IANOS

SUSTAINABLE SOLUTIONS
for islands' decarbonisation

Ethics and Cyber Security Management report v2

Authors: Denisa Ziu (ENG), Vincenzo Croce (ENG)

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

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

DOCUMENT DETAILS

Deliverable No	D1.11
Dissemination level	Public
Work Package	WP1 – Project Management
Task	T1.4 – Data, Ethics and Cyber Security Management
Due date	30/09/2022
Actual submission date	27/12/2022
Lead beneficiary	ENG

V	Date	Beneficiary	Changes
0.1	03/11/2022	ENG	First draft
0.2	19/12/2022	ENG, ETRA, EDPNEW	Questionnaire results elaboration
0.3	27/12/2022	ENG, EDPNEW	Final version after review

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.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 957810

Executive Summary

This document presents the IANOS' Deliverable D1.11 - Ethics and Cyber security Management report v2 - developed under task T1.4 - Data, Ethics and Cyber Security Management - of Work Package 1 - Project Management. The deliverable aims to report an update on ethics, guidelines for data protection and cyber security requirements for the correct course of IANOS project activities.

According to the Grant Agreement (GA), D1.11 is the second version of three reports which provide the updates of the ethics and cyber security management based on the development of the project activities. The current version describes the fundamental rights of personal/sensitive data protection and privacy, and the methods which the Consortium intends to use for managing data and cyber-risks. Beyond the data treatment and the cyber security aspects concerning IANOS system architecture, the report considers the ethical issues relevant for the research work expected by the project.

Table of Contents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 957810

List of Figures

List of Tables

Notations, abbreviations, and acronyms

Table 1 Acronym's list

AI	Artificial Intelligence
ALLEA	European Federation of Academies of Sciences and Humanities – All EU Academies
AWS	Amazon Web Services
DPIA	Data Protection Impact Assessment
DSO	Distribution System Operator
EC	European Commission
ESB	Enterprise Service Bus
EU	European Union
GA	Grant Agreement
GDPR	General Data Protection Regulation
TSO	Transmission System Operator

1 Introduction

1.1 Objectives and Scope

D1.11 is the second version of the "Ethics and Cyber Security Management report" corresponding to Task 1.4. The scope of the document is to put in light the ethical issues that could be relevant during the project lifetime. The document also collects information in relation to the implementation of Cyber security mechanisms, techniques, technicalities that the different tools/modules of IANOS architecture have implemented or planned to implement in order to fulfil the requirements collected in the previous Deliverable D1.10.

As highlighted by different studies [1], the aspects of cyber security, privacy, ethics, and data protection are particularly relevant for the engagement of the consumers in innovative technologies. The customers' trust, indeed, seems to be more and more conditioned by a responsible way of data treatment and behaviours ethically correct. Thus, the respect of the European directives and standards could be a key point in gaining consumers' confidence and reaching a competitive advantage in a long-term perspective.

1.2 Relation to other activities

T1.4 and its deliverables provide guidelines for cybersecurity and protection of sensitive data (GDPR compliance) to protect consumers privacy, allowing local energy consumers to take full control of their data and hence further motivating consumers engagement as local community members. This document is linked to overall activities of WP4 as it addresses cyber security and protection of sensitive data. The work of this deliverable is particularly relevant for T4.1 "Cyber-secure data monitoring and VPP governance", where cyber security issues will be addressed in relation to data transactions between IANOS ICT subsystems, services, applications, and their relationship between the iVPP platform and field-level components.

1.3 Structure of the deliverable

Deliverable D1.11 is structured as follows:

- Chapter 1 – Introduction to the objective of the document and its structure.
- Chapter 2 – Dissertation about the regulatory framework GDPR compliance and the ethics principles expected during the research work. Update on ethics and data protection survey results.
- Chapter 3 – Cyber security aspects applied to IANOS project.
- Chapter 4 – Summary of the document conclusions and next steps.

2 Ethics & Data protection

2.1 Ethics applied to IANOS

All the activities carried out within IANOS project need to comply with ethical and research integrity as identified by the" European Code of Conduct for Research Integrity" [2]. The document has been written by the "European Federation of Academies of Sciences and Humanities" (ALLEA) with the aim of defining the criteria for a proper research behaviour. The EU code describes the best as well as the unacceptable practices which can occur during a research activity. The code identifies some principles common to all the research fields (enterprise, academy, industry, etc.) such as reliability, honesty, respect for colleagues and accountability for the research. On the other hand, the code highlights some unacceptable practices such as the fabrication of unreal results, the falsification of data and the using of plagiarism both in actions and ideas.

Moreover, according to art. 19 of the EU regulation n° 1291/2013, all research activities carried out within the program Horizon 2020 shall comply with ethical principles [3].

2.1.1 Ethics of technology

The ethics of technology is a sub-field of ethics addressing the ethical implications of technological innovations. Ensuring that technologies are 'ethical' means verifying their compliance with values and human rights, going beyond the purely legal aspects related to the introduction of a technological innovation by addressing, in many cases, the issues that legislation then will tackle. In general, ethics of technology deals with two issues: the ethicality of a technology in itself, for example human cloning, and the impact a given technology may have on a given society, for example the impact of social networks on human sociality.

One of the main objectives of IANOS project is to develop a Virtual Power Plant (VPP) that uses Artificial Intelligence (AI) to optimise the generation of energy and

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 957810

balance demand and supply of energy on the islands. Today, in the European Union, there are two main pillars on which to base an assessment of the conformity of technological innovations with ethics. These are “Ethics Guidelines for Trustworthy AI”, the white paper by the High-Level Expert Group (HLEG) on AI appointed by the EU commission (Ethics Guidelines for Trustworthy AI, 2019), and the brand-new proposal for the European Regulation on AI (Proposal for a Regulation on a European Approach for Artificial Intelligence, 2021).

