Ethics and Cyber Security Management report

Authors: Denisa Ziu (ENG), Caterina Sarno (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	D1.10
Dissemination level	Public
Work Package	WP1 – Project Management
Task	T1.4 – Data, Ethics and Cyber Security Management
Due date	30/09/2021
Actual submission date	30/09/2021
Lead beneficiary	ENG

V	Date	Beneficiary	Changes
0.1	28/06/2021	ENG	First draft
0.2	31/07/2021	ENG	Consolidated methodology and EU Data protection framework
0.3	05/08/2021	ENG	Questionnaire results elaboration
0.4	27/08/2021	ENG	Cybersecurity recommendations for IANOS
0.5	10/09/2021	ENG	Complete draft
1.0	29/09/2021	ENG, EDP, CERTH	Final version after internal review

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº 957810

Executive Summary

This document presents the IANOS' Deliverable D1.10 - Ethics and Cyber security Management report - developed under task T1.4 - Data, Ethics and Cyber Security Management - of Work Package 1 - Project Management. The deliverable aims to guarantee the correct course of the project activities in fully compliance with General Data Protection Regulation (GDPR) and cyber security guidelines to safeguard the consumers' privacy through the anonymization and data aggregation.

According to the Grant Agreement (GA), D1.10 is the first version of three reports which will provide the updates of the ethic 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 the energy sector, the report considers the ethical issues relevant for the research work expected by the project.

With the scope of obtaining data protection recommendations and cyber security requirements, the methodology adopted provides the main legislative aspects, the tools which will be developed as part of the project, and the results provided by the questionnaire circulated among the Consortium partners.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº 957810

Table of Contents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº 957810

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº 957810

List of Figures

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº 957810

List of Tables

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº 957810

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
CEP	Clean Energy for all Europeans Package
CIP	Critical Infrastructure Protection
DPIA	Data Protection Impact Assessment
DSO	Distribution System Operator
EC	European Commission
ENISA	European Network and Information Security Agency
ESB	Enterprise Service Bus
ETSO-E	European Network of Transmission System Operators for Electricity
EU	European Union
GA	Grant Agreement
GDPR	General Data Protection Regulation
IED	Intelligent Electronic Devices
IEC TC 57	International Electrotechnical Commission Technical Committee
NERC	North American Electric Reliability Corporation
NISD	Network and Information Security Directives
NISITR	National Institute of Standards and Technology Interagency Report
SSCP	Standard for Secure SCADA Communications Protocol
TSO	Transmission system Operator

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº 957810

1 Introduction

1.1 Objectives and Scope

D1.10 is the first version of the “Ethics and Cyber Security Management report” corresponding to Task 1.4. The scope of the document is to define a set of cyber security guidelines to safeguard the consumers' privacy through the anonymization and aggregation of their data. The document also puts in light the ethical issues that could be relevant during the project lifetime.

As highlighted by different studies [1], these aspects 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 within IANOS 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 D1.10 is structured as follows:

- Chapter 1 – Introduction to the objective of the document and its structure.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement Nº 957810

- Chapter 2 – Description of the methodology used for the IANOS project concerning the data protection and the cyber security issues.
- Chapter 3 – Dissertation about the regulatory framework GDPR compliance and the ethics principles expected during the research work.
- Chapter 4 – Section dedicated to the elaboration of the survey results.
- Chapter 5 – Chapter concerning the cyber security aspects (standards, legislation, etc.).
- Chapter 6 – Summary of the document conclusions and next steps.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº 957810

2 Methodology

Task 1.4 of IANOS aims to address cyber security and protection of sensitive data in order to safeguard consumers' privacy. To do that, the document describes the actions that will be undertaken for building a IANOS data protection framework in the light of the software tools developed within the project.

The methodology adopted for this scope (Figure 1) involves the analysis of the European Union (EU) legislation concerning the management of sensitive data (GDPR compliance); the Network and Information Security Directives (NISD) [2] and the cyber security standards in the energy sector.

