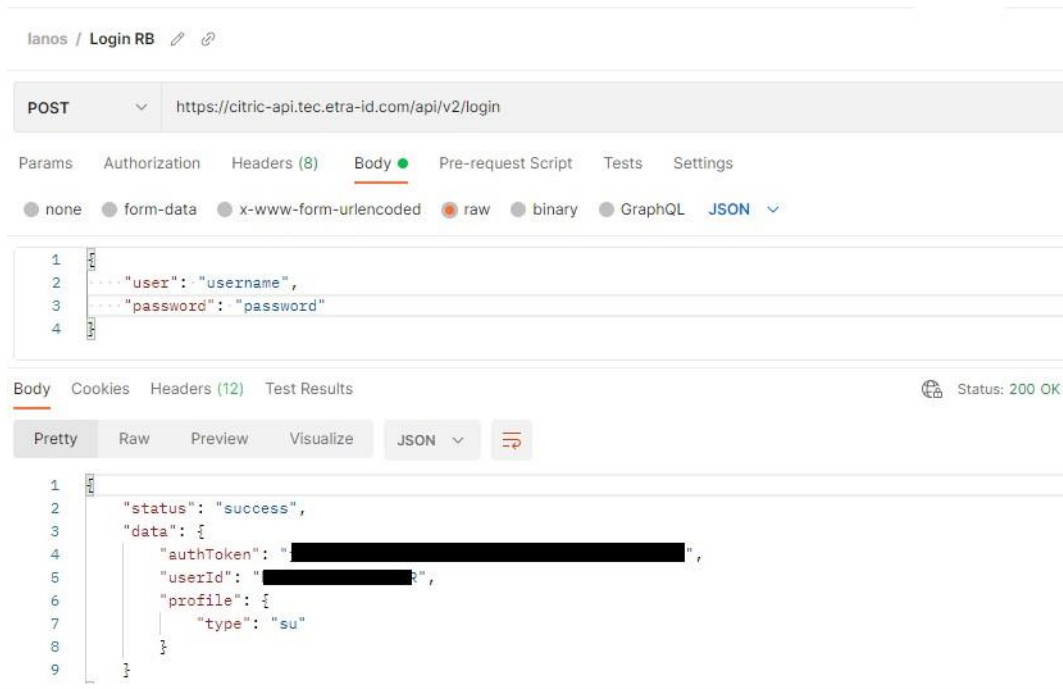
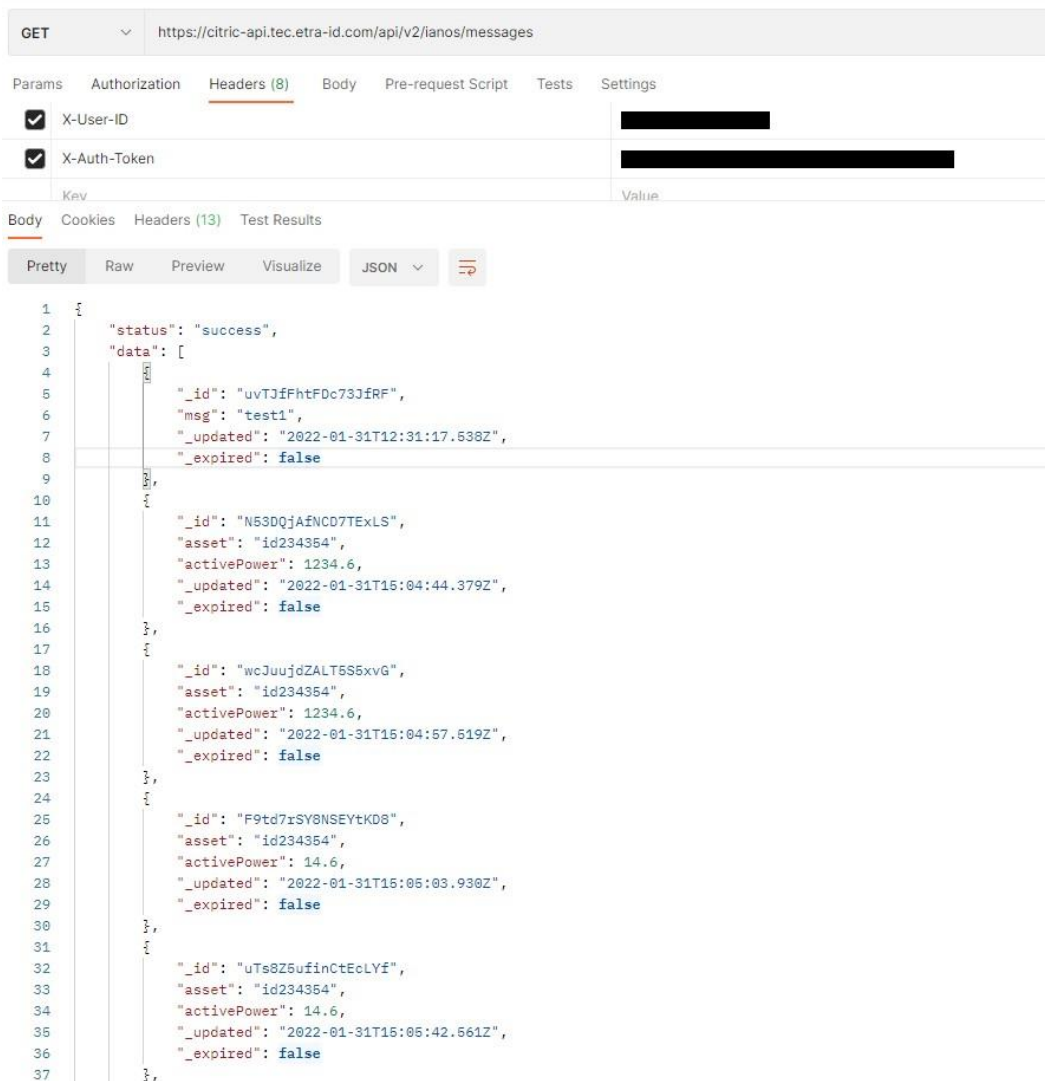


Figure 10: Login request with response using Postman

This way you will be provided a `userId` and a `token` that will be included in further calls to be authorized in the service. They can be used as headers, being `X-User-ID` and `X-Auth-Token` or as the query parameters `appid` and `keyId`.

Using these credentials in the API call you will be granted access to all the messages that has been sent to the RabbitMQ IANOS virtual host message queue. Here you can see an example in the Figure 11.



```

1  {
2    "status": "success",
3    "data": [
4      {
5        "_id": "uvTJfFhtFDc73JfRF",
6        "msg": "test1",
7        "_updated": "2022-01-31T12:31:17.538Z",
8        "_expired": false
9      },
10     {
11       "_id": "N53DQjAfNCD7TExLS",
12       "asset": "id234354",
13       "activePower": 1234.6,
14       "_updated": "2022-01-31T15:04:44.379Z",
15       "_expired": false
16     },
17     {
18       "_id": "wcJuujdZALT5S5xvG",
19       "asset": "id234354",
20       "activePower": 1234.6,
21       "_updated": "2022-01-31T15:04:57.519Z",
22       "_expired": false
23     },
24     {
25       "_id": "F9td7xSY8NSEYtKD8",
26       "asset": "id234354",
27       "activePower": 14.6,
28       "_updated": "2022-01-31T15:05:03.930Z",
29       "_expired": false
30     },
31     {
32       "_id": "uTs8Z6ufinCtEcLYf",
33       "asset": "id234354",
34       "activePower": 14.6,
35       "_updated": "2022-01-31T15:05:42.561Z",
36       "_expired": false
37     }
38   ]
39 }

```

Figure 11: Request and response to the messages queue

### 5.3.5 Collections allowed

Same as the messages collection, you will be granted access to all the queues created for this project. To access the database for 'ianos/ameland/asset', the route would be 'https://citricapi.tec.etra-id.com/api/v2/ianos/amelandAsset', take care with the camelcase in the last part of the route. Another interesting feature is that you can filter by id and receive only the entry with the id given. For example, if you want to know the actual value for the 'medidor1', you can write in the route 'https://citric-api.tec.etra-id.com/api/v2/ianos/amelandAsset/medidor1' and the result will be this only entry, as you can see in Figure 12. We are also currently working on a way to access the historic data for the sensors in a period of time using this same API, we will update this document with further work or information. The following version of this deliverable, to be summited in Month 32, will provide this further information and details of this information presented.

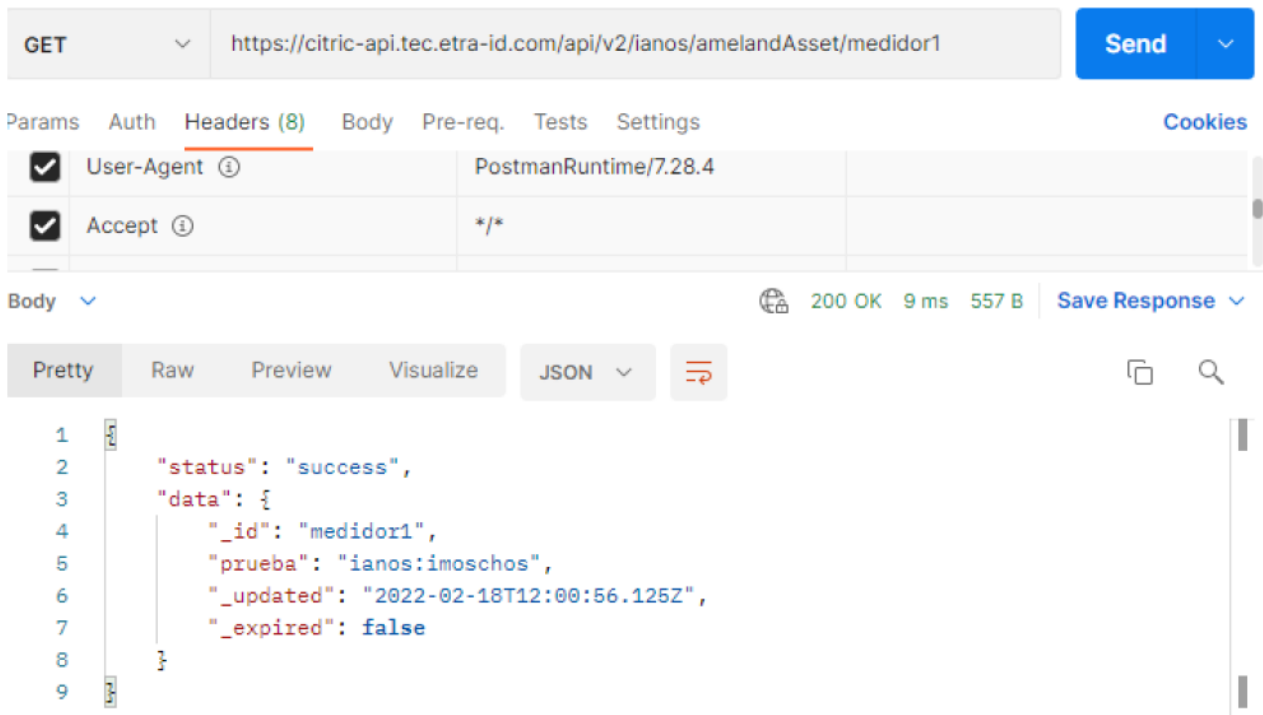


Figure 12: Filtered by ID on the route

## 5.4 Standards and Data models

The IANOS iVPP framework functionalities and energy services require the exchange and appropriate handling of data and control commands among the different system components and field devices. The iVPP platform must ensure the data transfer role, with a special focus on cyber-security aspects. Interoperability is seen as the key enabler of smart grids. A prominent definition describes interoperability as “the ability of two or more devices from the same vendor, or different vendors, to exchange information and use that information for correct cooperation”. In other words, two or more systems (devices or components) are interoperable, if these “two or more” systems are able to perform cooperatively a specific function by using information which is exchanged. This concept is illustrated below:



Figure 13: Interoperability definition

Interoperability can be categorized in eight levels from basic physical connectivity to a full alignment of business, policies and goals:



Figure 14: Interoperability categories

The different layers are focusing on specific interoperability aspects, from the most basic connectivity to business goal alignment. The lower layer refers to the physical connectivity of the assets. The 'network' and 'syntactic' interoperability is basically reached by agreeing on communication protocol (E.g., REST Web Services, MQTT, PLC, etc.) Semantic and business context interoperability is focusing on the pieces of information exchanged and tackles the selections of the appropriate data models to wrap the information messages. The upper layers are focusing on the functional alignment of components and comprises things like interoperability in the orchestration of messages, sequence of messaging, event handling, etc.

For some of the interoperability layers are standards widely used, that clearly define the interaction (especially for the communication protocols and data models). In this case, it's worth adopting the standard at both sides of communication. On the other hand, if such a standard for the communication does not exist, one has to be selected and adapted or even a specific ad-hoc mechanism should be defined. In any case, both sides of the communication must 'speak' the same language and give the same meaning to the information exchanged. In modern, decoupled, smart grid control systems, a set of different applications (potentially from different providers) are deployed for applying specific tasks. IANOS will not be an exception to that, and the different modules will be provided so that they can be 'plugged' or not to an installation or even replaced by other existing commercial software with few changes in case it would be necessary. Also, the field devices in the different pilots will be different (and compatible with different protocols, mechanisms, etc.) and thus a huge number of potential interconnections can be found while deploying IANOS components. Furthermore, any new component may imply developing or adapting several connectivity solutions to get full connectivity. This is even worse considering that legacy-monolithic distribution systems are not well suited to be extended with new functionalities offered by other modules, and therefore specific adapters and gateways are needed everywhere to maintain a coherence in data and business operations. This approach can become chaotic in small-to-mid sized systems. The solution proposed is to start using a common model for information exchange. With a common information model, different applications communicate with each other using the same language. This approach reduces the number of data transformations required from  $N * (N-1)$  to  $N$ . Integrating legacy applications typically involves the creation of application wrappers that map legacy data formats to a common one:

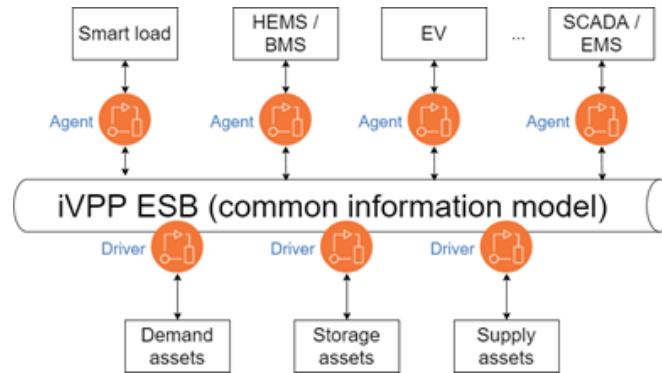


Figure 15: Common data exchange format interoperability

The field devices will be interfaced by means of drivers in the ESB, featuring the required communication protocols and transforming data to the common information model in the ESB. On the other hand, the different components in the VPP orchestration toolkit connects to the iVPP ESB by using gateways that adapts from the specific data model and the common information model. This model will allow IANOS to be extended and support multiple field device types. At the same time, the intelligent agents and applications in the VPP will be able to work without worrying about the details (connectivity, data models, etc.) of the specific field devices in each pilot or scenario.