The white paper, which has become a milestone for the development and design of ethical approaches to AI, provides the 7 key requirements on which the evaluation of the ethicality of an AI-based technology should be based:

1. Human agency and oversight
2. Technical Robustness and safety
3. Privacy and data governance
4. Transparency
5. Diversity, non-discrimination and fairness
6. Societal and environmental well-being
7. Accountability

The EU proposal for AI regulation, on the other hand, seeks to put these suggestions into practice by adopting a risk-based approach to regulate AI systems. The Commission has divided them in three main groups. A small group of AI systems are banned and prohibited, e.g., AI algorithms that allow a government to assign social credit scores to a population. Other groups are considered high-risk and need specific precautions: “For high-risk AI systems, the requirements of high-quality data, documentation and traceability, transparency, human oversight, accuracy, and robustness, are strictly necessary to mitigate the risks to fundamental rights and safety posed by AI and that are not covered by other existing legal frameworks.”.

In general, for an AI system to be considered high-risk it should satisfy both of the following conditions (*Proposal for a Regulation on a European Approach for Artificial Intelligence*, 2021, p.8):

1) AI systems intended to be used in any of the areas listed in points 1 to 8 of Annex III,

2) AI systems that pose a risk of harm to the health and safety, or a risk of adverse impact on fundamental rights, that is, in respect of its severity and probability of occurrence, equivalent to or greater than the risk of harm or of adverse impact posed by the high-risk AI systems already referred to in Annex III.

Furthermore, Annex III at point 2 affirms that any AI algorithm in charge of "management and operation of critical infrastructure: AI systems intended to be used as safety components in the management and operation of road traffic and the supply of water, gas, heating and electricity" should be considered as high risk. Since IANOS involves energy infrastructures, based on the EU proposal for the regulation of AI, the implementation of AI will imply that the project deals with high-risk AI, if and only if AI systems are integrated into safety components. Otherwise, IANOS will not include high risk AI systems.

In addition to the compliance with the ethical frameworks envisioned by the EU commission, IANOS technologies will be evaluated under T5.5 "Community and stakeholder engagement monitoring" (Ameland use cases), T6.5 "Community and stakeholder engagement monitoring" (Terceira use cases), and WP8 "Energy Cooperatives and Stakeholders Engagement". In these activities, IANOS will put in place communication efforts towards the pilot participants that enhance the social acceptability of the technologies implemented. These communication strategies will include, online and physical means and should aim to correctly communicate the ways to use the technologies implemented in the pilots, to avoid false expectations.

2.2 EU Data protection Framework

2.2.1 GDPR: guidelines for Data protection

The GDPR regulates the way in which any EU organization and any organization that caters to EU citizens processes personal data. Its aim is to protect "the fundamental rights and freedoms of individuals". With this purpose, the document describes some precise and rigorous requirements for data processing in order to guarantee the principle of transparency and give indications on data storing and users' consent in data using. As data controller, each organization must record and monitor personal data processing activities, both within the organization and when the data are transferred and processed by third parties.

Data controllers and data processors must be able to distinguish the types of data processed, the purpose of their processing, and the countries to which the data are transmitted. All consents to the data treatment must be recorded as proof of the procedure.

It is important to note that any individual has the "right to data portability", the "right to better access to their data", together with the "right to be forgotten" and the "right of revoking his consent at any time". In case of removal, the data controller must delete the personal data of the subject.

The same procedure must be followed if the data are no longer necessary for the purpose for which they were collected and, in the case of a data violation, the company must be able to notify data protection authorities and data subjects within 72 hours.

Article 5 of GDPR "Principles relating to processing of personal data" [4] defines the data protection principles for ensuring the rights of data subjects. The article describes the general rules for processing personal data, without explicit imposing the ways for observing them. The principles reported in Article 5 paragraph 1 are briefly described below:

a) The "lawfulness, fairness, and transparency" principle defines the way of processing personal data. It must be done "lawfully, fairly and in a transparent manner in relation to the data subject".

b) The "purpose limitation" principle requires that personal data must be collected for "specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes". This principle implies that the purpose must be identified before the starting of data processing and, further processing, it is only allowed under certain circumstances.

c) The "data minimization" principle requires that data must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".

d) The "accuracy" principle requires that personal data processed shall be "accurate and, where necessary, kept up to date". This implies that the data controller will use every reasonable step to ensure that inaccurate personal data is deleted or rectified.

e) The "storage limitation" principle aims to prevent the unlimited retention of personal data in a form which permits identification of data subjects. Thus, data no longer needed must be deleted or anonymized to comply with this principle. However, personal data can be stored for longer periods in some specific cases such as for public interest, scientific or historical research, etc.

f) The "integrity and confidentiality" principle requires personal data must be "processed in a manner that ensures appropriate data security". This includes protection against unauthorized processes and accidental loss using appropriate measures. This principle introduces an obligation for a prior risk assessment of personal data treatment.

The "accountability" principle reported in paragraph 2 of Article 5 requires the data controllers and processors to show how they comply with the principles and obligations imposed by the GDPR. This is a general requirement since the way for demonstrating it depends on the nature of the data; conducting a data protection impact assessment or documenting and creating a personal data inventory are some examples.

2.2.2 *Data protection impact assessment for smart grid and smart metering environment*

The energy sector benefits from the legislations on data access for smart metering and electricity network. These regulations are highly relevant for the smart grid environment as smart grids provide near real-time information about energy consumption and generation.