Moreover, with the scope of defining the IANOS' guidelines, the methodology adopted includes the elaboration of the results of a questionnaire that has been designed and distributed to the Consortium partners.

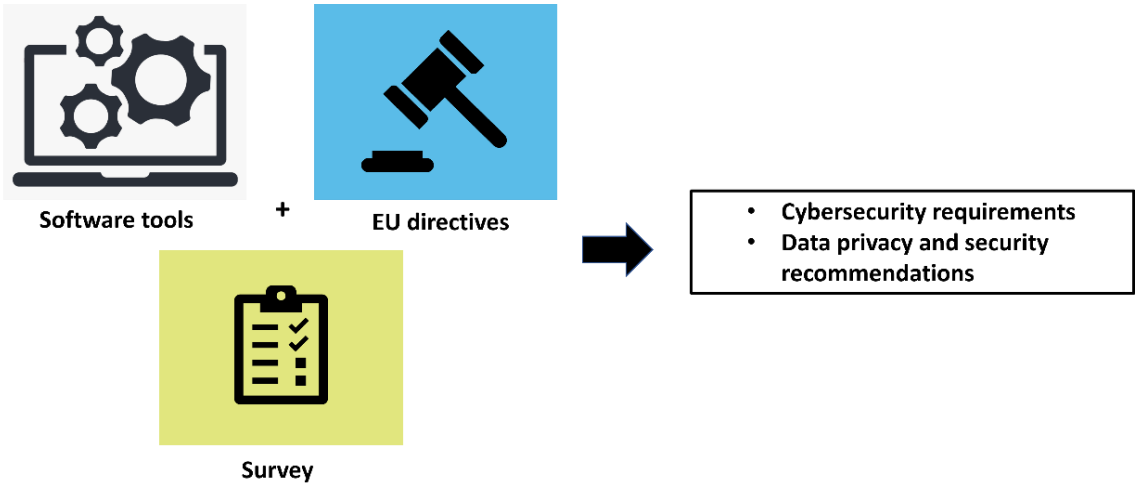


Figure 1 - Methodology adopted

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº 957810

3 Regulatory framework for data protection

3.1 Introduction to Data protection in the energy sector

The increase of the digital data-driven technologies has garnered more and more attention from the EU toward data protection. The management of personal and sensitive data has become central in the economic growth as well as the definition of a solid framework for the digital trust. From this need, the GDPR (EU) 2016/679, which represents the most significant regulation for data protection of the last 20 years, was released in 2016.

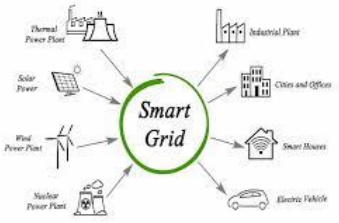
However, some other initiatives may be mentioned in this context: Cyber Security Act [2]., which introduces an EU-wide cyber security certification framework for ICT products, and the Open Data Directive [3]concerning the opportunity of using the open data for stimulating the economic growth and developing new technologies such as Artificial Intelligence- based (AI). It is worth mentioning the Regulation on the free flow of non-personal data [4]which aims to remove obstacles from the free movement of non-personal data between different EU countries and IT systems in Europe.

The EU energy policy has placed great attention on the security of the energy supply, supporting research and innovation in this area. Table 2 reports different legislative instruments adopted by the European Parliament as part of the program on “Clean Energy for all Europeans Package (CEP)” [5]. Beyond fixing the objectives for producing clean energy, these tools deal with other manners such as energy security, improvement of the operational efficiency, consumers protection and crisis management.