Based on the work performed in WP2 “Requirements, Engineering & Decarbonization Road mapping” the several UCs defined in the project developed accordingly indicating the pilots’ assets interrelations. According to this information, a number of data exchanges have been identified. They are summarized in the following table represented in Figure 16:

Origin/End	IANOS iVPP	Forecast Provider	Localized EMS (FEID Plus & HEMS)	Demand Side Assets/Prosumer	Large-scale BESS	Dispatchable Assets	Non-Dispatchable Assets	Grid	Storage Assets	Locally implemented actuators	Hybrid Transformer	Smart Energy Router	V2G Charging Station	Electric Charging station	Natural Gas Platform	AHPD	Electrolyzer	Load Points	Gas Grid	Local non-Dispatchable Assets	District Heating Network
IANOS iVPP				6	13, 14	13			14		18	20	23	26		34					
Forecast Provider	5, 42, 43																				
Localized EMS (FEID Plus & HEMS)	1, 2, 3, 4																				
Demand Side Assets/Prosumer			1, 2, 3, 4																		
Large-scale BESS	3, 7																				
Dispatchable Assets	8, 9, 10, 27, 28, 37, 38, 39																				
Non-Dispatchable Assets	10, 11																				
Grid	12									12											
Storage Assets	15, 16																				
Locally implemented actuators																					
Hybrid Transformer	17																				
Smart Energy Router	19																				
V2G Charging Station	21, 22																				
Electric Charging Station	24, 25																				
Natural Gas Platform	29																				
AHPD	30, 31																				
Electrolyzer	35, 36																				
Load Points	32, 33																				
Gas Grid																					
Local non-dispatchable Assets																					
District Heating Network	41																				

Figure 16: Information exchanges matrix

This matrix specifies the pieces of information exchanged among system components. These pieces of information are identified in Table 9:

ID	Information	ID	Information
1	Energy Consumption Data	23	Optimal Setpoints for V2X charging stations
2	Energy Generation Data	24	Electric charging station real-time data
3	Battery real-time data	25	Electric charging station hard technical constraints
4	End-User comfort restrictions and operation settings	26	Optimal Setpoints for electric charging stations
5	Local meteorological forecasts	27	Fuel Cells and CHP hard technical constraints
6	Optimal Setpoints for demand side assets	28	Fuel Cells and CHP real-time data
7	BESS and electrolyzer hard technical constraints	29	Natural gas platform real-time data
8	Dispatchable assets real-time data	30	AHPD hard technical constraints
9	Dispatchable assets hard technical constraints	31	AHPD real-time data
10	Local Generation Energy Prices	32	Loads hard technical constraints
11	Non-Dispatchable assets data	33	Loads real-time data
12	Grid data	34	Optimal Set-point for AHPD
13	Optimal Set-points for dispatchable assets	35	Electrolyser hard technical data
14	Optimal Set-points for BESS	36	Electrolyser real-time data
15	Storage Assets hard technical constraints	37	Fuel Cells and CHP hard technical constraints
16	Storage Assets real-time data	38	Fuel Cells and CHP real-time data
17	Hybrid Transformer Data	39	Heat and hybrid pumps real-time data
18	Optimal Set-point for hybrid transformer	40	Heat and hybrid pumps hard technical constraints
19	Smart Energy Router Data	41	District Heating Network data
20	Optimal Set-point for Smart Energy Router	42	Forecasted Energy Consumption Data
21	V2X charging station real-time data	43	Forecasted Energy Generation Data
22	V2X charging station hard technical constraints		

Table 9: Exchanged Information types

As can be seen, most of the communications in the project will happen between iVPP platform and other components, in both directions. Information linked to measurements, technical characteristic of assets and forecasts are flowing to the iVPP from field devices and external data providers whilst optimal set-points are flowing in the opposite direction (from iVPP to the components). FEID-PLUS device, acting as a local EMS at customer premises, is also connecting to DSM assets. The iVPP will also integrate the data handled by this device. The details of the iVPP data model for field energy devices messages are presented in section the following section 5.5 Available data models for IANOS.

## 5.5 Available data models for IANOS

This section is intended to present a first draft of the available data models to be used in the IANOS project. Nevertheless, this section is a work in progress, and some slight changes may appear from this preliminary version. The final data model will be presented at the second version of this deliverable, which is intended to be summited at Month 32.

### 5.5.1 Rationale

The data related to energy assets can be fed into the ESB message broker (RabbitMQ) in MQTT or AMQP protocols, in a IoT fashion (bulk or very frequent data ingest that is processed, scaled and balanced in a way that prevents the system from being overflowed). The information exchange among ESB clients or components at the business and decision layers can be done using the previously mentioned protocols or (preferably) using NATS, which is better suited for the request/response communication pattern.

### 5.5.2 Data format for field devices messages

The processes of monitoring the energy assets messages are expecting the messages to have the specific data model described here. Examples of systems or energy assets that may use this mechanism for sending messages could be: Smart meters, RES dispatching centres, EMS SCADAs, PV or simulation algorithms that produce fake data periodically. The messages must be valid JSON documents that adhere to the JSON schema described:

```
{
  "$schema": "http://json-schema.org/draft-07/schema#",
  "$id": "http://etraid-id.com/dataMessage.json",
  "definitions": {
    "complexValue": {
      "$id": "#complexValue",
      "type": "object",
      "properties": {
        "value": {
          "type": "string",
          "$id": "value",
          "pattern": "^(.*)$"
        },
        "timestamp": {
          "type": "string",
          "$id": "timestamp",
          "pattern": "^(.*)$"
        },
        "quality": {
          "type": "integer",
          "default": 1
        }
      },
      "required": [
        "value",
        "timestamp"
      ]
    },
    "type": "object",
    "title": "The Root Schema",
    "required": [
      "id"
    ],
    "properties": {
      "id": {
        "type": "string",
        "pattern": "^(.*)$"
      },
      "states": {
        "$ref": "#/definitions/complexValue",
        "$id": "#states"
      }
    }
  }
}
```

```

    },
    "statesTimestamp": {
      "type": "string",
      "pattern": "^(.*)$"
    },
    "measurements": {
      "$ref": "#/definitions/complexValue",
      "$id": "#measurements"
    },
    "measurementsTimestamp": {
      "type": "string",
      "pattern": "^(.*)$"
    }
  }
}

```

An example of a valid JSON message could be:

```

{
  "id": "device_id",
  "states": {
    "communicationState": {
      "value": "OK",
      "timestamp": "2019-11-08T12:45:40.035Z",
      "quality": 1.0
    }
  },
  "statesTimestamp": "2019-11-08T12:45:40.035Z",
  "measurements": {
    "activePower": {
      "value": 50.53363,
      "timestamp": "2019-11-08T12:45:40.035Z",
      "quality": 1.0
    },
    "reactivePower": {
      "value": 12.363,
      "timestamp": "2019-11-08T12:45:40.035Z",
      "quality": 1.0
    },
    "frequency": {
      "value": 50.002,
      "timestamp": "2019-11-08T12:45:40.035Z",
      "quality": 1.0
    }
  },
  "measurementsTimestamp": "2019-11-08T12:45:40.035Z"
}

```

Basically, the JSON message has:

- An «id» field with the identifier of the device the measures and states are related to.
- A «states» object holding the states of the device. More than one state can be identified simultaneously, e.g. the communication state, the working mode, «door open» flag, etc. The values are normally predefined values (tags) or flags
- A «measurements» object holding the representation of different measured magnitudes associated with the device, e.g. active power, voltage, etc.
- Two fields with the timestamp of the last state or measurement reported. This is optional and can be omitted

The list of measurements and states names is defined in next section. For every state or measurement, the value is actually represented by an object with three fields: Actual value, timestamp and quality of the measurement:

- The «quality» field is a float number between 0 and 1, being 1 the highest quality value. Normally lowest values are associated to values calculated captured far away in time and probably not accurate. This field is optional and if not provided, 1 is assumed.
- The «value» field is a float number with the actual value

The «timestamp» field is a string representation of the measurement capture timestamp, in the ISO 8601 extended format [23]. The measurements received are treated as accumulative. A measurement received will be valid in our system even though other messages could have been received for this device with no update for this specific measurement. Our system could reduce the quality of the measurement in case it is not updated for a long time, but the new measurements messages do not replace the old measurements unless they overwrite them.

### 5.5.3 Measurements and states names

#### 5.5.3.1 Measurements names

As it has been previously commented, this is a preliminary version of the data model. Currently now, the technical team is defining in more detail the upcoming version of this information model. Nevertheless, in this deliverable, a preliminary list regarding the measurements names to be used is presented:

Measurement name	Units	Comments
activeEnergyImported	(kWh)	Accumulated active energy imported
activeEnergyExported	(kWh)	Accumulated active energy exported
activeEnergyImportedDelta	(kWh)	Delta active energy imported
activeEnergyExportedDelta	(kWh)	Delta active energy exported
reactiveEnergyQi	(kvarh)	Reactive energy 1st Quadrant
reactiveEnergyQii	(kvarh)	Reactive energy 2nd Quadrant
reactiveEnergyQiii	(kvarh)	Reactive energy 3rd Quadrant
reactiveEnergyQiv	(kvarh)	Reactive energy 4th Quadrant
reactiveEnergyQiL1	(kvarh)	Reactive energy 1st Quadrant, Phase 1
reactiveEnergyQiiL1	(kvarh)	Reactive energy 2nd Quadrant, Phase 1
reactiveEnergyQiiiL1	(kvarh)	Reactive energy 3rd Quadrant, Phase 1
reactiveEnergyQivL1	(kvarh)	Reactive energy 4th Quadrant, Phase 1
reactiveEnergyQiL2	(kvarh)	Reactive energy 1st Quadrant, Phase 2
reactiveEnergyQiiL2	(kvarh)	Reactive energy 2nd Quadrant, Phase 2
reactiveEnergyQiiiL2	(kvarh)	Reactive energy 3rd Quadrant, Phase 2
reactiveEnergyQivL2	(kvarh)	Reactive energy 4th Quadrant, Phase 2
reactiveEnergyQiL3	(kvarh)	Reactive energy 1st Quadrant, Phase 3
reactiveEnergyQiiL3	(kvarh)	Reactive energy 2nd Quadrant, Phase 3
reactiveEnergyQiiiL3	(kvarh)	Reactive energy 3rd Quadrant, Phase 3
reactiveEnergyQivL3	(kvarh)	Reactive energy 4th Quadrant, Phase 3
reactiveEnergyCapacitive	(kvarh)	
reactiveEnergyInductive	(kvarh)	
activePower	(kW)	
activePowerL1	(kW)	Active power Phase 1
activePowerL2	(kW)	Active power Phase 2
activePowerL3	(kW)	Active power Phase 3
activePowerImported	(kW)	
activePowerExported	(kW)	
reactivePower	(kvar)	
reactivePowerL1	(kvar)	Reactive power Phase 1
reactivePowerL2	(kvar)	Reactive power Phase 2
reactivePowerL3	(kvar)	Reactive power Phase 3
reactivePowerCapacitive	(kvar)	
reactivePowerInductive	(kvar)	
reactivePowerQi	(kvar)	Reactive power 1st Quadrant

reactivePowerQii	(kvar)	Reactive power 2nd Quadrant
reactivePowerQiii	(kvar)	Reactive power 3rd Quadrant
reactivePowerQiv	(kvar)	Reactive power 4th Quadrant
reactivePowerQiL1	(kvar)	Reactive power 1st Quadrant, Phase 1
reactivePowerQiiL1	(kvar)	Reactive power 2nd Quadrant, Phase 1
reactivePowerQiiiL1	(kvar)	Reactive power 3rd Quadrant, Phase 1
reactivePowerQivL1	(kvar)	Reactive power 4th Quadrant, Phase 1
reactivePowerQiL2	(kvar)	Reactive power 1st Quadrant, Phase 2
reactivePowerQiiL2	(kvar)	Reactive power 2nd Quadrant, Phase 2
reactivePowerQiiiL2	(kvar)	Reactive power 3rd Quadrant, Phase 2
reactivePowerQivL2	(kvar)	Reactive power 4th Quadrant, Phase 2
reactivePowerQiL3	(kvar)	Reactive power 1st Quadrant, Phase 3
reactivePowerQiiL3	(kvar)	Reactive power 2nd Quadrant, Phase 3
reactivePowerQiiiL3	(kvar)	Reactive power 3rd Quadrant, Phase 3
reactivePowerQivL3	(kvar)	Reactive power 4th Quadrant, Phase 3
apparentPower	(kVA)	
apparentPowerL1	(kVA)	Apparent power, Phase 1
apparentPowerL2	(kVA)	Apparent power, Phase 2
apparentPowerL3	(kVA)	Apparent power, Phase 3
current	(A)	In 3 phase installations, average of the three phases
currentL1	(A)	Current, Phase 1
currentL2	(A)	Current, Phase 2
currentL3	(A)	Current, Phase 3
currentNeutral	(A)	Neutral current
voltage	(V)	
voltageL1	(V)	Voltage, Phase 1
voltageL2	(V)	Voltage, Phase 2
voltageL3	(V)	Voltage, Phase 3
voltageL1L2	(V)	Voltage difference between Phase 1 and Phase 2
voltageL2L3	(V)	Voltage difference between Phase 2 and Phase 3
voltageL3L1	(V)	Voltage difference between Phase 3 and Phase 1
powerFactor	0..1	
powerFactorL1	0..1	Power factor, Phase 1
powerFactorL2	0..1	Power factor, Phase 2
powerFactorL3	0..1	Power factor, Phase 3
frequency	(Hz)	
voltageTotalHarmonicDistortion	%	
voltageTotalHarmonicDistortionL1	%	Voltage Total Harmonic Distortion, Phase 1
voltageTotalHarmonicDistortionL2	%	Voltage Total Harmonic Distortion, Phase 2
voltageTotalHarmonicDistortionL3	%	Voltage Total Harmonic Distortion, Phase 3
voltageHarmonic1	(V)	Voltage Harmonic 1
voltageHarmonic2	%	Voltage Harmonic 2
voltageHarmonicN	%	Voltage Harmonic N (2 >= N >= 42)
currentTotalHarmonicDistortion	%	
currentTotalHarmonicDistortionL1	%	Current Total Harmonic Distortion, Phase 1
currentTotalHarmonicDistortionL2	%	Current Total Harmonic Distortion, Phase 2
currentTotalHarmonicDistortionL3	%	Current Total Harmonic Distortion, Phase 3
currentHarmonic1	(A)	Current Harmonic 1
currentHarmonic2	%	Current Harmonic 2
currentHarmonicN	%	Current Harmonic N (2 >= N >= 42)

Table 10: Measurements and states names lists

It is worth mentioning that the upcoming version of the deliverable 4.2 “iVPP secure data monitoring and governance” will include the definitive version of the information model to be followed in the IANOS project. This deliverable is expected to be forwarded in month 32 of the project.

#### 5.5.3.2 States names

Hereafter, a list regarding the states names to be used in the ESB Common Information Model is presented:

State name	Possible values	Comments
communicationStatus	0: ok	Asset connectivity
	1: noCommunication	

Table 11: States names list

### 5.5.3.3 Storage specific measurements names

Hereafter, a list regarding the storage specific measurements names to be used in the ESB Common Information Model is presented:

Measurement name	Units	Comments
stateOfCharge	%	State of charge
stateOfHealth	%	State of health
chargeAvailable	(kW)	
dischargeAvailable	(kW)	
maxBatteryCellTemperature	°C	Max battery cell temperature
minBatteryCellTemperature	°C	Min battery cell temperature
inverterTemperature	°C	Inverter temperature

Table 12: Storage specific measurements names lists

### 5.4.3.4 Storage specific status names

Hereafter, a list of the storage specific status name is being presented.

State name	Possible values	Comments
status	0: disconnected	Battery/storage status
	1: connected	
	2: charge	
	3: discharge	
	4: standby	
	5: error	
	6: busy	
	7: islanding	
workingMode	0: Standard	Battery/storage working mode
	1: Manual	
	2: Alarm	
	3: Backup	
	4: Test	
	5: Schedule	
	6: Config	
controlMode	0: System Manually set inverter target power	Battery/storage control model (closed loop)
	1: Load Manually set target power at meter	
	2: PvsF Frequency regulation	
	3: PvsV Voltage regulation	
	4: QvsV Voltage regulation	

Table 13: Storage specific status names lists

## 5.5.4 Data communication for field device messages

The generated JSON messages created according to the previous definition must be sent to the ESB message broker in MQTT or AMQP protocols. Both protocols provide an endpoint for the clients to “send” the data, and both protocols require the messages to be “tagged” or identified with a topic (or routing key in AMQP nomenclature). Topics are structured in a hierarchy similar to folders and files in a file system using a delimiter (the forward slash ‘/’ in MQTT, and the dot ‘.’ In AMQP). The hierarchy of the topics helps identifying the nature of the message and the format must be the following:

<SYSTEM\_NAME>.<ASSET\_TYPE>.<ASSET\_UNIQUE\_IDENTIFIER>

Examples of these could be:

AMELAND.METER.31245

## TERCEIRA/FARM/VELEBIT

Properties of the topic names:

- Are Case sensitive
- Use UTF-8 strings.
- Must consist of at least one character to be valid.

The asset type and identifier must be agreed between the relevant partners and ETRA as ESB developer.

### 5.5.5 Platform security

Regarding the security, different mechanisms will be established to enforce security:

- All connections to the ESB broker will require valid credentials
- The access to specific topics will be restricted by user, so that only the clients with specific credential will be able to publish or subscribe to data or restricted topics. The configuration of the permissions for each credential will be configured at the ESB.
- The ESB will allow clients to authenticate by using either user & password, long-time tokens or certificates
- All the communication channels will use the secure version using SSL (MQTTS, HTTPS, AMQPS)

## 5.6 Secured ESB weather information communication data model

### 5.6.1 Rationale

The data related to current and forecasted weather information is taken from online weather information server weatherbit.io by the ESB message broker and offered to ESB client by different protocols (AMQP and NATS).

The different ESB clients can subscribe to weather information in different locations, and the ESB will periodically forward them the most up-to data or the requested weather forecasting.