The devices connected to the smart grid collect a lot of data, however, not all are personal data. Beyond the consumer registration data, such as name, contact information, address and consumer's payment method, the devices record the usage data and the power provided to the grid.

When data treatment presents a high risk to the rights and freedoms of the individuals involved, for example, due to the automated monitoring of their behaviour, GDPR obligates data controllers to carry out an impact assessment before starting the data treatment.

Data Protection Impact Assessment (DPIA) is a key instrument identified by the GDPR for enhancing the data controlling rules. Indeed, it allows evaluating the risks tied to the sensitive data as well as analysing controls and mechanisms envisaged to address these risks.

The DPIA template is addressed to the operators such as DSO, generators, suppliers, etc. because the collection and the use of personal data are among their key business enablers. The DPIA can be considered an important tool in terms of accountability since, beyond complying with the requirements of the GDPR, it helps the data controllers to certify the adoption of all suitable measures to ensure them [5].

2.3 Ethics and Data protection questionnaire – Updating results

With the aim of clarifying which are the ethical issues in the context of the IANOS project, it has been circulated among partners a questionnaire. The questionnaire considers ethical aspects such as the individuals' involvement, the personal data using and the opportunity to share data out of the Consortium. Deliverable D1.10 already presented the results of the questionnaire, this document reports an update on the second period M12-M24 of IANOS activities. The survey is composed of 9 questions. In this deliverable, we only report the answers of the first six questions as the answers of the remaining three questions are unchanged.

Individuals' involvement

Except for EREF, all IANOS partners will involve individuals in their work activities as shown in Figure 1.

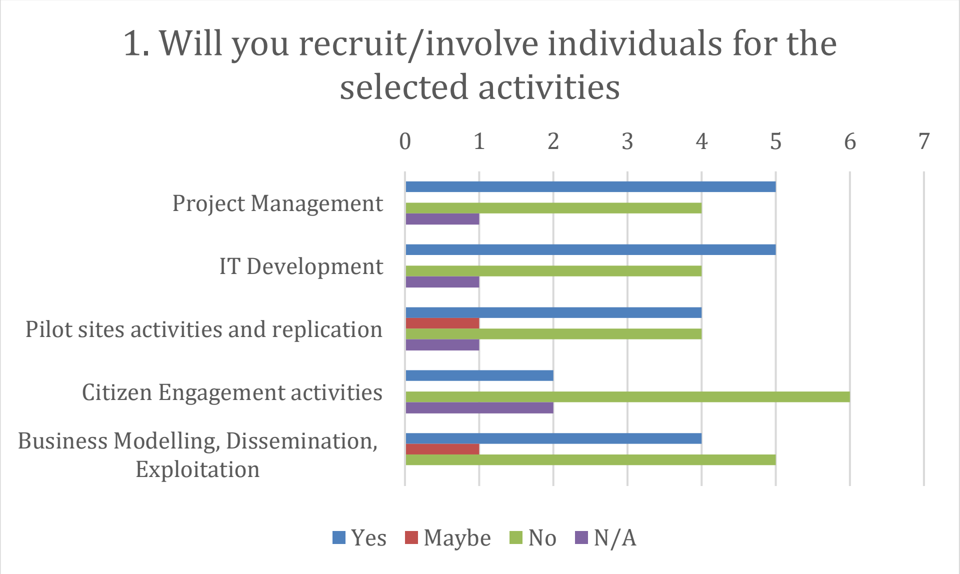

Figure 1 Involvement of individuals during the project lifetime

The partners who answered "Yes" or "Maybe" have pointed out how they intend to approach the individuals' recruitment. Compared to the results of the previous document, ETRA and EDPNEW added the following information:

- ETRA: ETRA will involve individuals from our own staff actively participating in the project to assist in every one of the activities during the project lifetime.
- EDPNEW: An external company has been hired to install the electrochemical batteries in the households of Terceira. This company was awarded the work through a public recruitment process where we have contacted several companies and requested budgets for the installation of 16 electrochemical batteries.

Processing personal and sensitive data

According to Figure 2 and Figure 3, most of the partners will not process personal and sensitive data. EDPNEW plans to process both types of data in "Pilot sites activities and replication", RINA plans to process both types of data in "Business Modelling, Dissemination, Exploitation" activities. CERTH intends to process personal data for "IT Development" activity, while for the same activity UBE and NEROA could process personal.