Table 2 – Directives and regulations foreseen from the clean energy for all European packages

Directives and Regulations	
	Directive (EU) 2018/844 amending Directive 2010/31/EU on the energy performance of buildings and Directive 2012/27/EU on energy efficiency. (30/05/2018) [6]

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement Nº 957810

	Directive (EU)2018/2002 amending Directive 2012/27/EU on energy efficiency. (11/12/2018) [7]
	Directive (EU) 2018/2001 on the promotion of the use of energy from renewable sources. (11/12/2018) [8]
 ***2030***	Regulation (EU) 2018/1999 on the Governance of the Energy Union and Climate Action. (11/12/2018) [9]
	Regulation (EU) 2019/941 on risk-preparedness in the electricity sector. (05/06/2019) [10].
ACER	Regulation (EU) 2019/942 establishing a European Union Agency for the Cooperation of Energy Regulators. (05/06/2019) [11]
	Regulation (EU) 2019/943 on the internal market for electricity (recast). (05/06/2019) [12]
	Directive (EU) 2019/944 on common rules for the internal market for electricity and amending Directive 2012/27/EU (recast). (05/06/2019) [13]

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº 957810

The CEP consists of eight legislative acts of which five are explicitly dealing with some cyber security topics. The CEP, indeed, lays down provisions on adequate cyber security measures for the electricity sector, especially considering the System Operators obligations.

- **Cyber security in the Energy Performance of Buildings Directive**

The application of new systems to the renovation actions provides cyber-risks. Thus, Thus, Annex IA of the directive states that building a smart readiness indicator calculation methodology shall take into account the principles of occupant ownership, data protection, privacy and security, in compliance with relevant EU data protection and privacy laws as well as best available techniques for cybersecurity.

- **Cyber security in the Energy Efficiency Directive**

The energy efficiency objective involves technologies and information used for this purpose. The directive lays down that smart metering, billing, and energy consumption have to be transferred and processed according to cyber security standards and to the existing rules for privacy and data protection.

- **Cyber security in the regulation on risk-preparedness in the electricity sector**

Regulation (EU) 2019/941 guarantees that a cyber-incident is properly identified as a risk. For addressing these risks promptly, the directive obligates the Operators to prearrange a risk-preparedness plan.

- **Cyber security in the Regulation on the internal market for electricity**

The regulation is focused on the data movements related to cross-border electricity flows. The aim is to establish a network code dealing with sector-specific rules for cyber security aspects.

Furthermore, the regulation formally establishes the “EU DSO entity” as a support of the European Network of Transmission System Operators for Electricity (ENTSO-E) with the specific aim of increasing efficiencies in the electricity distribution networks and promoting cyber security and data protection.

- **Cyber security in the Directive on common rules for the internal market in electricity**

Some cyber security obligations are reported in this directive as well. The document is explicitly focused on data management processes of Transmission System Operator (TSO) and Distribution System Operator (DSO) and on cyber security aspects of smart metering platforms.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement Nº 957810

3.2 EU Data protection Framework

3.2.1 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" [14] 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

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº 957810

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.

3.2.2 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 [15].

3.3 Ethical issues relevant for IANOS

All the activities carried out into the project need to comply with ethical and research integrity as identified by the" European Code of Conduct for Research Integrity" [16]. The document has been redacted 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 [17]. With the aim of clarifying which are the ethical issues in the context of the IANOS project, the next section elaborates the results provided by a questionnaire distributed among the Consortium partners. The questionnaire considers ethical aspects such as the individuals'

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº 957810

involvement, the personal data using and the opportunity to share data out of the Consortium.

4 Ethics and Data protection Questionnaire

This section presents the results of the “Ethics & Data Protection Questionnaire” distributed among the IANOS partners. The survey is composed of some multiple-choice answers, in which each partner had the opportunity to choose among “Yes”, “Maybe”, “No” and “N/A”, and some open questions, where the partners provided more details to their previous answers.

The questions concern the current and future usage, management and generation of information and data related to the project. Moreover, the last question of the survey asks if the partners intend to re-use results, data or experiments already carried out or collected in other projects or activities. The partners EDP and EREF intend to do that; however, EREF, in its contribution, has pointed out that: “EREF will use results from previous engagement strategies for community and citizen involvement in decarbonization processes for the tasks to be carried out under WP8. Yet, such information is neither sensitive nor personal and mostly publicly available”. Also “CERTH plans to re-use a set of custom-made software tools and web platforms. These software assets have been developed and tested during previous Horizon 2020 EU projects. The aim of using these custom-made tools is to assist and support actions defined under IANOS project work packages.”