### 5.6.2 Data model for weather information messages

The weather information messages will adhere to a specific data model described here. The messages will be valid JSON documents that adhere to the JSON schema described here:

### 5.6.3 Real time weather messages data model

```
{
  "location": {
    "name": "Valencia,ESP",
    "latitude": 39.469917,
    "longitude": -0.3763
  },
  "timestamp": "2019-11-20T13:50:00Z",
  "atmosphericPressure": 1004.1, // Pressure (mbar)
  "seaLevelPressure": 1008.3, // Sea level pressure (mbar)
  "windSpeed": 3.13, // Wind speed (m/s)
  "windDirection": 222, // Wind direction (degrees)
  "windDirectionCardinal": "SW", // Abbreviated wind direction
  "temperature": 18.3, // Temperature (Celcius)
  "apparentTemperature": 18.4, // Apparent temperature (Celcius)
  "relativeHumidity": 37, // Relative humidity (%)
  "dewPoint": 3.4, // Dew point (Celcius)
  "cloudCoverage": 33, // Cloud coverage (%)
}
```

```

    "visibility": 5, // Visibility (km)
    "precipitationAccumulation": 0, //Liquid equivalent precipitation rate
(mm/hr)
    "snowfallAccumulation": 0, // Snowfall (mm/hr)
    "ultravioletIndex": 4.34596, // UV Index (0-11+)
    "airQualityIndex": 0, // Air Quality Index [US - EPA standard 0 - +500]
    "diffuseHorizontalSolarIrradiance": 85.14, // Diffuse horizontal solar
irradiance (W/m^2) [Clear Sky]
    "directNormalSolarIrradiance": 729.53, // Direct normal solar irradiance
(W/m^2) [Clear Sky]
    "globalHorizontalSolarIrradiance": 363.91, // Global horizontal solar
irradiance (W/m^2) [Clear Sky]
    "solarRadiation": 357.2, // Estimated Solar Radiation (W/m^2)
    "elesolarElevationAngle": 23.05, // Solar elevation angle (degrees)
    "solarHourAngle": 54 // Solar hour angle (degrees)
}

```

### 5.6.4 Forecasted weather messages data model

```

[ {
  "location": {
    "name": "Valencia,ESP",
    "latitude": 39.469917,
    "longitude": -0.3763
  },
  "timestamp": "2019-11-20T15:00:00Z",
  "atmosphericPressure": 1007.61,
  "seaLevelPressure": 1008.73,
  "windSpeed": 2.74225,
  "windDirection": 247,
  "windDirectionCardinal": "WSW",
  "windGustSpeed": 6.59272, // Wind gust speed (m/s)
  "temperature": 16.4,
  "apparentTemperature": 16.4,
  "relativeHumidity": 34,
  "dewPoint": 0.4,
  "cloudCoverage": 33,
  "cloudCoverageHighLevel": 0, // High-level (>5km AGL) cloud coverage (%)
  "cloudCoverageMidLevel": 9, // Mid-level (~3-5km AGL) cloud coverage (%)
  "cloudCoverageLowLevel": 25, // Low-level (~0-3km AGL) cloud coverage (%)
  "visibility": 24.135,
  "precipitationAccumulation": 0,
  "precipitationProbability": 0, // Probability of Precipitation (%)
  "snowfallAccumulation": 0,
  "snowDepth": 0, // Snow Depth (mm)
  "ultravioletIndex": 1.79043,
  "diffuseHorizontalSolarIrradiance": 69.5,
  "directNormalSolarIrradiance": 616.06,
  "globalHorizontalSolarIrradiance": 226.87,
  "solarRadiation": 222.945,
  "ozone": 331.598 // Average Ozone (Dobson units)
},
... // One message per hour

```

### 5.6.6 Request API

The forecasted weather information can be queried by sending request messages to the NATS endpoint of the ESB. The request messages must be sent with the following routing keys:

IANOS.weather  
Or

## IANOS.weatherforecast

The body of the request message must contain the request parameters formatted as a JSON object with the following data model:

```
{
  "cityName": "Valencia", // (Mandatory) Name of the place, used as a kind of
  ID.
  "lat": "39.469917", // (Query option 1) Latitude.
  "lon": "-0.376300", // (Query option 1) Longitude.
  "city": "Valencia", // (Query option 2) Name of the city, e.g. "Valencia",
  "Valencia,ES". Can be combined with the property "country".
  "postalCode": "46014", // (Query option 3) Postal code.
  "country": "ES", // (Query options 2 and 3) Country in ISO 3166-1 alpha-2
  code format, e.g. "ES". It is mandatory for query option 3 and optional for query
  option 2.
  "hours": 48, // (Optional, only for forecast) Number of hours in the future
  to retrieve. Default (and maximum) value: 48
}
```

### 5.6.7 Subscribe to real time weather data

There will be the possibility to subscribe to weather data changes and receive the information proactively. This can be done by subscribing using AMQP to a specific 'Queue' and configuring a routing rule from the IANOS 'exchange' to this queue. Different routing rule based on the message topics could be defined to select What information to receive in the selected queue. Examples of such rules could be:

IANOS.VALENCIA.weather  
Or  
IANOS.46013.weatherforecast  
Or  
IANOS.myPoint.weather

The topic can be splitted by dots. The central part is the identifier of the piece of weather data (that could be configured using a web form). The final part of the topic will allow to indicate the willingness to receive real time or forecasted data. The messages received after subscribing will have the same data model as the one described in the request API. Accordingly, to the pilot's location, the weather service data is going to be configured to the following coordinates:

Coordinates Ameland demonstration site	
<b>Ballumerbocht</b>	53°26'10.4"N, 5°42'58.0"E

Table 14: Coordinates Ameland demonstration site

Coordinates Terceira demonstration site	
<b>Windfarm (CAEN)</b>	38°43'04.3"N 27°07'13.3"W
<b>Windfarm (EDA Renovaveis)</b>	38°42'12.6"N 27°06'25.3"W
<b>PV Solar Farm</b>	38°43'25.9"N 27°04'13.0"W
<b>Terra Cha Neighbourhood</b>	38°40'14.4"N 27°15'16.8"W

Table 15: Coordinates Terceira demonstration site

## 6. Conclusions

This deliverable consists of three main sections – the first one provides an insight of the personal data protection and security of networks. The second one addresses the issue of DPIA-PA for the products developed in IANOS and the recommendations emerging from the analysed products. In the third place, based on the security and privacy concepts that have been introduced, it will be presented the Enterprise Service Bus (ESB), one of the tools that would introduce the secured APIs and communication pipelines for sending the required information in-between VPP (regarded in the WP4-IANOS Multi-Layer VPP Operational Framework) with the field devices and external systems.

The analysis of the PDP legislation in the countries involved in the IANOS demonstration sites (In the Netherlands, the Island of Ameland and in Portugal, the Island of Terceira) has been analysed. These countries have transported to the EU PDP legislation into their primary law. According to the EU regulation – GRDP is obligatory for the EU MSs, a fact that has been checked since both demonstration site countries are Member States. In order to be in compliance with GDPR to mitigate the risks that could endanger the rights and freedoms of natural persons and the controller, the responsibility of performing a DPIA is given to the data controller. This procedure should be performed in those cases where processing operations that involve the use of new technologies where no DPIA has been carried out. The document also introduces the presentation of a leaflet that the EC has issued in order to prepare companies to the implementation of GDPR measures. (Seven steps for business to get ready for the General Data Protection Regulation) [7].

From the research reading the PDP in the IANOS products, the following conclusions can be extracted:

- DPIA-PA procedure was applied to each one of the IANOS products. The objective of this practice is to assess if the product/application that it is being developed, tested and demonstrated in the project could require collection, processing and archiving personal data in a manner that may result in a high risk to the rights and freedoms of natural persons. DPIA is one of the main tools that enables efficient enforcement of the rules prescribed by GDPR. Of course, the data controller deploying the product is obliged to perform its own DPIA about the implementation if it is considered necessary.
- For that purpose, a questionnaire was developed based on the questions for preassessment and the criteria determining the need to conduct a DPIA. The questionnaire has been structured in five parts covering the following criteria for determining whether to conduct a DPIA is necessary.
  - I. Cases foreseen by the GRPR, DPAs or EDPB
  - II. Relevant occurrence
  - III. Personal data involved and DPIA-related data processing activities
  - IV. Status of a data controller or a data processor
  - V. New technologies and other criteria
- Based on the DPIA-PA analysis of the product, some recommendations could be outlined in three different categories. This results are expressed in Section 4.2 Questionnaire results – DPIA Pre-assessment based on the responses that are available in 8. Annex:
  - I. Grid Oriented Optimizer, Virtual Energy Console, Non-intrusive characterization of Energy Flexibility in water heating systems, Hybrid Transformer, V2G Charging products do not process personal data and the conduction of a DPIA is not necessary.

- II. LCA/LCC Toolkit, System Modeller, OptiMEMS, CleanWatts KIPLO, Aggregation and Classification Intelligence, Forecasting Engine, DLLT-Based Transactive Platform, Enterprise Service Bus and FEID-Plus. These products do not process personal data in the scope of the IANOS Use Cases. They adequately process the data which is encrypted under an Identifier (ID). The act of providing those appropriate measures, such as pseudonymisation, are taken to preserve the rights of data subjects. Nevertheless, further commercial application of these products may foresee processing of personal data directly. In that case, measures have to be applied during the development of the products, such as adequate PDP measures. The potential DPIA assessment could be performed in order to assess if the developed PDP, after the commercialization, could reduce the risk on the rights and freedoms of the natural persons at an acceptable level.
- III. Crowdequity Platform, Smart Energy Router are both products that intended to process personal data, due to the nature of the products. Nevertheless, due to the scope of the IANOS project, personal data will not be processed as so as demonstration to prove the tool.

As far as the Enterprise Service Bus is concerned, this deliverable has reviewed the architecture in which the service is going to be developed, indicating the technologies that support the bulk data ingestion. Moreover, based on work performed by in Task 4.4, the architecture of the iVPP is developed, the ESB plays a central role in the information transmission, not only from iVPP modules communication, but with the information circulating from different assets. In order to coordinate a successful integration among the different communicating assets, a guide for the connection, a standards and data models list (including the weather information communication) is provided in this deliverable. Nevertheless, it must be stated that, as long as the integration of the assets in the different pilot sites is happening, changes may occur. This would be reflected in the upcoming version of the deliverable 4.1 “iVPP secure data monitoring and governance” v2 which will be submitted in month 32. As already mentioned, this first version will take a deeper look on the horizontal functionalities of the Enterprise Service Bus, whereas the upcoming version of this deliverable regarding Task 4.1 “Cyber-Secure data monitoring and VPP governance” will take a deeper look on the IANOS Def-Pi platform.

## 7. References

- [1] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.*
- [2] "Law for the protection of personal information. Dutch Government," [Online]. Available: <https://wetten.overheid.nl/BWBR0011468/2018-05-01>.
- [3] N. -. D. P. Overview. [Online]. Available: <https://www.dataguidance.com/notes/netherlands-data-protection-overview>.
- [4] DataGuidance, "Portugal - Data Protection Overview," [Online]. Available: <https://www.dataguidance.com/notes/portugal-data-protection-overview>.
- [5] G. D. P. Regulation. [Online]. Available: <https://gdpr-info.eu/>.
- [6] D. Guidance, "Portugal - Data Protection overview," [Online]. Available: <https://www.dataguidance.com/notes/portugal-data-protection-overview>.
- [7] European Commission, "Seven steps for business to get ready for the General Data Protection Regulation," [Online]. Available: [https://ec.europa.eu/info/sites/default/files/gdpr2019-smes\\_7\\_steps\\_brochure-en-v03\\_lr\\_qc.pdf](https://ec.europa.eu/info/sites/default/files/gdpr2019-smes_7_steps_brochure-en-v03_lr_qc.pdf).
- [8] "Guidelines on Data Protection Officers ('DPOs')," [Online]. Available: <https://ec.europa.eu/newsroom/article29/items/612048>.
- [9] European Commission, "The New EU Data Protection Regulation - Better Rules for European Businesses," [Online]. Available: [https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules\\_en](https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en).
- [10] Working Party on the Protection of Individuals with Regard to the Processing of Personal Data set by Directive 95/46/EC of the European Parliament (Article 29 Working Party), "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679," October 2017. [Online]. Available: <https://ec.europa.eu/newsroom/article29/items/611236>.
- [11] Smart Grids Task Force, Expert Group 2 (Regulatory Recommendations for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment), *Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems*, September, 2018.

- [12] E. S. Union. [Online]. Available: [https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/european-security-union\\_en](https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/european-security-union_en).
- [13] European Commission, *A Digital Single Market Strategy for Europe*, Brussels, 2015.
- [14] European Commission, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, Brussels, 2013.
- [15] *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.*
- [16] *Directive 2008/114/EC – identification and designation of European critical infrastructures and assessment of the need to improve their protection.*
- [17] P. Novotny, J. Markuci, D. Rehak, I. Almarzouqi and L. Janusova, "Critical Infrastructure Designation in European Union Countries: Implementation of Systems Approach," *Communications*, vol. 2, pp. 163-169, 2016.
- [18] European Commission, *Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure*, Brussels, 2013.
- [19] E. Luiif, A. Nieuwenhuijs, M. Klaver, M. van Eeten and E. Cruz, "Empirical Findings on Critical Infrastructure Dependencies in Europe," in *Critical Information Infrastructure Security. CRITIS 2008. Lecture Notes in Computer Science*, Berlin, Heidelberg, Springer, 2009, pp. 302-310.
- [20] E. Report, "Cyber Security in the Energy Sector," 2017.
- [21] ENISA, "Smart Grids Task Force EG2 Deliverable - Proposal of a list of security measures for smart grids," 2013.
- [22] D. P. a. C.-S. i. t. S. G. e. Smart Grid Task Force 2012-2014. Expert Group 2: Regulatory Recommendations for Privacy, "Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems," 2018.
- [23] "ISO 8601," [Online]. Available: [https://es.wikipedia.org/wiki/ISO\\_8601](https://es.wikipedia.org/wiki/ISO_8601).
- [24] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.*

- [25] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.*
- [26] *Law on Protection of Personal Data*, Official Gazette of Bosnia and Herzegovina No. 49/06, 76/11 and 89/11.
- [27] *Law on Personal Data Protection*, Official Gazette of the Republic of Macedonia No. 7/2005, 103/2008, 124/2008, 124/2010, 135/2011, 43/2014, 153/2015 and 99/2016.
- [28] *Personal Data Protection Law of Montenegro*, Official Gazette of Montenegro No. 79/08, 70/09, 44/12 and 22/17.
- [29] *Law on Personal Data Protection*, Official Gazette of Serbia No. 97/08, 104/09, 68/12.
- [30] *Law on Personal Data Protection*, Official Gazette of Serbia No. 87/18.
- [31] European Commission, "Seven steps for business to get ready for the General Data Protection Regulation," [Online]. Available: [https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules\\_en](https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en).
- [32] European Commission, "A new era of data protection in the EU - What changes after May 2018," [Online]. Available: [https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules\\_en](https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en).
- [33] Republic of Macedonia, Directorate for Personal Data Protection, Rulebook About the Form and Content of the Transfer of Personal Data to Other Countries and Manner of Keeping the Records.
- [34] *Directive 2005/89/EC of the European Parliament and of the Council of 18 January 2006 concerning measures to safeguard security of electricity supply and infrastructure investment.*
- [35] Smart Grids Task Force - Expert Group 2 - Cybersecurity, "Recommendations for the European Commission on Implementation of a Network Code on Cybersecurity, 2nd Interim Report," July, 2018.
- [36] ENISA, "Smart Grids Task Force EG2 Deliverable - Proposal of a list of security measures for smart grids," 2013.
- [37] Cooperation Group, *Reference document on security measures for Operators of Essential Services*, 2018.
- [38] ENISA, "Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors," 2015.
- [39] *Commission Regulation (EU) 2017/1485 establishing a guideline on electricity transmission system operation.*

- [40] European Commission, *Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union*, Brussels, 2017.
- [41] Cooperation Group, *Reference document on incident notification for Operators of Essential Services (circumstances of notification)*, 2018.