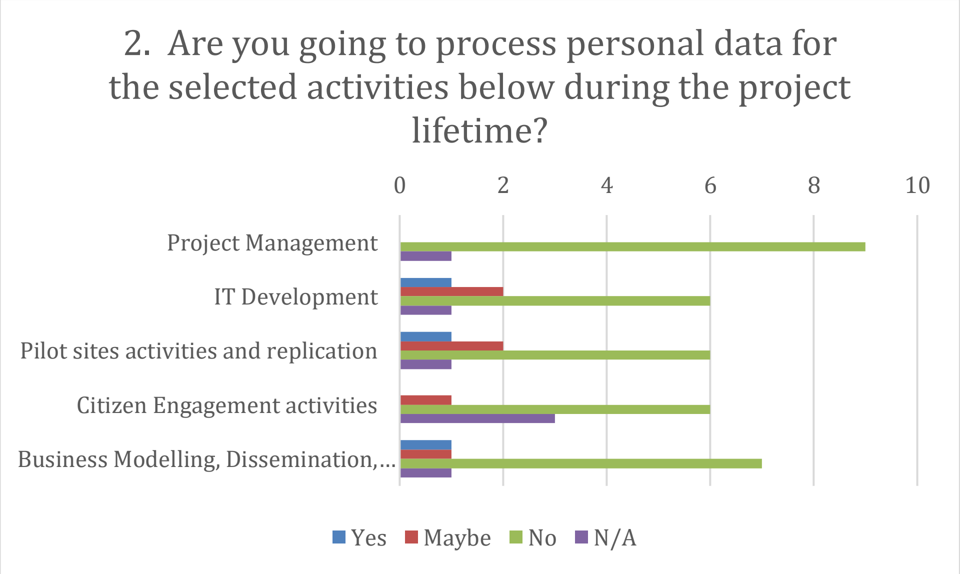

Figure 2 Processing of personal data results

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 957810

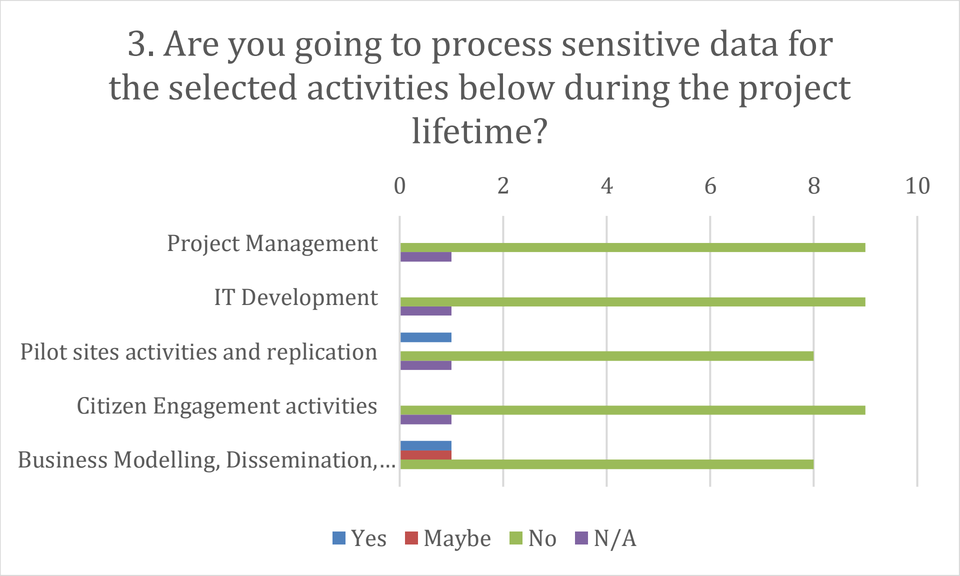

Figure 3 Processing of sensitive data results

Data profiling and tracking

The profiling activities are referred to the following definition: "Any activity of automated processing of personal data consisting of the use of personal data to extrapolate personal aspects relating to an individual, in particular to analyse or predict aspects of that person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements." As can be seen from graph in Figure 4 almost all partners answered no to the question on data profiling and tracking. On the other hand, CERTH will perform profiling on personal/sensitive data in "IT Development" and "Pilot sites activities and replication" activities. For this purpose, CERTH partners will prepare in cooperation with LH islands Site Managers, consent forms, explaining the end-users the scope of their profiling monitoring, how this data will be post-processed and the underlying data protection measures that will be taken.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 957810

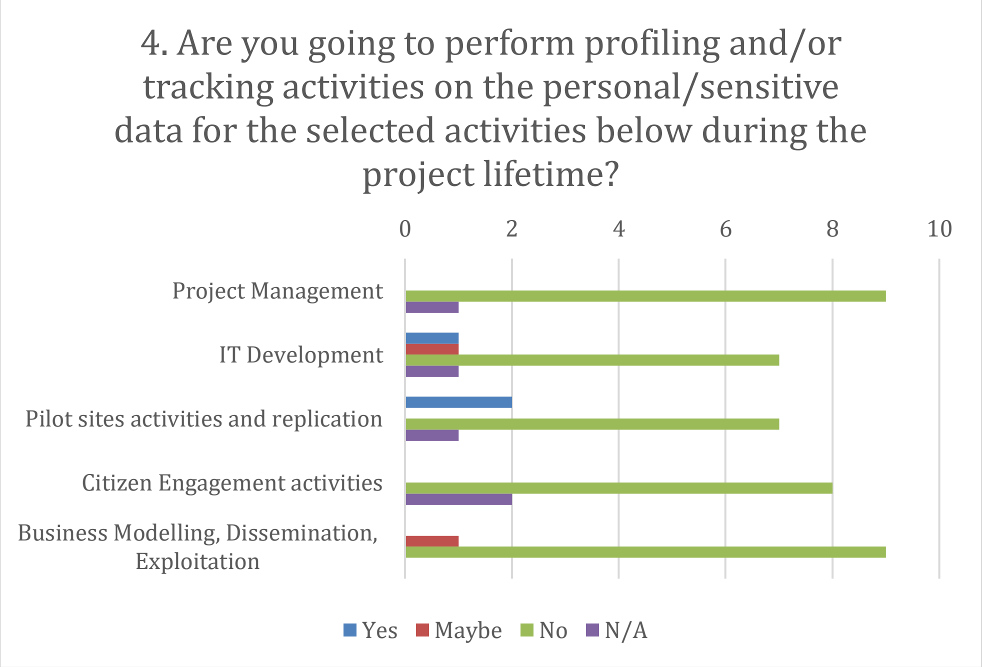

Figure 4 Intention to profiling and/or tracking activities on the personal/sensitive data during the project lifetime

Re-using data

Except ETRA, which will re-use the data as part of business modelling and dissemination activities, nobody else intends to re-use them.