Concerning the data reusing, HANZE has explained that they will re-use only conclusions from earlier studies in order to support the process for designing a community engagement strategy that they are developing. TNO intends to re-use information collected during other activities, but such information will not include personal data; for most part TNO will opt for publicly available, open access data, results and so on. TNO has added that “potential legal and IPR issues that may rise to be resolved case-by-case (via for example issuing NDA between involved projects).”

In consideration of the project complexity, partners were requested to answer the questionnaire referring to five macro-activities identified for IANOS project:

- Project Management;
- IT development (WP2, WP3, WP4);
- Pilot sites activities and replication (WP5, WP6, WP9);
- Citizen Engagement activities (WP8);

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement Nº 957810

- Business Modelling, Dissemination, Exploitation (WP7, WP10).

4.1 Data use and management

The first part of the survey focuses on the individuals' involvement; the questionnaire, indeed, aims to obtain information concerning the using of personal and sensitive data as well as their processing/tracking during the project lifetime. For sake of clarity, the definition of sensitive and personnel data are reported below:

- "Personal data is any information relating to an identified or identifiable individual. The various pieces of information which, when collected, can lead to the identification of a particular person also constitute personal data."
- "Sensitive data are personal data revealing racial or ethnic origin, philosophical, religious, or other beliefs, political opinions, membership of trade unions, parties, associations, or organisations of a philosophical, religious, political, or trade-unionist character, as well as personal data disclosing health and sex life."

4.1.1 Individuals' involvement

Except EREF and ETRA, all IANOS partners will involve individuals in their work during the project lifetime. Their recruitment will occur in all the identified activities as shown in Figure 2.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº 957810