## 8. Annex

### 8.1 Grid Oriented Optimizer

Pre-assessment and criteria determining the need to conduct a Data Protection Impact Assessment (DPIA)				
1	Cases foreseen by the GDPR, Data Protection Authorities (DPAs) or the European Data Protection Board			
1	Profiling: Consumers	a	Are you designing a Smart Grid application or system that allows for consumer profiling or another similar activity?	No, the INTEMA.grid tool does not allow for consumer profiling, but can estimate it based on design specification for related energy systems, in the form of synthetic data.
		b	Is your application using data (names, addresses, contact and other descriptor/identifier) for individual consumers that are natural persons?	No
		c	Do you collect data for energy consumption (demand information and time stamps) for households? Is the data for consumption in some way related to consumers' name, address or other identifiers?	No
		d	In the application, do you create profiles of types of consumers (natural persons)?	We create prosumers and major production/consumption profiles, based on design data, conducting simulations and not actual data
		e	In the application, do you collect any data for time of use/hours of operation for particular equipment in households or comfort indicators in households (temperature/humidity/lighting)? Is the data in some way related to owners' name, address or other identifiers?	No
2	Profiling: Generation and Storage	a	Do you collect data (names and addresses) from data subjects (natural persons) that are owners of generation/storage facilities?	No
		b	In the application, do you collect data for power and energy production/demand from data subjects (natural persons) that are owners of generation/storage facilities? Is the data in some way related to owners' name, address or other identifiers?	No
		c	In the application, do you create profiles of types of generators/storage owned by natural persons?	We create prosumers and major production/consumption profiles, based on design data, conducting simulations and not actual data
		d	In the application, do you collect any data for time of use/hours of operation for particular generation/storage facility owned by a natural person? Do you collect data on available storage capacity of a storage facility owned by natural person? Is the data in some way related to owners' name, address or other identifiers?	No

3	Profiling: data from natural persons	a	If you collect any data from natural persons in the application, what is the frequency of measurement and transmission of data? Please provide response for all types of data collected.	-
		b	In the application, do you perform remote readings for billing purposes or network planning from natural persons?	No
		c	In the application, do you collect/send any billing data and information on consumers' payment method from/to natural persons?	No
		d	Is your application providing online information to consumers/owners of generation or storage facilities that are natural persons? Please describe.	No
4	Large Scale Data Personal processing	a	Is your application processing <b>personal data</b> on a large scale? (large-scale processing operations which aim to process a considerable amount of <b>personal data</b> at regional, national or supranational level and which could affect a large number of data subjects)	No
5	International transfer of personal data	a	In case of international transfer of personal data to a third country, what mechanisms are in place to ensure adequacy of data protection?	No
		b	For your application, do you envisage any contracts with clauses for data transfer from data controllers in EU to data controllers in third countries?	No
6	Smart Grid operations that prevent users from using a service	a	Will the outcome of use of the Smart Grid application lead to preventing consumers from using a service (e.g. disconnection)?	No
		b	In the application, do you perform remote switching of equipment/facilities owned by natural persons? Please explain the purpose of the remote switching.	No
		c	If the use of the Smart Grid application leads to preventing consumers from using a service, do you make a contract with the consumer? Please describe what the contract includes.	No
7	Processing of special categories of personal data	a	In the application, are you processing special categories of data defined in Art. 9 or Art. 10 of the GDPR?	No
8	Applications for which the need to conduct DPIA is	a	Is the Smart Grid application or system under design listed by the national Data Protection Authority in your country or by the European Data Protection guidelines as one that requires DPIA?	No

	determined by authorities	b	Is the Smart Grid application or system under design listed by the national Data Protection Authority in your country or by the European Data Protection guidelines as one that does not require DPIA?	No
II	Relevant occurrence			
1	Introducing a new business process (If an existing product is revised or upgraded for the purposes of the project)	a	Are you designing a new business process within the Smart Grid situation or are you making significant changes to an existing Smart Grid situation?	No
		b	Are there new types of information introduced and processed in the new business process?	-
		c	Is the new business process connected to collection and processing of personal data? Description	-
III	Personal Data involved and DPIA-related Processing activities			
1		a	Does the design/change require your application to collect and process any personal data? Explain if it is affirmative.	No
		b	Is the purpose or scope of the process/application capable to have an impact on the rights and freedoms of natural persons? Explain if it is affirmative.	No
IV	Status of a Data Controller or a Data Processor			
1		a	Who will have the role of Data Controller and Data Processor for your product/application during the development and testing/implementation of the product within the project? (it may be too early to have an explicit answer to this question, but you may have an idea of the possible roles in future)	No
		b	Do you plan to define Data Protection (contractual) requirements between you as developer and the possible future Processor/Controller?	-
V	New technologies and other criteria			
1		a	In your application, do you plan to implement new technologies (smart meter environment, cloud processing, Internet of things)?	No
		b	Does the design/change of the product/application contain any other criterion that may affect rights and freedoms of natural persons?	No

Table 16: DPIA-PA Questionnaire for Grid Oriented Optimizer

## 8.2 LCA/LCC Toolkit

Pre-assessment and criteria determining the need to conduct a Data Protection Impact Assessment (DPIA)

I Cases foreseen by the GDPR, Data Protection Authorities (DPAs) or the European Data Protection Board				
1	Profiling: Consumers	a	Are you designing a Smart Grid application or system that allows for consumer profiling or another similar activity?	Yes
		b	Is your application using data (names, addresses, contact and other descriptor/identifier) for individual consumers that are natural persons?	No, the monitoring is on an asset basis, e.g. building, power plant, transformers....
		c	Do you collect data for energy consumption (demand information and time stamps) for households? Is the data for consumption in some way related to consumers' name, address or other identifiers?	Yes we collect, but the data is not related to any consumers' personal data and identity
		d	In the application, do you create profiles of types of consumers (natural persons)?	No
		e	In the application, do you collect any data for time of use/hours of operation for particular equipment in households or comfort indicators in households (temperature/humidity/lighting)? Is the data in some way related to owners' name, address or other identifiers?	Yes, primarily energy consumption and production profiles from RES based systems and in specific case storage ones. This data is not related to any owners personal data
2	Profiling: Generation and Storage	a	Do you collect data (names and addresses) from data subjects (natural persons) that are owners of generation/storage facilities?	No
		b	In the application, do you collect data for power and energy production/demand from data subjects (natural persons) that are owners of generation/storage facilities? Is the data in some way related to owners' name, address or other identifiers?	No
		c	In the application, do you create profiles of types of generators/storage owned by natural persons?	Yes in some cases, particularly for those who live in buildings
		d	In the application, do you collect any data for time of use/hours of operation for particular generation/storage facility owned by a natural person? Do you collect data on available storage capacity of a storage facility owned by natural person? Is the data in some way related to owners' name, address or other identifiers?	Yes and the data is not related to any personal data
3	Profiling: data from natural persons	a	If you collect any data from natural persons in the application, what is the frequency of measurement and transmission of data? Please provide response for all types of data collected.	-
		b	In the application, do you perform remote readings for billing purposes or network planning from natural persons?	We perform readings but not for billing purposes, rather than planning purposes
		c	In the application, do you collect/send any billing data and information on consumers' payment method from/to natural persons?	No

		d	Is your application providing online information to consumers/owners of generation or storage facilities that are natural persons? Please describe.	If required by the natural persons, we are available providing such information; though is not our primary scope
4	Large Scale Data Personal processing	a	Is your application processing <b>personal data</b> on a large scale? (large-scale processing operations which aim to process a considerable amount of <b>personal data</b> at regional, national or supranational level and which could affect a large number of data subjects)	No
5	International transfer of personal data	a	In case of international transfer of personal data to a third country, what mechanisms are in place to ensure adequacy of data protection?	Data anonymization, while any data are stored only for serving the needs of IANOS partnership
		b	For your application, do you envisage any contracts with clauses for data transfer from data controllers in EU to data controllers in third countries?	No
6	Smart Grid operations that prevent users from using a service	a	Will the outcome of use of the Smart Grid application lead to preventing consumers from using a service (e.g. disconnection)?	No
		b	In the application, do you perform remote switching of equipment/facilities owned by natural persons? Please explain the purpose of the remote switching.	No
		c	If the use of the Smart Grid application leads to preventing consumers from using a service, do you make a contract with the consumer? Please describe what the contract includes.	No
7	Processing of special categories of personal data	a	In the application, are you processing special categories of data defined in Art. 9 or Art. 10 of the GDPR?	No
8	Applications for which the need to conduct DPIA is determined by authorities	a	Is the Smart Grid application or system under design listed by the national Data Protection Authority in your country or by the European Data Protection guidelines as one that requires DPIA?	No
		b	Is the Smart Grid application or system under design listed by the national Data Protection Authority in your country or by the European Data Protection guidelines as one that does not require DPIA?	
II	Relevant occurrence			
1	Introducing a new business process (If an existing product is revised or upgraded for the purposes of the project)	a	Are you designing a new business process within the Smart Grid situation or are you making significant changes to an existing Smart Grid situation?	No
		b	Are there new types of information introduced and processed in the new business process?	No
		c	Is the new business process connected to collection and processing of personal data? Description	-
III	Personal Data involved and DPIA-related Processing activities			

1		a	Does the design/change require your application to collect and process any personal data? Explain if it is affirmative.	No
		b	Is the purpose or scope of the process/application capable to have an impact on the rights and freedoms of natural persons? Explain if it is affirmative.	No
IV	Status of a Data Controller or a Data Processor			
1		a	Who will have the role of Data Controller and Data Processor for your product/application during the development and testing/implementation of the product within the project? (it may be too early to have an explicit answer to this question, but you may have an idea of the possible roles in future)	CERTH's DPO
		b	Do you plan to define Data Protection (contractual) requirements between you as developer and the possible future Processor/Controller?	No
V	New technologies and other criteria			
1		a	In your application, do you plan to implement new technologies (smart meter environment, cloud processing, Internet of things)?	Yes
		b	Does the design/change of the product/application contain any other criterion that may affect rights and freedoms of natural persons?	No

Table 17: DPIA-PA Questionnaire for the LCA/LCC Toolkit

## 8.3 Crowdequity Platform

I Cases foreseen by the GDPR, Data Protection Authorities (DPAs) or the European Data Protection Board				
1	Profiling: Consumers	a	Are you designing a Smart Grid application or system that allows for consumer profiling or another similar activity?	Yes
		b	Is your application using data (names, addresses, contact and other descriptor/identifier) for individual consumers that are natural persons?	Yes
		c	Do you collect data for energy consumption (demand information and time stamps) for households? Is the data for consumption in some way related to consumers' name, address or other identifiers?	No
		d	In the application, do you create profiles of types of consumers (natural persons)?	No
		e	In the application, do you collect any data for time of use/hours of operation for particular equipment in households or comfort indicators in households (temperature/humidity/lighting)? Is the data in some way related to owners' name, address or other identifiers?	No
2	Profiling: Generation and Storage	a	Do you collect data (names and addresses) from data subjects (natural persons) that are owners of generation/storage facilities?	Yes
		b	In the application, do you collect data for power and energy production/demand from data subjects (natural persons) that are owners of generation/storage facilities? Is the data in some way related to owners' name, address or other identifiers?	No
		c	In the application, do you create profiles of types of generators/storage owned by natural persons?	No

		d	In the application, do you collect any data for time of use/hours of operation for particular generation/storage facility owned by a natural person? Do you collect data on available storage capacity of a storage facility owned by natural person? Is the data in some way related to owners' name, address or other identifiers?	No
3	Profiling: data from natural persons	a	If you collect any data from natural persons in the application, what is the frequency of measurement and transmission of data? Please provide response for all types of data collected.	-
		b	In the application, do you perform remote readings for billing purposes or network planning from natural persons?	No
		c	In the application, do you collect/send any billing data and information on consumers' payment method from/to natural persons?	Yes
		d	Is your application providing online information to consumers/owners of generation or storage facilities that are natural persons? Please describe.	Yes. The users of the platform can create fundraising campaigns for future renewable energy installations. Together with the description of the projects, information about the creator will be provided to the potential investor.
4	Large Scale Data Personal processing	a	Is your application processing <b>personal data</b> on a large scale? (large-scale processing operations which aim to process a considerable amount of <b>personal data</b> at regional, national or supranational level and which could affect a large number of data subjects)	Yes
5	International transfer of personal data	a	In case of international transfer of personal data to a third country, what mechanisms are in place to ensure adequacy of data protection?	Data in Transit are encrypted and only authorized users are capable of accessing the actual information
		b	For your application, do you envisage any contracts with clauses for data transfer from data controllers in EU to data controllers in third countries?	No
6	Smart Grid operations that prevent users from using a service	a	Will the outcome of use of the Smart Grid application lead to preventing consumers from using a service (e.g. disconnection)?	No
		b	In the application, do you perform remote switching of equipment/facilities owned by natural persons? Please explain the purpose of the remote switching.	No
		c	If the use of the Smart Grid application leads to preventing consumers from using a service, do you make a contract with the consumer? Please describe what the contract includes.	-
7	Processing of special categories of personal data	a	In the application, are you processing special categories of data defined in Art. 9 or Art. 10 of the GDPR?	No
8	Applications for which the need to conduct	a	Is the Smart Grid application or system under design listed by the national Data Protection Authority in your country or by the European Data Protection guidelines as one that requires DPIA?	Not explicitly listed

	DPIA is determined by authorities	b	Is the Smart Grid application or system under design listed by the national Data Protection Authority in your country or by the European Data Protection guidelines as one that does not require DPIA?	Not explicitly listed
II	Relevant occurrence			
1	Introducing a new business process (If an existing product is revised or upgraded for the purposes of the project)	a	Are you designing a new business process within the Smart Grid situation or are you making significant changes to an existing Smart Grid situation?	No
		b	Are there new types of information introduced and processed in the new business process?	-
		c	Is the new business process connected to collection and processing of personal data? Description	-
III	Personal Data involved and DPIA-related Processing activities			
1		a	Does the design/change require your application to collect and process any personal data? Explain if it is affirmative.	YES. The users of the platform will be able to create user profiles that contain personal information
		b	Is the purpose or scope of the process/application capable to have an impact on the rights and freedoms of natural persons? Explain if it is affirmative.	No
IV	Status of a Data Controller or a Data Processor			
1		a	Who will have the role of Data Controller and Data Processor for your product/ application during the development and testing/ implementation of the product within the project? (it may be too early to have an explicit answer to this question, but you may have an idea of the possible roles in future)	Too early
		b	Do you plan to define Data Protection (contractual) requirements between you as developer and the possible future Processor/Controller?	-
V	New technologies and other criteria			
1		a	In your application, do you plan to implement new technologies (smart meter environment, cloud processing, Internet of things)?	Yes. A platform will be implemented for funding new projects
		b	Does the design/change of the product/application contain any other criterion that may affect rights and freedoms of natural persons?	No

Table 18: DPIA-PA Questionnaire for Crowdequity Platform

## 8.4 Reflex TNO

Pre-assessment and criteria determining the need to conduct a Data Protection Impact Assessment (DPIA)				
I	Cases foreseen by the GDPR, Data Protection Authorities (DPAs) or the European Data Protection Board			
1	Profiling: Consumers	a	Are you designing a Smart Grid application or system that allows for consumer profiling or another similar activity?	No

		b	Is your application using data (names, addresses, contact and other descriptor/identifier) for individual consumers that are natural persons?	No
		c	Do you collect data for energy consumption (demand information and time stamps) for households? Is the data for consumption in some way related to consumers' name, address or other identifiers?	This is unclear yet and subject to research in this IANOS project: specifically for the hybrid heat pumps in households at Ameland.
		d	In the application, do you create profiles of types of consumers (natural persons)?	No
		e	In the application, do you collect any data for time of use/hours of operation for particular equipment in households or comfort indicators in households (temperature/humidity/lighting)? Is the data in some way related to owners' name, address or other identifiers?	See 1c
2	<b>Profiling: Generation and Storage</b>	a	Do you collect data (names and addresses) from data subjects (natural persons) that are owners of generation/storage facilities?	No
		b	In the application, do you collect data for power and energy production/demand from data subjects (natural persons) that are owners of generation/storage facilities? Is the data in some way related to owners' name, address or other identifiers?	Yes, energy measurements of PV panels installed on roofs of households / In the application these PV panels are registered under a unique ID and from that perspective not related to the owner, furthermore data related to household or natural persons not processed in our application. I.e. our application does not need personal information to function.
		c	In the application, do you create profiles of types of generators/storage owned by natural persons?	No
		d	In the application, do you collect any data for time of use/hours of operation for particular generation/storage facility owned by a natural person? Do you collect data on available storage capacity of a storage facility owned by natural person? Is the data in some way related to owners' name, address or other identifiers?	No storage owned by natural persons are part of the pilot on Ameland.
3	<b>Profiling: data from natural persons</b>	a	If you collect any data from natural persons in the application, what is the frequency of measurement and transmission of data? Please provide response for all types of data collected.	To be determined, and depends on the frequency the devices can give. In principle 5min interval, except for PV panels in the local congestion management use case where higher frequencies are required.

		b	In the application, do you perform remote readings for billing purposes or network planning from natural persons?	No
		c	In the application, do you collect/send any billing data and information on consumers' payment method from/to natural persons?	No
		d	Is your application providing online information to consumers/owners of generation or storage facilities that are natural persons? Please describe.	No
4	Large Scale Data Personal processing	a	Is your application processing <b>personal data</b> on a large scale? (large-scale processing operations which aim to process a considerable amount of <b>personal data</b> at regional, national or supranational level and which could affect a large number of data subjects)	No
5	International transfer of personal data	a	In case of international transfer of personal data to a third country, what mechanisms are in place to ensure adequacy of data protection?	N/A
		b	For your application, do you envisage any contracts with clauses for data transfer from data controllers in EU to data controllers in third countries?	No
6	Smart Grid operations that prevent users from using a service	a	Will the outcome of use of the Smart Grid application lead to preventing consumers from using a service (e.g. disconnection)?	No
		b	In the application, do you perform remote switching of equipment/facilities owned by natural persons? Please explain the purpose of the remote switching.	Yes, optimizing their energy consumption (hybrid heat pumps).
		c	If the use of the Smart Grid application leads to preventing consumers from using a service, do you make a contract with the consumer? Please describe what the contract includes.	It does not restrict customers in using any service. They are still in control.
7	Processing of special categories of personal data	a	In the application, are you processing special categories of data defined in Art. 9 or Art. 10 of the GDPR?	No
8	Applications for which the need to conduct DPIA is determined by authorities	a	Is the Smart Grid application or system under design listed by the national Data Protection Authority in your country or by the European Data Protection guidelines as one that requires DPIA?	No
		b	Is the Smart Grid application or system under design listed by the national Data Protection Authority in your country or by the European Data Protection guidelines as one that does not require DPIA?	No
II	Relevant occurrence			
1	Introducing a new business process (If an existing product is revised or upgraded for the purposes of the project)	a	Are you designing a new business process within the Smart Grid situation or are you making significant changes to an existing Smart Grid situation?	No
		b	Are there new types of information introduced and processed in the new business process?	No
		c	Is the new business process connected to collection and processing of personal data? Description	No