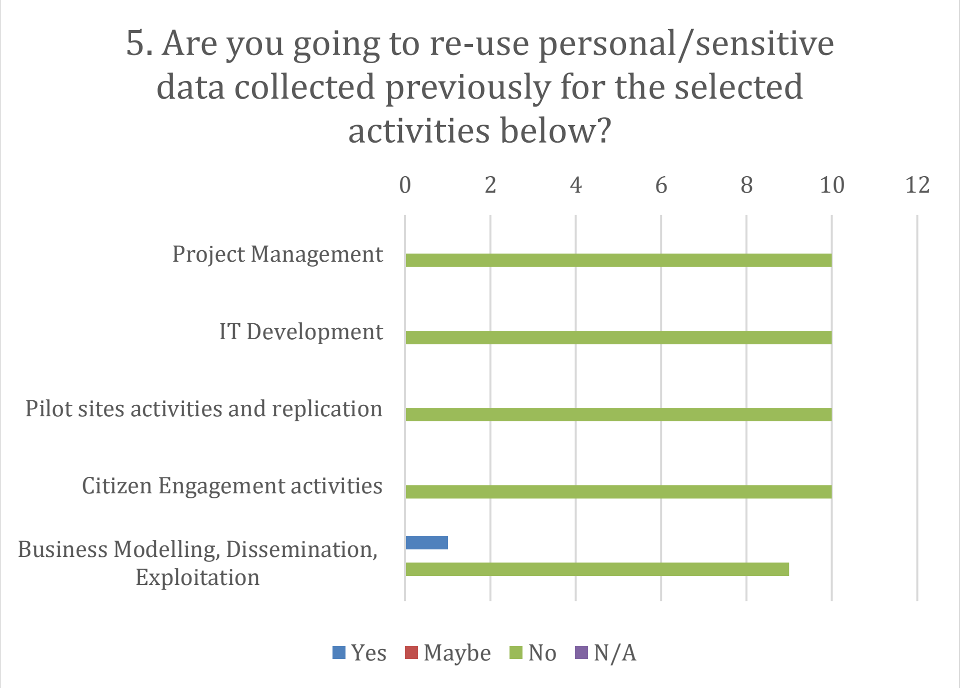

Figure 5 Intention to re-use personal/sensitive data previously collected

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 957810

Data sharing outside the Consortium

According to the GDPR, the "data processor" has the responsibility of the data treatment and of their transmission out of the organization. Question no. 6 considers the opportunity of sharing data outside the Consortium. Figure 6 shows that only in two activities it will be performed data sharing outside the Consortium. The partners that answered yes to the question added the following information:

- ETRA: Regarding Business Modelling, Dissemination and Exploitation activities, ETRA may share general data from the IANOS project. Always bearing in mind that the shared data is considered free access and publicly available data that will be used for publications, project assessments, conferences, or workshops.
- EDPNEW: Data like household address and personal contact of the residents will need to be provided to the companies performing the installations. Only name, address and contact will be provided in order for the installers to be able to schedule all activities.

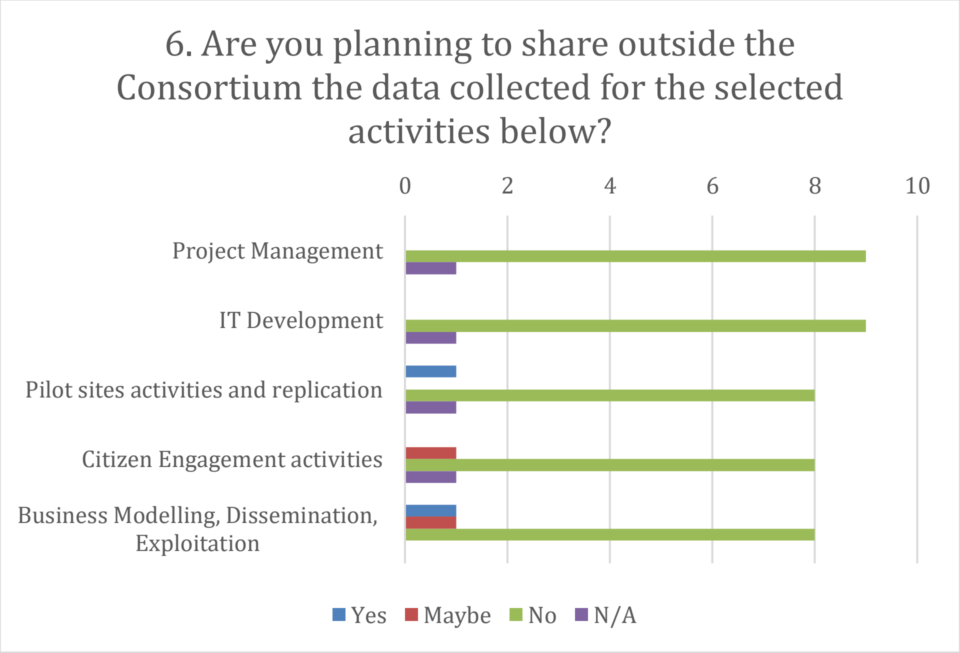

Figure 6 Planning to share data collected outside the Consortium

3 Cyber security

3.1 IANOS system architecture

Based on use cases and requirements of pilots islands a deployment architecture was developed for each of the demonstration pilots (Figure 7). The architecture has been defined in task T4.4 “Optimized cross-resource VPP coordination for energy service provision” with the participation of partners in the demonstration work packages.