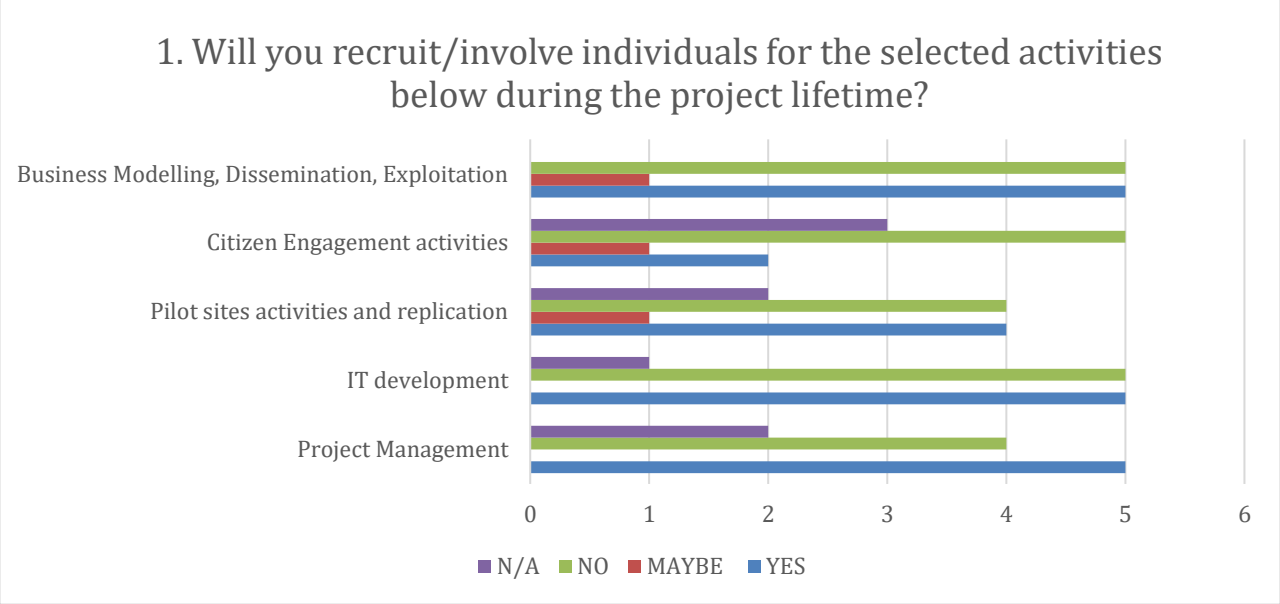


Figure 2 – Involvement of individuals during the project lifetime

The partners who answered "Yes" or "Maybe" have pointed out how they intend to approach the individuals' recruitment. The additional information provided by the partners in the survey is reported below:

- CERTH - The selected group of individuals would be the ones actively involved in IANOS pilot site activities through the utilization of metering equipment installed in their premises.

  Both external and internal stuff have been recruited to assist in the project management as well as in the IT development. The recruitment has been done thought job posting in the CERTH website, following standard recruitment practices, according to the national legislation.
- EDP - Although EDP is a partner of the project, the team involved belongs to the Innovation Department of São Miguel Island. For the activities in Terceira, the team from Terceira will be involved. For citizen engagement activities and dissemination, the Centro Comunitário Terra Chã and Escola Secundária Tomás de Borba will be involved. There might occur recruitment for installation of some of the solutions that will be installed in Terceira. This installation might be performed through local partners.
- ENG - ENG will recruit people from their own staff.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº 957810

- HANZE - From their own staff and from the other organisations that are participants in IANOS.
- NEROA - NEROA is assigned to do 1) project management and 2) IT development. Their work is to gather information on all innovative elements on the island to be able to enclose the elements on an open platform. Afterwards, we are building this dEFpi-platform as well. The project management part is done by staff of NEROA (Luuk Meijer) and gather all information to be able to build the platform. The IT-development (the platform-building itself) is yet to be assigned.
- RINA - In the course of the dissemination activities, different individuals will be reached, with the scope of communicating and disseminating the IANOS project. They will be approached following different paths, both in person and online. In the case of events and surveys involving stakeholders or general public, a specific attention to the personal/sensitive data is provided, for example during the subscription phase. More details about the communication and dissemination strategy can be found in D10.1.
- TNO - For all activities personnel already affiliated with TNO will be involved primarily, according to the TNO employment conditions. For ancillary activities such as translations, printing, catering and so on ("other goods and services") they may hire in professionals via the TNO established procurement services whose guidelines are regularly reviewed to be compliant with EU project's regulations. For DC&E activities they will approach identified stakeholders communities and their representatives via communication channels as decided by the project's communication plan and TNO communication and marketing strategy.
- UBE - UBE will recruit people from their organization.
- VPS - VPS will recruit people from their own current staff, but maybe it can have the necessity to recruit some outside people for the pilot site activities (e.g., locals for equipment installation).

4.1.2 Processing personal and sensitive data

With the term "processing" the GDPR is referred to a set of activities in which the personal and sensitive data are used beyond their collection and analysis.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº 957810

According to Figure 3 and Figure 4, most of the partners will not process personal and sensitive data. RINA plans to process both types of data in the “business modelling, dissemination and exploitation” activity, whereas EDP intends to process personal data for performing the “pilot sites and replication, the citizen engagement, and the business modelling and dissemination” activities. CERTH, UBE and NEROA could process the personal data in the “IT development” (Figure 3). As shown by the red bar graph in Figure 4, there is only one “Maybe” answer related to the sensitive data processing which belongs to ETRA partner.