III	Personal Data involved and DPIA-related Processing activities			
1		a	Does the design/change require your application to collect and process any personal data? Explain if it is affirmative.	No
		b	Is the purpose or scope of the process/application capable to have an impact on the rights and freedoms of natural persons? Explain if it is affirmative.	No
IV	Status of a Data Controller or a Data Processor			
1		a	Who will have the role of Data Controller and Data Processor for your product/application during the development and testing/implementation of the product within the project? (it may be too early to have an explicit answer to this question, but you may have an idea of the possible roles in future)	ReFlex will have both roles probably. It requires some information of the devices to function properly and processes that data to create an optimal dispatch of these devices.
		b	Do you plan to define Data Protection (contractual) requirements between you as developer and the possible future Processor/Controller?	Only if commercial steps are made after the project ends.
V	New technologies and other criteria			
1		a	In your application, do you plan to implement new technologies (smart meter environment, cloud processing, Internet of things)?	No
		b	Does the design/change of the product/application contain any other criterion that may affect rights and freedoms of natural persons?	No

Table 19: DPIA-PA Questionnaire for TNO Reflex

## 8.5 System Modeler

Pre-assessment and criteria determining the need to conduct a Data Protection Impact Assessment (DPIA)				
I	Cases foreseen by the GDPR, Data Protection Authorities (DPAs) or the European Data Protection Board			
1	<b>Profiling: Consumers</b>	a	Are you designing a Smart Grid application or system that allows for consumer profiling or another similar activity?	Yes, but in the case of IANOS, no real data is used, but data points taken from publicly available sources or general technical specifications.
		b	Is your application using data (names, addresses, contact and other descriptor/identifier) for individual consumers that are natural persons?	Precise geographic locations of hybrid heat pumps known, IDs of HHPs and manufactures of HHP known. However no identifiers used for the households (no names, addresses stored in our model)

		c	Do you collect data for energy consumption (demand information and time stamps) for households? Is the data for consumption in some way related to consumers' name, address or other identifiers?	Yes, we collect data for energy consumption, but data is based on estimation of available data sources (online) No, we do not have names of households or other identifiers.
		d	In the application, do you create profiles of types of consumers (natural persons)?	Standard NEDU energy demand profiles for different consumer types, but not specific to a household (profiles are generic based on standards for the entire NL)
		e	In the application, do you collect any data for time of use/hours of operation for particular equipment in households or comfort indicators in households (temperature/humidity/lighting)? Is the data in some way related to owners' name, address or other identifiers?	No, this data is not collected
2	Profiling: Generation and Storage	a	Do you collect data (names and addresses) from data subjects (natural persons) that are owners of generation/storage facilities?	No
		b	In the application, do you collect data for power and energy production/demand from data subjects (natural persons) that are owners of generation/storage facilities? Is the data in some way related to owners' name, address or other identifiers?	No
		c	In the application, do you create profiles of types of generators/storage owned by natural persons?	We do not have data on the data production of individual households (use of aggregate data). Use of standard profiles based on technical specifications and weather forecasts (no individual model for production or storage).
		d	In the application, do you collect any data for time of use/hours of operation for particular generation/storage facility owned by a natural person? Do you collect data on available storage capacity of a storage facility owned by natural person? Is the data in some way related to owners' name, address or other identifiers?	No, we use estimations and data provided.
3	Profiling: data from natural persons	a	If you collect any data from natural persons in the application, what is the frequency of measurement and transmission of data? Please provide response for all types of data collected.	We do not collect data.

		b	In the application, do you perform remote readings for billing purposes or network planning from natural persons?	No
		c	In the application, do you collect/send any billing data and information on consumers' payment method from/to natural persons?	No
		d	Is your application providing online information to consumers/owners of generation or storage facilities that are natural persons? Please describe.	No
4	Large Scale Data Personal processing	a	Is your application processing <b>personal data</b> on a large scale? (large-scale processing operations which aim to process a considerable amount of <b>personal data</b> at regional, national or supranational level and which could affect a large number of data subjects)	No
5	International transfer of personal data	a	In case of international transfer of personal data to a third country, what mechanisms are in place to ensure adequacy of data protection?	No international transfer
		b	For your application, do you envisage any contracts with clauses for data transfer from data controllers in EU to data controllers in third countries?	No
6	Smart Grid operations that prevent users from using a service	a	Will the outcome of use of the Smart Grid application lead to preventing consumers from using a service (e.g. disconnection)?	No
		b	In the application, do you perform remote switching of equipment/facilities owned by natural persons? Please explain the purpose of the remote switching.	No
		c	If the use of the Smart Grid application leads to preventing consumers from using a service, do you make a contract with the consumer? Please describe what the contract includes.	No
7	Processing of special categories of personal data	a	In the application, are you processing special categories of data defined in Art. 9 or Art. 10 of the GDPR?	No
8	Applications for which the need to conduct DPIA is determined by authorities	a	Is the Smart Grid application or system under design listed by the national Data Protection Authority in your country or by the European Data Protection guidelines as one that requires DPIA?	No
		b	Is the Smart Grid application or system under design listed by the national Data Protection Authority in your country or by the European Data Protection guidelines as one that does not require DPIA?	NA
II	Relevant occurrence			
1	Introducing a new business process (If an existing product is revised or upgraded for the	a	Are you designing a new business process within the Smart Grid situation or are you making significant changes to an existing Smart Grid situation?	Not from a TNO perspective, but the project will design a 'new' flex valorisation model using REFLEX. But that is under the responsibility of RePowered + AEC
		b	Are there new types of information introduced and processed in the new business process?	-

	<b>purposes of the project)</b>	c	Is the new business process connected to collection and processing of personal data? Description	-
III	<b>Personal Data involved and DPIA-related Processing activities</b>			
1		a	Does the design/change require your application to collect and process any personal data? Explain if it is affirmative.	No
		b	Is the purpose or scope of the process/application capable to have an impact on the rights and freedoms of natural persons? Explain if it is affirmative.	No
IV	<b>Status of a Data Controller or a Data Processor</b>			
1		a	Who will have the role of Data Controller and Data Processor for your product/application during the development and testing/implementation of the product within the project? (it may be too early to have an explicit answer to this question, but you may have an idea of the possible roles in future)	TNO is data controller and does not engage a data processor
		b	Do you plan to define Data Protection (contractual) requirements between you as developer and the possible future Processor/Controller?	No, during the project TNO does not foresee to share or transfer data to another organization either as a processor or controller.
V	<b>New technologies and other criteria</b>			
1		a	In your application, do you plan to implement new technologies (smart meter environment, cloud processing, Internet of things)?	No
		b	Does the design/change of the product/application contain any other criterion that may affect rights and freedoms of natural persons?	No

Table 20: PIA-PA Questionnaire System Modeler

## 8.6 OptiMEMS

Pre-assessment and criteria determining the need to conduct a Data Protection Impact Assessment (DPIA)				
I	Cases foreseen by the GDPR, Data Protection Authorities (DPAs) or the European Data Protection Board			
1	<b>Profiling: Consumers</b>	a	Are you designing a Smart Grid application or system that allows for consumer profiling or another similar activity?	Yes
		b	Is your application using data (names, addresses, contact and other descriptor/identifier) for individual consumers that are natural persons?	Yes, the id of the infrastructure and the asset.
		c	Do you collect data for energy consumption (demand information and time stamps) for households? Is the data for consumption in some way related to consumers' name, address or other identifiers?	Yes, the energy consumption is related to each infrastructure and asset respectively.
		d	In the application, do you create profiles of types of consumers (natural persons)?	No
		e	In the application, do you collect any data for time of use/hours of operation for particular equipment in households or comfort indicators in households (temperature/humidity/lighting)? Is the data in some way related to owners' name, address or other identifiers?	Yes (user preferences) and the data is related to the infrastructure id.

2	Profiling: Generation and Storage	a	Do you collect data (names and addresses) from data subjects (natural persons) that are owners of generation/storage facilities?	No
		b	In the application, do you collect data for power and energy production/demand from data subjects (natural persons) that are owners of generation/storage facilities? Is the data in some way related to owners' name, address or other identifiers?	Yes, the energy generation and storage data is related to each infrastructure and asset individually
		c	In the application, do you create profiles of types of generators/storage owned by natural persons?	No
		d	In the application, do you collect any data for time of use/hours of operation for particular generation/storage facility owned by a natural person? Do you collect data on available storage capacity of a storage facility owned by natural person? Is the data in some way related to owners' name, address or other identifiers?	Yes, the data is related to the infrastructure id.
3	Profiling: data from natural persons	a	If you collect any data from natural persons in the application, what is the frequency of measurement and transmission of data? Please provide response for all types of data collected.	Yes, the data will most likely be obtained with a minutely resolution.
		b	In the application, do you perform remote readings for billing purposes or network planning from natural persons?	No
		c	In the application, do you collect/send any billing data and information on consumers' payment method from/to natural persons?	No
		d	Is your application providing online information to consumers/owners of generation or storage facilities that are natural persons? Please describe.	No
4	Large Scale Data Personal processing	a	Is your application processing <b>personal data</b> on a large scale? (large-scale processing operations which aim to process a considerable amount of <b>personal data</b> at regional, national or supranational level and which could affect a large number of data subjects)	No
5	International transfer of personal data	a	In case of international transfer of personal data to a third country, what mechanisms are in place to ensure adequacy of data protection?	Data in transit are encrypted and only authorized users are capable of accessing the actual information.
		b	For your application, do you envisage any contracts with clauses for data transfer from data controllers in EU to data controllers in third countries?	No
6	Smart Grid operations that prevent users from using a service	a	Will the outcome of use of the Smart Grid application lead to preventing consumers from using a service (e.g. disconnection)?	No
		b	In the application, do you perform remote switching of equipment/facilities owned by natural persons? Please explain the purpose of the remote switching.	No
		c	If the use of the Smart Grid application leads to preventing consumers from using a service, do you make a contract with the consumer? Please describe what the contract includes.	-
7	Processing of special categories of personal data	a	In the application, are you processing special categories of data defined in Art. 9 or Art. 10 of the GDPR?	No

8	Applications for which the need to conduct DPIA is determined by authorities	a	Is the Smart Grid application or system under design listed by the national Data Protection Authority in your country or by the European Data Protection guidelines as one that requires DPIA?	Not explicitly listed
		b	Is the Smart Grid application or system under design listed by the national Data Protection Authority in your country or by the European Data Protection guidelines as one that does not require DPIA?	Not explicitly listed
II	Relevant occurrence			
1	Introducing a new business process (If an existing product is revised or upgraded for the purposes of the project)	a	Are you designing a new business process within the Smart Grid situation or are you making significant changes to an existing Smart Grid situation?	No
		b	Are there new types of information introduced and processed in the new business process?	-
		c	Is the new business process connected to collection and processing of personal data? Description	-
III	Personal Data involved and DPIA-related Processing activities			
1		a	Does the design/change require your application to collect and process any personal data? Explain if it is affirmative.	No
		b	Is the purpose or scope of the process/application capable to have an impact on the rights and freedoms of natural persons? Explain if it is affirmative.	No
IV	Status of a Data Controller or a Data Processor			
1		a	Who will have the role of Data Controller and Data Processor for your product/application during the development and testing/implementation of the product within the project? (it may be too early to have an explicit answer to this question, but you may have an idea of the possible roles in future)	Too early
		b	Do you plan to define Data Protection (contractual) requirements between you as developer and the possible future Processor/Controller?	-
V	New technologies and other criteria			
1		a	In your application, do you plan to implement new technologies (smart meter environment, cloud processing, Internet of things)?	No
		b	Does the design/change of the product/application contain any other criterion that may affect rights and freedoms of natural persons?	No

Table 21: DPIA-PA Questionnaire for OptiMEMS

## 8.7 CleanWatts KIPLO

Pre-assessment and criteria determining the need to conduct a Data Protection Impact Assessment (DPIA)				
I	Cases foreseen by the GDPR, Data Protection Authorities (DPAs) or the European Data Protection Board			
1	<b>Profiling: Consumers</b>	a	Are you designing a Smart Grid application or system that allows for consumer profiling or another similar activity?	Yes

		b	Is your application using data (names, addresses, contact and other descriptor/identifier) for individual consumers that are natural persons?	No
		c	Do you collect data for energy consumption (demand information and time stamps) for households? Is the data for consumption in some way related to consumers' name, address or other identifiers?	Yes
		d	In the application, do you create profiles of types of consumers (natural persons)?	No
		e	In the application, do you collect any data for time of use/hours of operation for particular equipment in households or comfort indicators in households (temperature/humidity/lighting)? Is the data in some way related to owners' name, address or other identifiers?	Yes, but we do not store personal data, just pilot sites ID.
2	Profiling: Generation and Storage	a	Do you collect data (names and addresses) from data subjects (natural persons) that are owners of generation/storage facilities?	Yes
		b	In the application, do you collect data for power and energy production/demand from data subjects (natural persons) that are owners of generation/storage facilities? Is the data in some way related to owners' name, address or other identifiers?	Yes, but we do not store personal data, just pilot sites ID.
		c	In the application, do you create profiles of types of generators/storage owned by natural persons?	No
		d	In the application, do you collect any data for time of use/hours of operation for particular generation/storage facility owned by a natural person? Do you collect data on available storage capacity of a storage facility owned by natural person? Is the data in some way related to owners' name, address or other identifiers?	Yes, but we do not store personal data, just pilot sites ID.
3	Profiling: data from natural persons	a	If you collect any data from natural persons in the application, what is the frequency of measurement and transmission of data? Please provide response for all types of data collected.	Highly dependent on each Use case, but on average, 12 times each day.
		b	In the application, do you perform remote readings for billing purposes or network planning from natural persons?	No
		c	In the application, do you collect/send any billing data and information on consumers' payment method from/to natural persons?	No
		d	Is your application providing online information to consumers/owners of generation or storage facilities that are natural persons? Please describe.	Yes. Dashboards that show their individual consumption and generation.
4	Large Scale Data Personal processing	a	Is your application processing <b>personal data</b> on a large scale? (large-scale processing operations which aim to process a considerable amount of <b>personal data</b> at regional, national or supranational level and which could affect a large number of data subjects)	No
5	International transfer of	a	In case of international transfer of personal data to a third country, what mechanisms are in place to ensure adequacy of data protection?	N/A

	personal data	b	For your application, do you envisage any contracts with clauses for data transfer from data controllers in EU to data controllers in third countries?	N/A
6	Smart Grid operations that prevent users from using a service	a	Will the outcome of use of the Smart Grid application lead to preventing consumers from using a service (e.g. disconnection)?	No
		b	In the application, do you perform remote switching of equipment/facilities owned by natural persons? Please explain the purpose of the remote switching.	Yes. To participate on Energy Markets according or according to each Use Case main objective.
		c	If the use of the Smart Grid application leads to preventing consumers from using a service, do you make a contract with the consumer? Please describe what the contract includes.	Yes
7	Processing of special categories of personal data	a	In the application, are you processing special categories of data defined in Art. 9 or Art. 10 of the GDPR?	No
8	Applications for which the need to conduct DPIA is determined by authorities	a	Is the Smart Grid application or system under design listed by the national Data Protection Authority in your country or by the European Data Protection guidelines as one that requires DPIA?	N/A
		b	Is the Smart Grid application or system under design listed by the national Data Protection Authority in your country or by the European Data Protection guidelines as one that does not require DPIA?	N/A
II	Relevant occurrence			
1	Introducing a new business process (If an existing product is revised or upgraded for the purposes of the project)	a	Are you designing a new business process within the Smart Grid situation or are you making significant changes to an existing Smart Grid situation?	No
		b	Are there new types of information introduced and processed in the new business process?	No
		c	Is the new business process connected to collection and processing of personal data? Description	No
III	Personal Data involved and DPIA-related Processing activities			
1		a	Does the design/change require your application to collect and process any personal data? Explain if it is affirmative.	No
		b	Is the purpose or scope of the process/application capable to have an impact on the rights and freedoms of natural persons? Explain if it is affirmative.	No
IV	Status of a Data Controller or a Data Processor			
1		a	Who will have the role of Data Controller and Data Processor for your product/application during the development and testing/implementation of the product within the project? (it may be too early to have an explicit answer to this question, but you may have an idea of the possible roles in future)	Jorge Landeck
		b	Do you plan to define Data Protection (contractual) requirements between you as developer and the possible future Processor/Controller?	Yes
V	New technologies and other criteria			