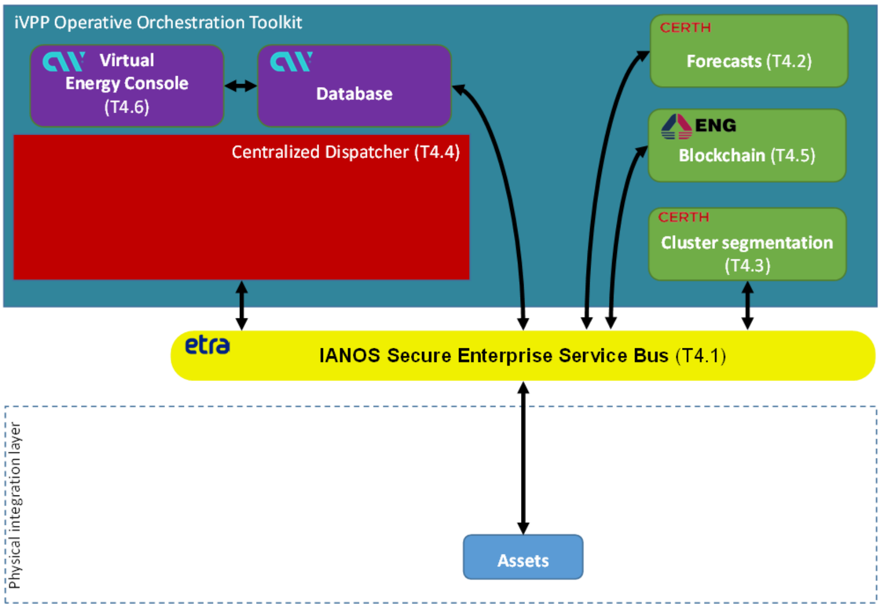
iVPP Operative Orchestration Toolkit
Virtual Energy Console (T4.6)
Database
Centralized Dispatcher (T4.4)
CERTH
Forecasts (T4.2)
ENG
Blockchain (T4.5)
CERTH
Cluster segmentation (T4.3)
etra
IANOS Secure Enterprise Service Bus (T4.1)
Physical integration layer
Assets

Figure 7 IANOS general architecture

TNO, Cleanwatts and CERTH provide similar controller functionality required for the Centralized Dispatcher (CD) in the IANOS project. TNO provides this functionality in WP5 and both Cleanwatts and CERTH are providing this in WP6. To avoid multiple controllers interfering with each other, the decision was made to keep the high-level IANOS architecture generic (there is a single centralized dispatcher) while the technology used to realize this architecture in the demonstrations on the islands can be different. Figure 8 and Figure 9 show the different deployments in Ameland and Terceira pilots.

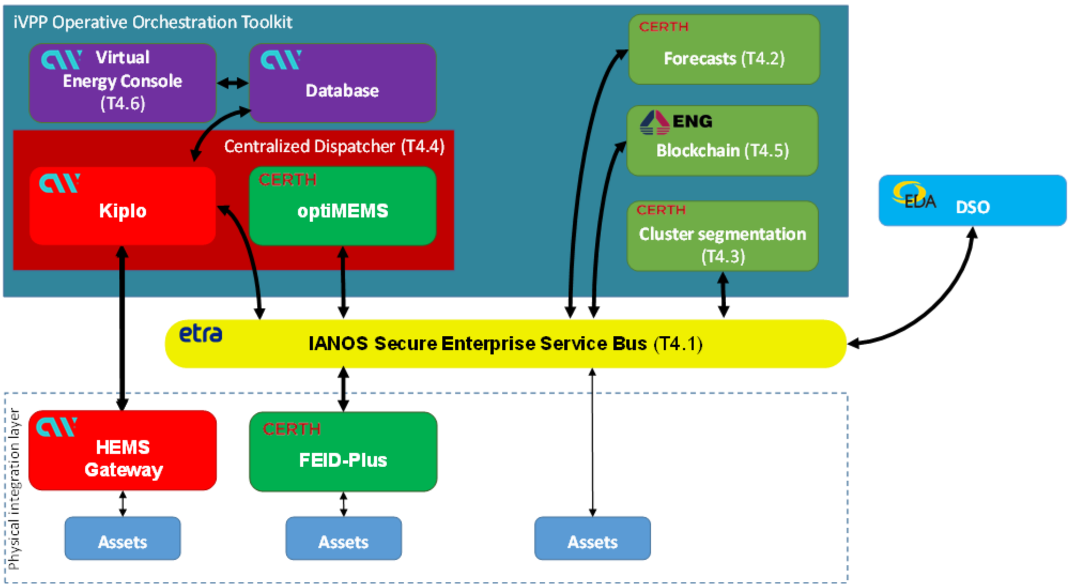
iVPP Operative Orchestration Toolkit
Virtual Energy Console (T4.6)
Database
Centralized Dispatcher (T4.4)
Kiplo
CERTH
optiMEMS
CERTH
Forecasts (T4.2)
ENG
Blockchain (T4.5)
CERTH
Cluster segmentation (T4.3)
EDA
DSO
etra
IANOS Secure Enterprise Service Bus (T4.1)
Physical integration layer
HEMS Gateway
CERTH
FEID-Plus
Assets
Assets
Assets