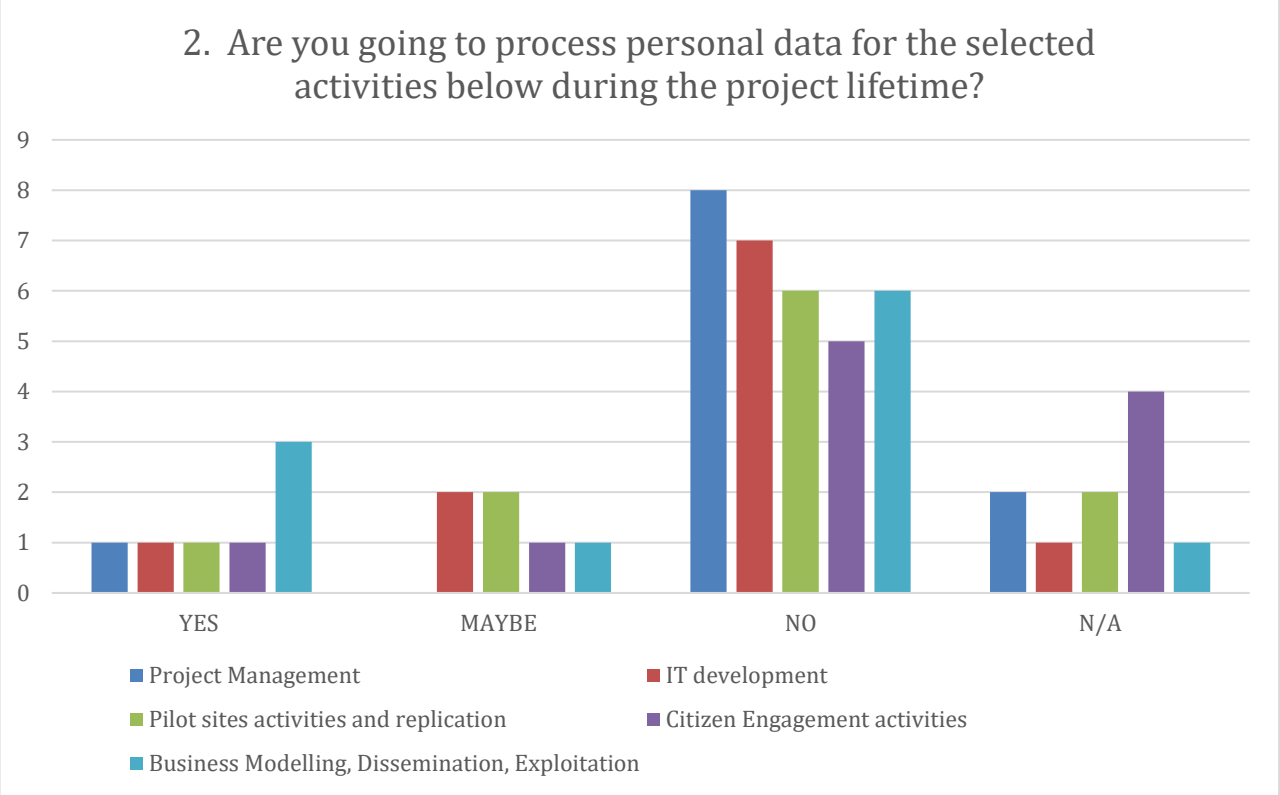


Figure 3 - Processing of personal data during the project lifetime

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement Nº 957810

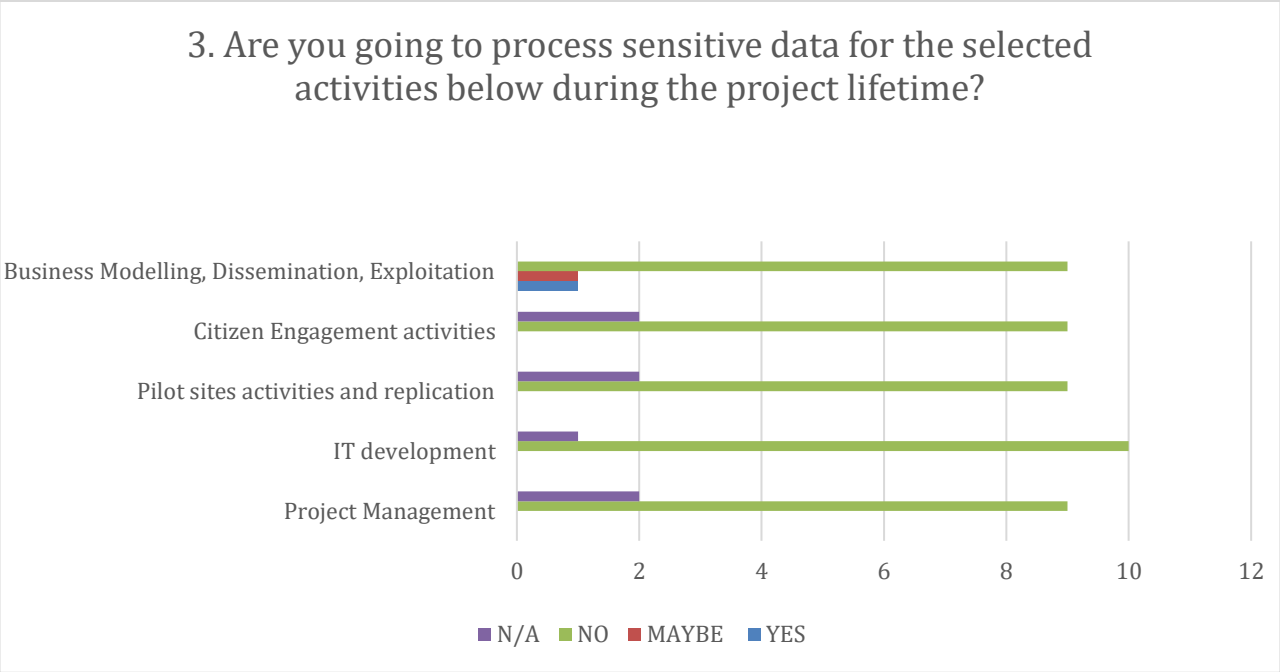


Figure 4 - Processing of sensitive data during the project lifetime

The partner HANZE has answered negatively to the multiple-choice questions no. 2 and no. 3 specifying that: “Linked to the process of citizen engagement on the island of Ameland, we have the intention to have those citizens that will join in on any of the use cases (that get engaged, so to say) also cooperate with a separate project in which we will gather smart meter data and some general data about people’s houses, education a family composition. If they do not want to participate, then that is ok. So, it is not really a IANOS activity, therefore I have not included it in my answers.”.

TNO has also contributed to the questions explaining: “Personnel information such as name, surname, contact details and job description will be shared with both partners and potentially European Commission (EC) and reviewers for both reporting purposes and day-to-day operations. For all research and development activities, the current plan is to use anonymized data; the expectation is that pilot partners will transfer, if necessary, anonymized data to TNO servers for processing; strong preference to open access and publicly available data.”

Moreover, CERTH has added: “Data will be retrieved, pre-applying standard anonymization and encryption techniques, in collaboration with main systems operators, coordinated by the LH islands site managers, dealing with the monitoring of communities’ consumption and production profiles, for assessing the environmental and energy impact of the deployed

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement Nº 957810

innovative technologies. CERTH will use VERIFY platform to retrieve this anonymized data, from the two LH islands, to perform the environmental assessment."

4.1.3 Data profiling and tracking

Another aspect that should be considered is if the partners are going to perform profiling and/or tracking activities of the personal and sensitive data (Figure 5). 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."

Beyond the large part of IANOS partners answering "No", Figure 5 shows seven affirmative answers and three "Maybe" answers.

These last are probably due to the current uncertain definition of some activities of the project, thus, this information will be clarified in the second version of the deliverable. Indeed, TNO has pointed out that its profiling and tracking activities will be in accordance with the project's communication strategy and plan (in case, for example, of tailoring the IANOS message to a certain target group of stakeholder/audience to meet their needs and interest).