1		a	In your application, do you plan to implement new technologies (smart meter environment, cloud processing, Internet of things)?	Yes
		b	Does the design/change of the product/application contain any other criterion that may affect rights and freedoms of natural persons?	No

Table 22: DPIA-PA Questionnaire for KIPLO

## 8.8 Aggregation and Classification Intelligence

Pre-assessment and criteria determining the need to conduct a Data Protection Impact Assessment (DPIA)				
1	Cases foreseen by the GDPR, Data Protection Authorities (DPAs) or the European Data Protection Board			
1	Profiling: Consumers	a	Are you designing a Smart Grid application or system that allows for consumer profiling or another similar activity?	Yes
		b	Is your application using data (names, addresses, contact and other descriptor/identifier) for individual consumers that are natural persons?	Yes, the id of the infrastructure and the asset.
		c	Do you collect data for energy consumption (demand information and time stamps) for households? Is the data for consumption in some way related to consumers' name, address or other identifiers?	Yes, the energy consumption is related to each infrastructure and asset respectively.
		d	In the application, do you create profiles of types of consumers (natural persons)?	No
		e	In the application, do you collect any data for time of use/hours of operation for particular equipment in households or comfort indicators in households (temperature/humidity/lighting)? Is the data in some way related to owners' name, address or other identifiers?	No, only the raw measurements are retrieved.
2	Profiling: Generation and Storage	a	Do you collect data (names and addresses) from data subjects (natural persons) that are owners of generation/storage facilities?	No
		b	In the application, do you collect data for power and energy production/demand from data subjects (natural persons) that are owners of generation/storage facilities? Is the data in some way related to owners' name, address or other identifiers?	Yes, the energy generation is related to each infrastructure and asset individually
		c	In the application, do you create profiles of types of generators/storage owned by natural persons?	No
		d	In the application, do you collect any data for time of use/hours of operation for particular generation/storage facility owned by a natural person? Do you collect data on available storage capacity of a storage facility owned by natural person? Is the data in some way related to owners' name, address or other identifiers?	No
3	Profiling: data from natural persons	a	If you collect any data from natural persons in the application, what is the frequency of measurement and transmission of data? Please provide response for all types of data collected.	Yes, the data will most likely be obtained with a minutely resolution.
		b	In the application, do you perform remote readings for billing purposes or network planning from natural persons?	No
		c	In the application, do you collect/send any billing data and information on consumers' payment method from/to natural persons?	No
		d	Is your application providing online information to consumers/owners of generation or storage facilities that are natural persons? Please describe.	No

4	<b>Large Scale Data Personal processing</b>	a	Is your application processing <b>personal data</b> on a large scale? (large-scale processing operations which aim to process a considerable amount of <b>personal data</b> at regional, national or supranational level and which could affect a large number of data subjects)	No
5	<b>International transfer of personal data</b>	a	In case of international transfer of personal data to a third country, what mechanisms are in place to ensure adequacy of data protection?	Data in transit are encrypted and only authorized users are capable of accessing the actual information.
		b	For your application, do you envisage any contracts with clauses for data transfer from data controllers in EU to data controllers in third countries?	No
6	<b>Smart Grid operations that prevent users from using a service</b>	a	Will the outcome of use of the Smart Grid application lead to preventing consumers from using a service (e.g. disconnection)?	No
		b	In the application, do you perform remote switching of equipment/facilities owned by natural persons? Please explain the purpose of the remote switching.	No
		c	If the use of the Smart Grid application leads to preventing consumers from using a service, do you make a contract with the consumer? Please describe what the contract includes.	-
7	Processing of special categories of personal data	a	In the application, are you processing special categories of data defined in Art. 9 or Art. 10 of the GDPR?	No
8	Applications for which the need to conduct DPIA is determined by authorities	a	Is the Smart Grid application or system under design listed by the national Data Protection Authority in your country or by the European Data Protection guidelines as one that requires DPIA?	Not explicitly listed
		b	Is the Smart Grid application or system under design listed by the national Data Protection Authority in your country or by the European Data Protection guidelines as one that does not require DPIA?	Not explicitly listed
II	<b>Relevant occurrence</b>			
1	<b>Introducing a new business process (If an existing product is revised or upgraded for the purposes of the project)</b>	a	Are you designing a new business process within the Smart Grid situation or are you making significant changes to an existing Smart Grid situation?	No
		b	Are there new types of information introduced and processed in the new business process?	-
		c	Is the new business process connected to collection and processing of personal data? Description	-
III	<b>Personal Data involved and DPIA-related Processing activities</b>			
1		a	Does the design/change require your application to collect and process any personal data? Explain if it is affirmative.	No
		b	Is the purpose or scope of the process/application capable to have an impact on the rights and freedoms of natural persons? Explain if it is affirmative.	No
IV	<b>Status of a Data Controller or a Data Processor</b>			

1		a	Who will have the role of Data Controller and Data Processor for your product/application during the development and testing/implementation of the product within the project? (it may be too early to have an explicit answer to this question, but you may have an idea of the possible roles in future)	Too early
		b	Do you plan to define Data Protection (contractual) requirements between you as developer and the possible future Processor/Controller?	-
V	New technologies and other criteria			
1		a	In your application, do you plan to implement new technologies (smart meter environment, cloud processing, Internet of things)?	No
		b	Does the design/change of the product/application contain any other criterion that may affect rights and freedoms of natural persons?	No

Table 23: DPIA-PA Questionnaire for the Aggregation and Classification Intelligence

## 8.9 Forecasting Engine

Pre-assessment and criteria determining the need to conduct a Data Protection Impact Assessment (DPIA)				
I	Cases foreseen by the GDPR, Data Protection Authorities (DPAs) or the European Data Protection Board			
1	Profiling: Consumers	a	Are you designing a Smart Grid application or system that allows for consumer profiling or another similar activity?	Yes
		b	Is your application using data (names, addresses, contact and other descriptor/identifier) for individual consumers that are natural persons?	Yes, the id of the infrastructure and the asset.
		c	Do you collect data for energy consumption (demand information and time stamps) for households? Is the data for consumption in some way related to consumers' name, address or other identifiers?	Yes, the energy consumption is related to each infrastructure and asset respectively.
		d	In the application, do you create profiles of types of consumers (natural persons)?	No
		e	In the application, do you collect any data for time of use/hours of operation for particular equipment in households or comfort indicators in households (temperature/humidity/lighting)? Is the data in some way related to owners' name, address or other identifiers?	No, only the raw measurements are retrieved.
2	Profiling: Generation and Storage	a	Do you collect data (names and addresses) from data subjects (natural persons) that are owners of generation/storage facilities?	No
		b	In the application, do you collect data for power and energy production/demand from data subjects (natural persons) that are owners of generation/storage facilities? Is the data in some way related to owners' name, address or other identifiers?	Yes, the energy generation is related to each infrastructure and asset individually
		c	In the application, do you create profiles of types of generators/storage owned by natural persons?	No

		d	In the application, do you collect any data for time of use/hours of operation for particular generation/storage facility owned by a natural person? Do you collect data on available storage capacity of a storage facility owned by natural person? Is the data in some way related to owners' name, address or other identifiers?	No
3	Profiling: data from natural persons	a	If you collect any data from natural persons in the application, what is the frequency of measurement and transmission of data? Please provide response for all types of data collected.	Yes, the data will most likely be obtained with a minutely resolution.
		b	In the application, do you perform remote readings for billing purposes or network planning from natural persons?	No
		c	In the application, do you collect/send any billing data and information on consumers' payment method from/to natural persons?	No
		d	Is your application providing online information to consumers/owners of generation or storage facilities that are natural persons? Please describe.	No
4	Large Scale Data Personal processing	a	Is your application processing <b>personal data</b> on a large scale? (large-scale processing operations which aim to process a considerable amount of <b>personal data</b> at regional, national or supranational level and which could affect a large number of data subjects)	No
5	International transfer of personal data	a	In case of international transfer of personal data to a third country, what mechanisms are in place to ensure adequacy of data protection?	Data in transit are encrypted and only authorized users are capable of accessing the actual information.
		b	For your application, do you envisage any contracts with clauses for data transfer from data controllers in EU to data controllers in third countries?	No
6	Smart Grid operations that prevent users from using a service	a	Will the outcome of use of the Smart Grid application lead to preventing consumers from using a service (e.g. disconnection)?	No
		b	In the application, do you perform remote switching of equipment/facilities owned by natural persons? Please explain the purpose of the remote switching.	No
		c	If the use of the Smart Grid application leads to preventing consumers from using a service, do you make a contract with the consumer? Please describe what the contract includes.	-
7	Processing of special categories of personal data	a	In the application, are you processing special categories of data defined in Art. 9 or Art. 10 of the GDPR?	No
8	Applications for which the need to conduct DPIA is determined by authorities	a	Is the Smart Grid application or system under design listed by the national Data Protection Authority in your country or by the European Data Protection guidelines as one that requires DPIA?	Not explicitly listed
		b	Is the Smart Grid application or system under design listed by the national Data Protection Authority in your country or by the European Data Protection guidelines as one that does not require DPIA?	Not explicitly listed

II	Relevant occurrence			
1	Introducing a new business process (If an existing product is revised or upgraded for the purposes of the project)	a	Are you designing a new business process within the Smart Grid situation or are you making significant changes to an existing Smart Grid situation?	No
		b	Are there new types of information introduced and processed in the new business process?	-
		c	Is the new business process connected to collection and processing of personal data? Description	-
III	Personal Data involved and DPIA-related Processing activities			
1		a	Does the design/change require your application to collect and process any personal data? Explain if it is affirmative.	No
		b	Is the purpose or scope of the process/application capable to have an impact on the rights and freedoms of natural persons? Explain if it is affirmative.	No
IV	Status of a Data Controller or a Data Processor			
1		a	Who will have the role of Data Controller and Data Processor for your product/application during the development and testing/implementation of the product within the project? (it may be too early to have an explicit answer to this question, but you may have an idea of the possible roles in future)	Too early
		b	Do you plan to define Data Protection (contractual) requirements between you as developer and the possible future Processor/Controller?	-
V	New technologies and other criteria			
1		a	In your application, do you plan to implement new technologies (smart meter environment, cloud processing, Internet of things)?	No
		b	Does the design/change of the product/application contain any other criterion that may affect rights and freedoms of natural persons?	No

Table 24: DPIA-PA Questionnaire for Forecasting Engine

## 8.10 DLT-based Transactive Platform

Pre-assessment and criteria determining the need to conduct a Data Protection Impact Assessment (DPIA)				
I	Cases foreseen by the GDPR, Data Protection Authorities (DPAs) or the European Data Protection Board			
1	Profiling: Consumers	a	Are you designing a Smart Grid application or system that allows for consumer profiling or another similar activity?	No prosumers are profiled in our application. In our database they are identified with an ID and nothing else.
		b	Is your application using data (names, addresses, contact and other descriptor/identifier) for individual consumers that are natural persons?	No, no names, addresses, contacts or anything else, we use anonymous data.
		c	Do you collect data for energy consumption (demand information and time stamps) for households? Is the data for consumption in some way related to consumers' name, address or other identifiers?	During the testing phase, we only use simulated consumption/production data for each prosumer. In the future in the pilot we will use real data. They contain IDs of the prosumer and are linked to energy measures and

				timestamps.
		d	In the application, do you create profiles of types of consumers (natural persons)?	Users are created in our database. Each user in addition to username and password is linked to an ID (indicating a prosumer) and an ethereum address. Users are created at application deployment and there is no possibility of autonomous registration by a new user.
		e	In the application, do you collect any data for time of use/hours of operation for particular equipment in households or comfort indicators in households (temperature/humidity/lighting)? Is the data in some way related to owners' name, address or other identifiers?	No we only collect aggregated consumption/production data, we do not collect individual equipment data.
2	Profiling: Generation and Storage	a	Do you collect data (names and addresses) from data subjects (natural persons) that are owners of generation/storage facilities?	No, no names, addresses, contacts or anything else, we use anonymous data.
		b	In the application, do you collect data for power and energy production/demand from data subjects (natural persons) that are owners of generation/storage facilities? Is the data in some way related to owners' name, address or other identifiers?	During the testing phase, we only use simulated consumption/production data for each prosumer. In the future in the pilot we will use real data. They contain IDs of the prosumer and are linked to energy measures and timestamps.
		c	In the application, do you create profiles of types of generators/storage owned by natural persons?	No
		d	In the application, do you collect any data for time of use/hours of operation for particular generation/storage facility owned by a natural person? Do you collect data on available storage capacity of a storage facility owned by natural person? Is the data in some way related to owners' name, address or other identifiers?	No we only collect aggregated consumption/production data, we do not collect individual equipment data.
3	Profiling: data from natural persons	a	If you collect any data from natural persons in the application, what is the frequency of measurement and transmission of data? Please provide response for all types of data collected.	We don't know yet, he could be either a natural person or a legal person. We assume we will have an hourly consumption/production data rate.
		b	In the application, do you perform remote readings for billing purposes or network planning from natural persons?	In the pilot we will perform remote readings.
		c	In the application, do you collect/send any billing data and information on consumers' payment method from/to natural persons?	In the pilot we will perform value transactions related to the energy exchanges.
		d	Is your application providing online information to consumers/owners of generation or storage facilities that are natural persons? Please describe.	The application will provide, via dashboard, details on value and energy transactions.

4	Large Scale Data Personal processing	a	Is your application processing <b>personal data</b> on a large scale? (large-scale processing operations which aim to process a considerable amount of <b>personal data</b> at regional, national or supranational level and which could affect a large number of data subjects)	No
5	International transfer of personal data	a	In case of international transfer of personal data to a third country, what mechanisms are in place to ensure adequacy of data protection?	It shouldn't be our case. Data from pilots site will be handled by ENG in Italy.
		b	For your application, do you envisage any contracts with clauses for data transfer from data controllers in EU to data controllers in third countries?	It shouldn't be our case. Data from pilots site will be handled by ENG in Italy.
6	Smart Grid operations that prevent users from using a service	a	Will the outcome of use of the Smart Grid application lead to preventing consumers from using a service (e.g. disconnection)?	No
		b	In the application, do you perform remote switching of equipment/facilities owned by natural persons? Please explain the purpose of the remote switching.	No
		c	If the use of the Smart Grid application leads to preventing consumers from using a service, do you make a contract with the consumer? Please describe what the contract includes.	
7	Processing of special categories of personal data	a	In the application, are you processing special categories of data defined in Art. 9 or Art. 10 of the GDPR?	No
8	Applications for which the need to conduct DPIA is determined by authorities	a	Is the Smart Grid application or system under design listed by the national Data Protection Authority in your country or by the European Data Protection guidelines as one that requires DPIA?	
		b	Is the Smart Grid application or system under design listed by the national Data Protection Authority in your country or by the European Data Protection guidelines as one that does not require DPIA?	
II	Relevant occurrence			
1	Introducing a new business process (If an existing product is revised or upgraded for the purposes of the project)	a	Are you designing a new business process within the Smart Grid situation or are you making significant changes to an existing Smart Grid situation?	It's a new business process.
		b	Are there new types of information introduced and processed in the new business process?	We use power meter readings.
		c	Is the new business process connected to collection and processing of personal data? Description	No.
III	Personal Data involved and DPIA-related Processing activities			
1		a	Does the design/change require your application to collect and process any personal data? Explain if it is affirmative.	No.
		b	Is the purpose or scope of the process/application capable to have an impact on the rights and	No.

			freedoms of natural persons? Explain if it is affirmative.	
IV	Status of a Data Controller or a Data Processor			
1		a	Who will have the role of Data Controller and Data Processor for your product/application during the development and testing/implementation of the product within the project? (it may be too early to have an explicit answer to this question, but you may have an idea of the possible roles in future)	At this moment we are testing with simulated data. We have to decide about for the pilots validations.
		b	Do you plan to define Data Protection (contractual) requirements between you as developer and the possible future Processor/Controller?	Not yet.
V	New technologies and other criteria			
1		a	In your application, do you plan to implement new technologies (smart meter environment, cloud processing, Internet of things)?	No.
		b	Does the design/change of the product/application contain any other criterion that may affect rights and freedoms of natural persons?	No.