Figure 8 Deployment architecture for Terceira island

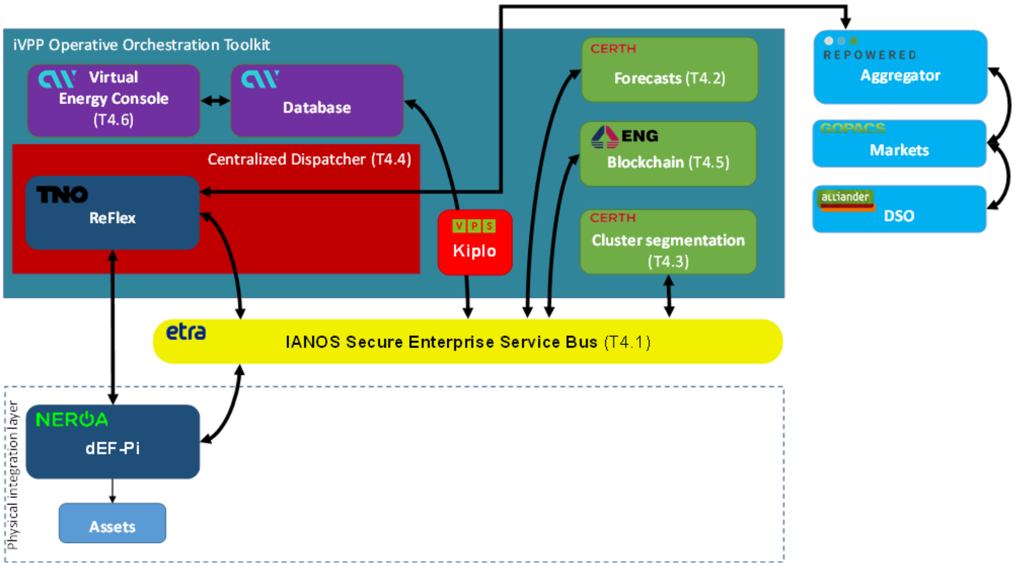
iVPP Operative Orchestration Toolkit
Virtual Energy Console (T4.6)
Database
Centralized Dispatcher (T4.4)
TNO
ReFlex
VPS
Kiplo
CERTH
Forecasts (T4.2)
ENG
Blockchain (T4.5)
CERTH
Cluster segmentation (T4.3)
REPOWERED
Aggregator
GOPACS
Markets
alliander
DSO
etra
IANOS Secure Enterprise Service Bus (T4.1)
Physical integration layer
NEROA
dEF-Pi
Assets

Figure 9 Deployment architecture for Ameland island

The different components of the architectures are described in more detail in deliverable D4.7 “The iVPP Centralized Dispatcher”. From cyber security point of view the role of the Enterprise Service Bus (ESB) is crucial. The ESB acts as an enabler of the secure data transfer within in-between VPP and the external devices.

The ESB is 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. 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. All microservices are scaled out using replicas and load balancers based on the needs of each installation. From a security perspective 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.

3.2 Cyber security recommendations for IANOS

After analysing the legislative framework on cybersecurity and the fundamental standards for energy automation systems, in deliverable D1.10 we identified a set of high-level security requirements that must be implemented in the IANOS architecture. The following table reports these requirements.

Table 2 High-level security requirements

Requirement ID	Name	Description
SR1	Implementation of security measures	The IT infrastructure must implement adequate and appropriate security measures to protect the data to be included in the infrastructure and its functionalities.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 957810

		These measures include physical or technological measures, and in any case are designed applying a risk-based approach that considers all components and their interactions.
SR2	Notification system	The IT infrastructure must be able to: 1) detect and send an early warning notification/message in case of actual or even potential attacks to the most appropriate authority; 2) send a notification message complete with all the information needed to detect the threats and determine countermeasures; 3) the notification system itself must also be designed and implemented applying appropriate security measures.
SR3	Availability	The information exchanged within the smart grid is timely and reliably accessible when needed.
SR4	Integrity	It is important to protect against improper modification or destruction of information and ensuring the non-repudiation and authenticity of information.
SR5	Confidentiality	The requirement of confidentiality aims to protect both personal and non-personal information from un-authorized access and/or use.
SR6	Accountability	Data and the operations made on certain data can be tracked and traced back to specific and pre-authorised individuals.

Table 3 provides a list of guidelines and recommendations to IANOS IT partners to apply them in developing IANOS IT architecture and its relevant components. In order to implement an appropriate IT solution, it is necessary to develop all the above requirements in order to avoid - or at least mitigate - impacts from potential concerns or threats. Each guideline/recommendation is associated to the impacted high-level requirement described before.

Table 3 Cybersecurity recommendations for IANOS project

Recommendations	Related high-level requirement
It is recommended that the ICT processes in the IANOS project address for each component the definition of security test procedures, acceptance thresholds and reports, in order to assess the coverage of all defined threats, as well as to identify new potential and unforeseen threats. It is also recommended that the IANOS components should be released with their test reports, in order to provide evidence of the security level.	SR1
It is recommended that parties be promptly notified of the status of any event occurring in the system that may have a direct or indirect impact on them. The notification system should take appropriate measures to ensure the authenticity and integrity of the reports themselves.	SR2

It is recommended to identify the most reasonable level of security with respect to time constraints. Lightweight hashing algorithms and high-performance encryption mechanisms should be considered when designing communication protocols and architecture mechanisms.	SR3
It is recommended to adopt techniques of data integrity management such as hashing, EDCs, etc.	SR4
It is recommended to define, implement and test an appropriate management of authorisations to access and/or use data. Moreover, it is recommended to continuously update the reputation level of the entities involved in data collection, access and processing. Based on the updated information, the authorisation to access and/or use the data should be reviewed accordingly.	SR5
It is recommended to ensure the traceability of permits, authorisations, reputations, events and any vital information needed to provide evidence of system accountability.	SR6

As reported in the previous chapter, the ESB is the architectural component of IANOS that plays data transfer role with a special focus on cyber security aspects. Table describes how the IANOS security requirements are met by the ESB.

Table 4 Security requirements addressed by the ESB module

Requirement ID	Name	How the module/tool addressed the requirement
SR1	Implementation of security measures	Regarding the security, different mechanisms will be stablished 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). 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.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 957810

		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. The CITRIC platform supports the following technologies to ensure security: - API REST: CITRIC has a robust secure and protected HTTPs Rest API with rate limit control to prevent attacks and allows a lot of flexibility for data ingestion through it. Besides authentication, API security allows to authorize only a certain set of data to each authenticated user. The implementation of this API has been done with Express. - 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.

		Also, a common practice today is to align a separate ESB with each network security zone, using flows/proxies to map services across security boundaries. Services can still be bridged across zones, but only with explicit flow mapping (within the ESB) and via network security (firewall) changes. This additional level of effort of needed, when coupled with appropriate business processes, can ensure appropriate security access to services within each service bus.
SR2	Notification system	The notification system of the EBS allows to define and send messages to different recipients (SMS, EMAIL, Twitter, etc.). These messages are triggered by certain events, which could be problems or security gaps.
SR3	Availability	ESB product enables the cooperation, interaction and data exchange between IANOS actors. This interface will provide a platform that informs the different actors of the project for the amount of available energy from accessible controllable loads and the availability of services that can be offered. This product provides an event-driven messaging engine that provides an abstraction layer which allows messages to be passed between systems without the need for writing application and data model

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 957810

		specific code. Therefore, this product does not process personal data. A high availability architecture should be designed securing the critical infrastructure. CITRIC 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. 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. Thanks to its architecture, CITRICT maintains the availability and integrity of the communications infrastructure, while protecting data and supporting communications infrastructure. Different processes can be applied to the ingested data: • 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
SR4	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. 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 [6], 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 [7]. A DPIA-PA Questionnaire should be

		conducted. 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" [8]. 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. In the ESB case, 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.
SR5	Confidentiality	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. 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 [6], 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 [7]. A DPIA-PA Questionnaire should be

		conducted. 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" [8]. 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. In the ESB case, 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.
SR6	Accountability	The actors in data processing have to prove their accountability to carry out responsibilities allocated to them with GDPR. These responsibilities are built on the main principles relating to processing of personal data, which are stipulated in Article 5 of GDPR [1]. Considering the importance of this Article, it is entirely cited in the following: "(1) Personal data shall be: a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'); b) 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 ('purpose limitation'); c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'); d) accurate and, 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'); e) kept in a form which permits 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'); f) 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 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.

4 Conclusions and next steps

In this deliverable we reported an update on ethical issues, data protection and cyber security mechanisms applied in the context of IANOS project.

From an ethical point of view, compliance with the European Commission's ethical frameworks must be taken into account to base an assessment of the conformity of project's technological innovations with ethics. With reference to data protection, the main guidelines are described in the GDPR, which can be considered the most significant regulation of the last 20 years in this context. Moreover, a survey has been circulated among the IANOS partners. It aims to identify security measures to be implemented by the Consortium during the project. The measurements which will be adopted aims to respect the GDPR principles and guarantee an adequate protection of data and fundamental rights of the involved subjects.

The last chapter of the document describes the cybers security measures and techniques that the different tools/modules of IANOS architecture have implemented or planned to implement in order to fulfil the requirements already defined in Deliverable D1.10. In particular, the ESB is the architectural component of IANOS that plays data transfer role with a special focus on cyber security aspects.

A final version of the document is expected to be submitted in M 48. In the next version of the deliverable, an update on ethics and cyber security challenges concerning different aspects of IANOS VPP platform will be reported.

References

[1] Timothy Morey, Theodore Forbath, and Allison Schoop, «Customer Data: Designing for Transparency and Trust,» [Online]. Available: https://d1wqtxts1xzle7.cloudfront.net/49352349/CUSTOMER_DATA-DESIGNING_FOR_TRANSPARENCY_AND_TRUST-R1505H-PDF-ENG.desbloqueado-with-cover-page-v2.pdf?Expires=1632757635&Signature=ABeBhGQOZDCySfOFvRZdufdnx9LouaE2uzgv1l4~EB5bRDpXNfNIp1S7Ra14IduNi4xmKy9Jc1e5z.

[2] ALLEA - All EU Accademies, «European Code of Conduct for Research Integrity,» 2017. [Online]. Available: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/european-code-of-conduct-for-research-integrity_horizon_en.pdf.

[3] European Parliament and the Council, «REGULATION (EU) No 1291/2013 establishing Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020),» 2013. [Online]. Available: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:347:0104:0173:EN:PDF.

[4] European Parliament and Council , «GDPR - Art. 5 Principles relating to processing of personal data,» 2016. [Online]. Available: https://gdpr-info.eu/art-5-gdpr/.

[5] European Commission, «Data protection impact assessment for smart grid and smart metering environment,» [Online]. Available:

https://ec.europa.eu/energy/topics/markets-and-consumers/smart-grids-and-meters/smart-grids-task-force/data-protection-impact-assessment-smart-grid-and-smart-metering-environment_en.

[6] «Netherlands - Data Protection Overview,» [Online]. Available: https://www.dataguidance.com/notes/netherlands-data-protection-overview.

[7] «Portugal - Data protection overview,» [Online]. Available: https://www.dataguidance.com/notes/portugal-data-protection-overview.

[8] D.-G. f. Energy, «Data protection impact assessment template for smart grid and smart metering systems,» 2018.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 957810