Table 25: DPIA-PA Questionnaire for the DLT-based Transactive Platform

## 8.11 Virtual Energy Console

Pre-assessment and criteria determining the need to conduct a Data Protection Impact Assessment (DPIA)				
I	Cases foreseen by the GDPR, Data Protection Authorities (DPAs) or the European Data Protection Board			
1	Profiling: Consumers	a	Are you designing a Smart Grid application or system that allows for consumer profiling or another similar activity?	No
		b	Is your application using data (names, addresses, contact and other descriptor/identifier) for individual consumers that are natural persons?	No
		c	Do you collect data for energy consumption (demand information and time stamps) for households? Is the data for consumption in some way related to consumers' name, address or other identifiers?	No
		d	In the application, do you create profiles of types of consumers (natural persons)?	No
		e	In the application, do you collect any data for time of use/hours of operation for particular equipment in households or comfort indicators in households (temperature/humidity/lighting)? Is the data in some way related to owners' name, address or other identifiers?	No
2	Profiling: Generation and Storage	a	Do you collect data (names and addresses) from data subjects (natural persons) that are owners of generation/storage facilities?	No
		b	In the application, do you collect data for power and energy production/demand from data subjects (natural persons) that are owners of generation/storage facilities? Is the data in some way related to owners' name, address or other identifiers?	No
		c	In the application, do you create profiles of types of generators/storage owned by natural persons?	No
		d	In the application, do you collect any data for time of use/hours of operation for particular generation/storage facility owned by a natural person? Do you collect data on available storage capacity of a storage facility owned by natural person? Is the data in some way related to owners' name, address or other identifiers?	No

3	Profiling: data from natural persons	a	If you collect any data from natural persons in the application, what is the frequency of measurement and transmission of data? Please provide response for all types of data collected.	No
		b	In the application, do you perform remote readings for billing purposes or network planning from natural persons?	No
		c	In the application, do you collect/send any billing data and information on consumers' payment method from/to natural persons?	No
		d	Is your application providing online information to consumers/owners of generation or storage facilities that are natural persons? Please describe.	No
4	Large Scale Data Personal processing	a	Is your application processing <b>personal data</b> on a large scale? (large-scale processing operations which aim to process a considerable amount of <b>personal data</b> at regional, national or supranational level and which could affect a large number of data subjects)	No
5	International transfer of personal data	a	In case of international transfer of personal data to a third country, what mechanisms are in place to ensure adequacy of data protection?	N/A
		b	For your application, do you envisage any contracts with clauses for data transfer from data controllers in EU to data controllers in third countries?	N/A
6	Smart Grid operations that prevent users from using a service	a	Will the outcome of use of the Smart Grid application lead to preventing consumers from using a service (e.g. disconnection)?	N/A
		b	In the application, do you perform remote switching of equipment/facilities owned by natural persons? Please explain the purpose of the remote switching.	N/A
		c	If the use of the Smart Grid application leads to preventing consumers from using a service, do you make a contract with the consumer? Please describe what the contract includes.	N/A
7	Processing of special categories of personal data	a	In the application, are you processing special categories of data defined in Art. 9 or Art. 10 of the GDPR?	No
8	Applications for which the need to conduct DPIA is determined by authorities	a	Is the Smart Grid application or system under design listed by the national Data Protection Authority in your country or by the European Data Protection guidelines as one that requires DPIA?	N/A
		b	Is the Smart Grid application or system under design listed by the national Data Protection Authority in your country or by the European Data Protection guidelines as one that does not require DPIA?	N/A
II	Relevant occurrence			
1	Introducing a new business process (If an existing product is revised or upgraded for the purposes of the project)	a	Are you designing a new business process within the Smart Grid situation or are you making significant changes to an existing Smart Grid situation?	No
		b	Are there new types of information introduced and processed in the new business process?	N/A
		c	Is the new business process connected to collection and processing of personal data? Description	N/A
III	Personal Data involved and DPIA-related Processing activities			
1		a	Does the design/change require your application to collect and process any personal data? Explain if it is affirmative.	No
		b	Is the purpose or scope of the process/application capable to have an impact on the rights and freedoms of natural persons? Explain if it is affirmative.	No
IV	Status of a Data Controller or a Data Processor			

1		a	Who will have the role of Data Controller and Data Processor for your product/application during the development and testing/implementation of the product within the project? (it may be too early to have an explicit answer to this question, but you may have an idea of the possible roles in future)	Jorge Landeck
		b	Do you plan to define Data Protection (contractual) requirements between you as developer and the possible future Processor/Controller?	Yes
V	New technologies and other criteria			
1		a	In your application, do you plan to implement new technologies (smart meter environment, cloud processing, Internet of things)?	Yes
		b	Does the design/change of the product/application contain any other criterion that may affect rights and freedoms of natural persons?	No

Table 26: DPIA-PA Questionnaire for Virtual Energy Console

## 8.12 Enterprise Service Bus

Pre-assessment and criteria determining the need to conduct a Data Protection Impact Assessment (DPIA)				
I	Cases foreseen by the GDPR, Data Protection Authorities (DPAs) or the European Data Protection Board			
1	Profiling: Consumers	a	Are you designing a Smart Grid application or system that allows for consumer profiling or another similar activity?	No
		b	Is your application using data (names, addresses, contact and other descriptor/identifier) for individual consumers that are natural persons?	No
		c	Do you collect data for energy consumption (demand information and time stamps) for households? Is the data for consumption in some way related to consumers' name, address or other identifiers?	No
		d	In the application, do you create profiles of types of consumers (natural persons)?	No
		e	In the application, do you collect any data for time of use/hours of operation for particular equipment in households or comfort indicators in households (temperature/humidity/lighting)? Is the data in some way related to owners' name, address or other identifiers?	No
2	Profiling: Generation and Storage	a	Do you collect data (names and addresses) from data subjects (natural persons) that are owners of generation/storage facilities?	No
		b	In the application, do you collect data for power and energy production/demand from data subjects (natural persons) that are owners of generation/storage facilities? Is the data in some way related to owners' name, address or other identifiers?	No
		c	In the application, do you create profiles of types of generators/storage owned by natural persons?	No
		d	In the application, do you collect any data for time of use/hours of operation for particular generation/storage facility owned by a natural person? Do you collect data on available storage capacity of a storage facility owned by natural person? Is the data in some way related to owners' name, address or other identifiers?	No
3	Profiling: data from natural persons	a	If you collect any data from natural persons in the application, what is the frequency of measurement and transmission of data? Please provide response for all types of data collected.	No
		b	In the application, do you perform remote readings for billing purposes or network planning from natural persons?	No

		c	In the application, do you collect/send any billing data and information on consumers' payment method from/to natural persons?	No
		d	Is your application providing online information to consumers/owners of generation or storage facilities that are natural persons? Please describe.	No
4	Large Scale Data Personal processing	a	Is your application processing <b>personal data</b> on a large scale? (large-scale processing operations which aim to process a considerable amount of <b>personal data</b> at regional, national or supranational level and which could affect a large number of data subjects)	No
5	International transfer of personal data	a	In case of international transfer of personal data to a third country, what mechanisms are in place to ensure adequacy of data protection?	N/A
		b	For your application, do you envisage any contracts with clauses for data transfer from data controllers in EU to data controllers in third countries?	N/A
6	Smart Grid operations that prevent users from using a service	a	Will the outcome of use of the Smart Grid application lead to preventing consumers from using a service (e.g. disconnection)?	N/A
		b	In the application, do you perform remote switching of equipment/facilities owned by natural persons? Please explain the purpose of the remote switching.	No
		c	If the use of the Smart Grid application leads to preventing consumers from using a service, do you make a contract with the consumer? Please describe what the contract includes.	N/A
7	Processing of special categories of personal data	a	In the application, are you processing special categories of data defined in Art. 9 or Art. 10 of the GDPR?	No
8	Applications for which the need to conduct DPIA is determined by authorities	a	Is the Smart Grid application or system under design listed by the national Data Protection Authority in your country or by the European Data Protection guidelines as one that requires DPIA?	No
		b	Is the Smart Grid application or system under design listed by the national Data Protection Authority in your country or by the European Data Protection guidelines as one that does not require DPIA?	N/A
II	Relevant occurrence			
1	Introducing a new business process (If an existing product is revised or upgraded for the purposes of the project)	a	Are you designing a new business process within the Smart Grid situation or are you making significant changes to an existing Smart Grid situation?	No
		b	Are there new types of information introduced and processed in the new business process?	No
		c	Is the new business process connected to collection and processing of personal data? Description	No
III	Personal Data involved and DPIA-related Processing activities			
1		a	Does the design/change require your application to collect and process any personal data? Explain if it is affirmative.	No
		b	Is the purpose or scope of the process/application capable to have an impact on the rights and freedoms of natural persons? Explain if it is affirmative.	No
IV	Status of a Data Controller or a Data Processor			

1		a	Who will have the role of Data Controller and Data Processor for your product/application during the development and testing/implementation of the product within the project? (it may be too early to have an explicit answer to this question, but you may have an idea of the possible roles in future)	Not considered
		b	Do you plan to define Data Protection (contractual) requirements between you as developer and the possible future Processor/Controller?	Yes
V	New technologies and other criteria			
1		a	In your application, do you plan to implement new technologies (smart meter environment, cloud processing, Internet of things)?	No
		b	Does the design/change of the product/application contain any other criterion that may affect rights and freedoms of natural persons?	No

Table 27: DPIA-PA Questionnaire for Enterprise Service Bus

## 8.13 Non-intrusive characterization of energy flexibility in water heating systems

Pre-assessment and criteria determining the need to conduct a Data Protection Impact Assessment (DPIA)				
I	Cases foreseen by the GDPR, Data Protection Authorities (DPAs) or the European Data Protection Board			
1	<b>Profiling: Consumers</b>	a	Are you designing a Smart Grid application or system that allows for consumer profiling or another similar activity?	Yes, hot water consumption profile is collected by this solution.
		b	Is your application using data (names, addresses, contact and other descriptor/identifier) for individual consumers that are natural persons?	No
		c	Do you collect data for energy consumption (demand information and time stamps) for households? Is the data for consumption in some way related to consumers' name, address or other identifiers?	No, this solution does not collect the overall energy consumption.
		d	In the application, do you create profiles of types of consumers (natural persons)?	No
		e	In the application, do you collect any data for time of use/hours of operation for particular equipment in households or comfort indicators in households (temperature/humidity/lighting)? Is the data in some way related to owners' name, address or other identifiers?	Hot water consumption profile is collected by this solution. No, collected data is not related to owners' name, address or other identifiers.
2	<b>Profiling: Generation and Storage</b>	a	Do you collect data (names and addresses) from data subjects (natural persons) that are owners of generation/storage facilities?	This is solutions is not related with electric energy generation and storage.
		b	In the application, do you collect data for power and energy production/demand from data subjects (natural persons) that are owners of generation/storage facilities? Is the data in some way related to owners' name, address or other identifiers?	This is solutions is not related with electric energy generation and storage.
		c	In the application, do you create profiles of types of generators/storage owned by natural persons?	This is solutions is not related with electric energy generation and storage.
		d	In the application, do you collect any data for time of use/hours of operation for particular generation/storage facility owned by a natural person?	This is solutions is not related with electric energy generation and storage.

			Do you collect data on available storage capacity of a storage facility owned by natural person? Is the data in some way related to owners' name, address or other identifiers?	
3	Profiling: data from natural persons	a	If you collect any data from natural persons in the application, what is the frequency of measurement and transmission of data? Please provide response for all types of data collected.	Hot water consumption profiles are collected with 1-min resolution.
		b	In the application, do you perform remote readings for billing purposes or network planning from natural persons?	No
		c	In the application, do you collect/send any billing data and information on consumers' payment method from/to natural persons?	No
		d	Is your application providing online information to consumers/owners of generation or storage facilities that are natural persons? Please describe.	No.
4	Large Scale Data Personal processing	a	Is your application processing <b>personal data</b> on a large scale? (large-scale processing operations which aim to process a considerable amount of <b>personal data</b> at regional, national or supranational level and which could affect a large number of data subjects)	No
5	International transfer of personal data	a	In case of international transfer of personal data to a third country, what mechanisms are in place to ensure adequacy of data protection?	This is not foreseen
		b	For your application, do you envisage any contracts with clauses for data transfer from data controllers in EU to data controllers in third countries?	This is not foreseen
6	Smart Grid operations that prevent users from using a service	a	Will the outcome of use of the Smart Grid application lead to preventing consumers from using a service (e.g. disconnection)?	No
		b	In the application, do you perform remote switching of equipment/facilities owned by natural persons? Please explain the purpose of the remote switching.	Yes, this solution controls the supply of electric energy to water heaters to achieve specific objectives (e.g., reduce costs to citizens) always ensuring the minimum and maximum water temperature limits.
		c	If the use of the Smart Grid application leads to preventing consumers from using a service, do you make a contract with the consumer? Please describe what the contract includes.	Consumers are not prevented from using the electric water heaters.
7	Processing of special categories of personal data	a	In the application, are you processing special categories of data defined in Art. 9 or Art. 10 of the GDPR?	No
8	Applications for which the need to conduct DPIA is determined by authorities	a	Is the Smart Grid application or system under design listed by the national Data Protection Authority in your country or by the European Data Protection guidelines as one that requires DPIA?	No
		b	Is the Smart Grid application or system under design listed by the national Data Protection Authority in your country or by the European Data Protection guidelines as one that does not require DPIA?	No
II	Relevant occurrence			
1	Introducing a new business	a	Are you designing a new business process within the Smart Grid situation or are you making significant changes to an existing Smart Grid situation?	No

	process (If an existing product is revised or upgraded for the purposes of the project)	b	Are there new types of information introduced and processed in the new business process?	-
		c	Is the new business process connected to collection and processing of personal data? Description	-
III	Personal Data involved and DPIA-related Processing activities			
1		a	Does the design/change require your application to collect and process any personal data? Explain if it is affirmative.	No
		b	Is the purpose or scope of the process/application capable to have an impact on the rights and freedoms of natural persons? Explain if it is affirmative.	No
IV	Status of a Data Controller or a Data Processor			
1		a	Who will have the role of Data Controller and Data Processor for your product/application during the development and testing/implementation of the product within the project? (it may be too early to have an explicit answer to this question, but you may have an idea of the possible roles in future)	See data management structure.
		b	Do you plan to define Data Protection (contractual) requirements between you as developer and the possible future Processor/Controller?	-
V	New technologies and other criteria			
1		a	In your application, do you plan to implement new technologies (smart meter environment, cloud processing, Internet of things)?	No
		b	Does the design/change of the product/application contain any other criterion that may affect rights and freedoms of natural persons?	No

Table 28: DPIA-PA Questionnaire for Non-Intrusive characterization of energy flexibility in water heating systems

## 8.14 FEID-PLUS

Pre-assessment and criteria determining the need to conduct a Data Protection Impact Assessment (DPIA)				
I	Cases foreseen by the GDPR, Data Protection Authorities (DPAs) or the European Data Protection Board			
1	Profiling: Consumers	a	Are you designing a Smart Grid application or system that allows for consumer profiling or another similar activity?	Yes
		b	Is your application using data (names, addresses, contact and other descriptor/identifier) for individual consumers that are natural persons?	Yes, the id of the infrastructure and the asset.
		c	Do you collect data for energy consumption (demand information and time stamps) for households? Is the data for consumption in some way related to consumers' name, address or other identifiers?	Yes, the energy consumption is related to each infrastructure and asset respectively.
		d	In the application, do you create profiles of types of consumers (natural persons)?	No

		e	In the application, do you collect any data for time of use/hours of operation for particular equipment in households or comfort indicators in households (temperature/humidity/lighting)? Is the data in some way related to owners' name, address or other identifiers?	No, only the raw measurements are retrieved.
2	Profiling: Generation and Storage	a	Do you collect data (names and addresses) from data subjects (natural persons) that are owners of generation/storage facilities?	No
		b	In the application, do you collect data for power and energy production/demand from data subjects (natural persons) that are owners of generation/storage facilities? Is the data in some way related to owners' name, address or other identifiers?	Yes, the energy generation is related to each infrastructure and asset individually
		c	In the application, do you create profiles of types of generators/storage owned by natural persons?	No
		d	In the application, do you collect any data for time of use/hours of operation for particular generation/storage facility owned by a natural person? Do you collect data on available storage capacity of a storage facility owned by natural person? Is the data in some way related to owners' name, address or other identifiers?	No
3	Profiling: data from natural persons	a	If you collect any data from natural persons in the application, what is the frequency of measurement and transmission of data? Please provide response for all types of data collected.	Yes, the data will most likely be obtained with a minutely resolution.
		b	In the application, do you perform remote readings for billing purposes or network planning from natural persons?	No
		c	In the application, do you collect/send any billing data and information on consumers' payment method from/to natural persons?	No
		d	Is your application providing online information to consumers/owners of generation or storage facilities that are natural persons? Please describe.	No
4	Large Scale Data Personal processing	a	Is your application processing <b>personal data</b> on a large scale? (large-scale processing operations which aim to process a considerable amount of <b>personal data</b> at regional, national or supranational level and which could affect a large number of data subjects)	No
5	International transfer of personal data	a	In case of international transfer of personal data to a third country, what mechanisms are in place to ensure adequacy of data protection?	Data in transit are encrypted and only authorized users are capable of accessing the actual information.
		b	For your application, do you envisage any contracts with clauses for data transfer from data controllers in EU to data controllers in third countries?	No
6	Smart Grid operations that prevent users from using a service	a	Will the outcome of use of the Smart Grid application lead to preventing consumers from using a service (e.g. disconnection)?	No
		b	In the application, do you perform remote switching of equipment/facilities owned by natural persons? Please explain the purpose of the remote switching.	No
		c	If the use of the Smart Grid application leads to preventing consumers from using a service, do you make a contract with the consumer? Please describe what the contract includes.	-

7	Processing of special categories of personal data	a	In the application, are you processing special categories of data defined in Art. 9 or Art. 10 of the GDPR?	No
8	Applications for which the need to conduct DPIA is determined by authorities	a	Is the Smart Grid application or system under design listed by the national Data Protection Authority in your country or by the European Data Protection guidelines as one that requires DPIA?	Not explicitly listed
		b	Is the Smart Grid application or system under design listed by the national Data Protection Authority in your country or by the European Data Protection guidelines as one that does not require DPIA?	Not explicitly listed
II	Relevant occurrence			
1	Introducing a new business process (If an existing product is revised or upgraded for the purposes of the project)	a	Are you designing a new business process within the Smart Grid situation or are you making significant changes to an existing Smart Grid situation?	No
		b	Are there new types of information introduced and processed in the new business process?	-
		c	Is the new business process connected to collection and processing of personal data? Description	-
III	Personal Data involved and DPIA-related Processing activities			
1		a	Does the design/change require your application to collect and process any personal data? Explain if it is affirmative.	No
		b	Is the purpose or scope of the process/application capable to have an impact on the rights and freedoms of natural persons? Explain if it is affirmative.	No
IV	Status of a Data Controller or a Data Processor			
1		a	Who will have the role of Data Controller and Data Processor for your product/application during the development and testing/implementation of the product within the project? (it may be too early to have an explicit answer to this question, but you may have an idea of the possible roles in future)	Too early
		b	Do you plan to define Data Protection (contractual) requirements between you as developer and the possible future Processor/Controller?	-
V	New technologies and other criteria			
1		a	In your application, do you plan to implement new technologies (smart meter environment, cloud processing, Internet of things)?	Yes, communication with smart meters.
		b	Does the design/change of the product/application contain any other criterion that may affect rights and freedoms of natural persons?	No

Table 29: DPIA-PA Questionnaire for FEID-Plus

## 8.15 Smart Energy Router

Pre-assessment and criteria determining the need to conduct a Data Protection Impact Assessment (DPIA)

I Cases foreseen by the GDPR, Data Protection Authorities (DPAs) or the European Data Protection Board				
1	Profiling: Consumers	a	Are you designing a Smart Grid application or system that allows for consumer profiling or another similar activity?	No, the overall consumption is not measured by the energy router
		b	Is your application using data (names, addresses, contact and other descriptor/identifier) for individual consumers that are natural persons?	No
		c	Do you collect data for energy consumption (demand information and time stamps) for households? Is the data for consumption in some way related to consumers' name, address or other identifiers?	No, the energy router does not collect the overall consumption
		d	In the application, do you create profiles of types of consumers (natural persons)?	No
		e	In the application, do you collect any data for time of use/hours of operation for particular equipment in households or comfort indicators in households (temperature/humidity/lighting)? Is the data in some way related to owners' name, address or other identifiers?	No, the only equipments that are monitored are the PV panels and the batteries.
2	Profiling: Generation and Storage	a	Do you collect data (names and addresses) from data subjects (natural persons) that are owners of generation/storage facilities?	Yes.
		b	In the application, do you collect data for power and energy production/demand from data subjects (natural persons) that are owners of generation/storage facilities? Is the data in some way related to owners' name, address or other identifiers?	Yes.
		c	In the application, do you create profiles of types of generators/storage owned by natural persons?	The energy router does not create profiles. It is a power electronics device that manages the energy flow, according to higher level instructions.
		d	In the application, do you collect any data for time of use/hours of operation for particular generation/storage facility owned by a natural person? Do you collect data on available storage capacity of a storage facility owned by natural person? Is the data in some way related to owners' name, address or other identifiers?	Yes.
3	Profiling: data from natural persons	a	If you collect any data from natural persons in the application, what is the frequency of measurement and transmission of data? Please provide response for all types of data collected.	PV production and energy storage are collected with 1-min resolution.
		b	In the application, do you perform remote readings for billing purposes or network planning from natural persons?	No
		c	In the application, do you collect/send any billing data and information on consumers' payment method from/to natural persons?	No
		d	Is your application providing online information to consumers/owners of generation or storage facilities that are natural persons? Please describe.	Yes. PV and batteries owners are informed of the PV production and energy storage.
4	Large Scale Data Personal processing	a	Is your application processing <b>personal data</b> on a large scale? (large-scale processing operations which aim to process a considerable amount of <b>personal data</b> at regional, national or supranational level and which could affect a large number of data subjects)	No

5	<b>International transfer of personal data</b>	a	In case of international transfer of personal data to a third country, what mechanisms are in place to ensure adequacy of data protection?	This is not foreseen
		b	For your application, do you envisage any contracts with clauses for data transfer from data controllers in EU to data controllers in third countries?	This is not foreseen
6	<b>Smart Grid operations that prevent users from using a service</b>	a	Will the outcome of use of the Smart Grid application lead to preventing consumers from using a service (e.g. disconnection)?	No
		b	In the application, do you perform remote switching of equipment/facilities owned by natural persons? Please explain the purpose of the remote switching.	No
		c	If the use of the Smart Grid application leads to preventing consumers from using a service, do you make a contract with the consumer? Please describe what the contract includes.	No
7	Processing of special categories of personal data	a	In the application, are you processing special categories of data defined in Art. 9 or Art. 10 of the GDPR?	No
8	Applications for which the need to conduct DPIA is determined by authorities	a	Is the Smart Grid application or system under design listed by the national Data Protection Authority in your country or by the European Data Protection guidelines as one that requires DPIA?	No
		b	Is the Smart Grid application or system under design listed by the national Data Protection Authority in your country or by the European Data Protection guidelines as one that does not require DPIA?	No
II	Relevant occurrence			
1	Introducing a new business process (If an existing product is revised or upgraded for the purposes of the project)	a	Are you designing a new business process within the Smart Grid situation or are you making significant changes to an existing Smart Grid situation?	No
		b	Are there new types of information introduced and processed in the new business process?	-
		c	Is the new business process connected to collection and processing of personal data? Description	-
III	Personal Data involved and DPIA-related Processing activities			
1		a	Does the design/change require your application to collect and process any personal data? Explain if it is affirmative.	-
		b	Is the purpose or scope of the process/application capable to have an impact on the rights and freedoms of natural persons? Explain if it is affirmative.	-
IV	Status of a Data Controller or a Data Processor			
1		a	Who will have the role of Data Controller and Data Processor for your product/application during the development and testing/implementation of the product within the project?(it may be too early to have an explicit answer to this question, but you may have an idea of the possible roles in future)	See data management structure.
		b	Do you plan to define Data Protection (contractual) requirements between you as developer and the possible future Processor/Controller?	-

V	New technologies and other criteria			
1		a	In your application, do you plan to implement new technologies (smart meter environment, cloud processing, Internet of things)?	No
		b	Does the design/change of the product/application contain any other criterion that may affect rights and freedoms of natural persons?	No

Table 30: DPIA-PA Questionnaire for Smart Energy Router

## 8.16 Hybrid Transformer

Pre-assessment and criteria determining the need to conduct a Data Protection Impact Assessment (DPIA)				
I Cases foreseen by the GDPR, Data Protection Authorities (DPAs) or the European Data Protection Board				
1	Profiling: Consumers	a	Are you designing a Smart Grid application or system that allows for consumer profiling or another similar activity?	No
		b	Is your application using data (names, addresses, contact and other descriptor/identifier) for individual consumers that are natural persons?	No
		c	Do you collect data for energy consumption (demand information and time stamps) for households? Is the data for consumption in some way related to consumers' name, address or other identifiers?	No
		d	In the application, do you create profiles of types of consumers (natural persons)?	No
		e	In the application, do you collect any data for time of use/hours of operation for particular equipment in households or comfort indicators in households (temperature/humidity/lighting)? Is the data in some way related to owners' name, address or other identifiers?	No
2	Profiling: Generation and Storage	a	Do you collect data (names and addresses) from data subjects (natural persons) that are owners of generation/storage facilities?	No
		b	In the application, do you collect data for power and energy production/demand from data subjects (natural persons) that are owners of generation/storage facilities? Is the data in some way related to owners' name, address or other identifiers?	No
		c	In the application, do you create profiles of types of generators/storage owned by natural persons?	No
		d	In the application, do you collect any data for time of use/hours of operation for particular generation/storage facility owned by a natural person? Do you collect data on available storage capacity of a storage facility owned by natural person? Is the data in some way related to owners' name, address or other identifiers?	No. No. No.
3	Profiling: data from natural persons	a	If you collect any data from natural persons in the application, what is the frequency of measurement and transmission of data? Please provide response for all types of data collected.	No.
		b	In the application, do you perform remote readings for billing purposes or network planning from natural persons?	No.
		c	In the application, do you collect/send any billing data and information on consumers' payment method from/to natural persons?	No.
		d	Is your application providing online information to consumers/owners of generation or storage facilities that are natural persons? Please describe.	No.

4	Large Scale Data Personal processing	a	Is your application processing <b>personal data</b> on a large scale? (large-scale processing operations which aim to process a considerable amount of <b>personal data</b> at regional, national or supranational level and which could affect a large number of data subjects)	No.
5	International transfer of personal data	a	In case of international transfer of personal data to a third country, what mechanisms are in place to ensure adequacy of data protection?	N.A.
		b	For your application, do you envisage any contracts with clauses for data transfer from data controllers in EU to data controllers in third countries?	N.A.
6	Smart Grid operations that prevent users from using a service	a	Will the outcome of use of the Smart Grid application lead to preventing consumers from using a service (e.g. disconnection)?	No.
		b	In the application, do you perform remote switching of equipment/facilities owned by natural persons? Please explain the purpose of the remote switching.	No.
		c	If the use of the Smart Grid application leads to preventing consumers from using a service, do you make a contract with the consumer? Please describe what the contract includes.	N.A.
7	Processing of special categories of personal data	a	In the application, are you processing special categories of data defined in Art. 9 or Art. 10 of the GDPR?	No
8	Applications for which the need to conduct DPIA is determined by authorities	a	Is the Smart Grid application or system under design listed by the national Data Protection Authority in your country or by the European Data Protection guidelines as one that requires DPIA?	No
		b	Is the Smart Grid application or system under design listed by the national Data Protection Authority in your country or by the European Data Protection guidelines as one that does not require DPIA?	No
II	Relevant occurrence			
1	Introducing a new business process (If an existing product is revised or upgraded for the purposes of the project)	a	Are you designing a new business process within the Smart Grid situation or are you making significant changes to an existing Smart Grid situation?	No
		b	Are there new types of information introduced and processed in the new business process?	N.A.
		c	Is the new business process connected to collection and processing of personal data? Description	N.A.
III	Personal Data involved and DPIA-related Processing activities			
1		a	Does the design/change require your application to collect and process any personal data? Explain if it is affirmative.	No
		b	Is the purpose or scope of the process/application capable to have an impact on the rights and freedoms of natural persons? Explain if it is affirmative.	No
IV	Status of a Data Controller or a Data Processor			
1		a	Who will have the role of Data Controller and Data Processor for your product/application during the development and testing/implementation of the product within the project? (it may be too early to have an explicit answer to this question, but you may have an idea of the possible roles in future)	

		b	Do you plan to define Data Protection (contractual) requirements between you as developer and the possible future Processor/Controller?	N.A.
V	New technologies and other criteria			
1		a	In your application, do you plan to implement new technologies (smart meter environment, cloud processing, Internet of things)?	Yes
		b	Does the design/change of the product/application contain any other criterion that may affect rights and freedoms of natural persons?	No

Table 31: DPIA-PA Questionnaire for Hybrid Transformer

## 8.17 V2G Charging

Pre-assessment and criteria determining the need to conduct a Data Protection Impact Assessment (DPIA)				
I	Cases foreseen by the GDPR, Data Protection Authorities (DPAs) or the European Data Protection Board			
1	Profiling: Consumers	a	Are you designing a Smart Grid application or system that allows for consumer profiling or another similar activity?	No.
		b	Is your application using data (names, addresses, contact and other descriptor/identifier) for individual consumers that are natural persons?	No.
		c	Do you collect data for energy consumption (demand information and time stamps) for households? Is the data for consumption in some way related to consumers' name, address or other identifiers?	No.
		d	In the application, do you create profiles of types of consumers (natural persons)?	No.
		e	In the application, do you collect any data for time of use/hours of operation for particular equipment in households or comfort indicators in households (temperature/humidity/lighting)? Is the data in some way related to owners' name, address or other identifiers?	No.
2	Profiling: Generation and Storage	a	Do you collect data (names and addresses) from data subjects (natural persons) that are owners of generation/storage facilities?	No.
		b	In the application, do you collect data for power and energy production/demand from data subjects (natural persons) that are owners of generation/storage facilities? Is the data in some way related to owners' name, address or other identifiers?	No.
		c	In the application, do you create profiles of types of generators/storage owned by natural persons?	No.
		d	In the application, do you collect any data for time of use/hours of operation for particular generation/storage facility owned by a natural person? Do you collect data on available storage capacity of a storage facility owned by natural person? Is the data in some way related to owners' name, address or other identifiers?	No.
3	Profiling: data from natural persons	a	If you collect any data from natural persons in the application, what is the frequency of measurement and transmission of data? Please provide response for all types of data collected.	No.
		b	In the application, do you perform remote readings for billing purposes or network planning from natural persons?	No.
		c	In the application, do you collect/send any billing data and information on consumers' payment method from/to natural persons?	No.
		d	Is your application providing online information to consumers/owners of generation or storage facilities that are natural persons? Please describe.	No.

4	<b>Large Scale Data Personal processing</b>	a	Is your application processing <b>personal data</b> on a large scale? (large-scale processing operations which aim to process a considerable amount of <b>personal data</b> at regional, national or supranational level and which could affect a large number of data subjects)	No.
5	<b>International transfer of personal data</b>	a	In case of international transfer of personal data to a third country, what mechanisms are in place to ensure adequacy of data protection?	No.
		b	For your application, do you envisage any contracts with clauses for data transfer from data controllers in EU to data controllers in third countries?	No.
6	<b>Smart Grid operations that prevent users from using a service</b>	a	Will the outcome of use of the Smart Grid application lead to preventing consumers from using a service (e.g. disconnection)?	No.
		b	In the application, do you perform remote switching of equipment/facilities owned by natural persons? Please explain the purpose of the remote switching.	No.
		c	If the use of the Smart Grid application leads to preventing consumers from using a service, do you make a contract with the consumer? Please describe what the contract includes.	No.
7	<b>Processing of special categories of personal data</b>	a	In the application, are you processing special categories of data defined in Art. 9 or Art. 10 of the GDPR?	No
8	<b>Applications for which the need to conduct DPIA is determined by authorities</b>	a	Is the Smart Grid application or system under design listed by the national Data Protection Authority in your country or by the European Data Protection guidelines as one that requires DPIA?	No
		b	Is the Smart Grid application or system under design listed by the national Data Protection Authority in your country or by the European Data Protection guidelines as one that does not require DPIA?	No
II	<b>Relevant occurrence</b>			
1	<b>Introducing a new business process (If an existing product is revised or upgraded for the purposes of the project)</b>	a	Are you designing a new business process within the Smart Grid situation or are you making significant changes to an existing Smart Grid situation?	No
		b	Are there new types of information introduced and processed in the new business process?	No
		c	Is the new business process connected to collection and processing of personal data? Description	No
III	<b>Personal Data involved and DPIA-related Processing activities</b>			
1		a	Does the design/change require your application to collect and process any personal data? Explain if it is affirmative.	No.
		b	Is the purpose or scope of the process/application capable to have an impact on the rights and freedoms of natural persons? Explain if it is affirmative.	No.
IV	<b>Status of a Data Controller or a Data Processor</b>			
1		a	Who will have the role of Data Controller and Data Processor for your product/application during the development and testing/implementation of the product within the project? (it may be too early to have an explicit answer to this question, but you may have an idea of the possible roles in future)	This role will be defined in the next weeks, aligned with the Efacec corporate directives

		b	Do you plan to define Data Protection (contractual) requirements between you as developer and the possible future Processor/Controller?	No
V	New technologies and other criteria			
1		a	In your application, do you plan to implement new technologies (smart meter environment, cloud processing, Internet of things)?	No.
		b	Does the design/change of the product/application contain any other criterion that may affect rights and freedoms of natural persons?	No.

*Table 32: DPIA-PA Questionnaire for V2G charger*