In this context, CERTH has added that "it 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. These forms can be prepared using native languages, i.e., Portuguese and Dutch. More specifically, pilot participants will be informed with clarity about the procedure of the pilot trials and the objectives of the data storage and analysis that will result from the pilot trials; no sensitive personal data will be collected; a data minimization policy will be adopted at all levels of the project: this will ensure that no data which are not strictly necessary to the completion of the particular study will be collected; no data will be collected without the explicit consent of the individuals; participants will be able to quit the pilot trial at any point, if they wish, without any consequences. He/she can exercise his/her right to access and delete his/her data at any moment. "

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº 957810

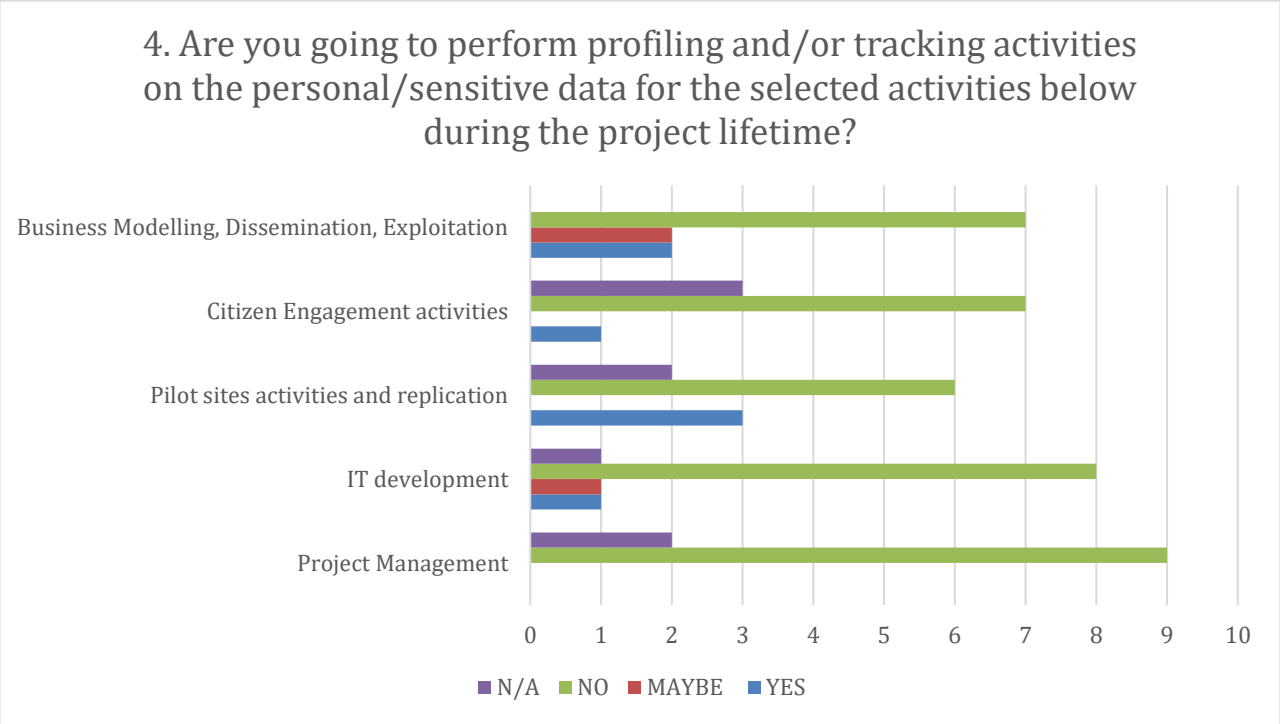


Figure 5 - Intention to profiling and/or tracking activities on the personal/sensitive data during the project lifetime

4.1.4 Re-using data

In ethics and data protection, the planning of re-using of the personal/sensitive data previously collected is relevant. Except ETRA, which will re-use the data as part of business modelling and dissemination activities, and EDP which has answered “Maybe”, nobody else intends to re-use them.

ETRA, in its contribution, has explained that the Business Modelling analysis will require the use of sensitive data collected from the solutions implemented to quantify the impact of the business models developed within IANOS. The business model task (WP7) is not still active, so the users have not been warned for these purposes yet.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement Nº 957810

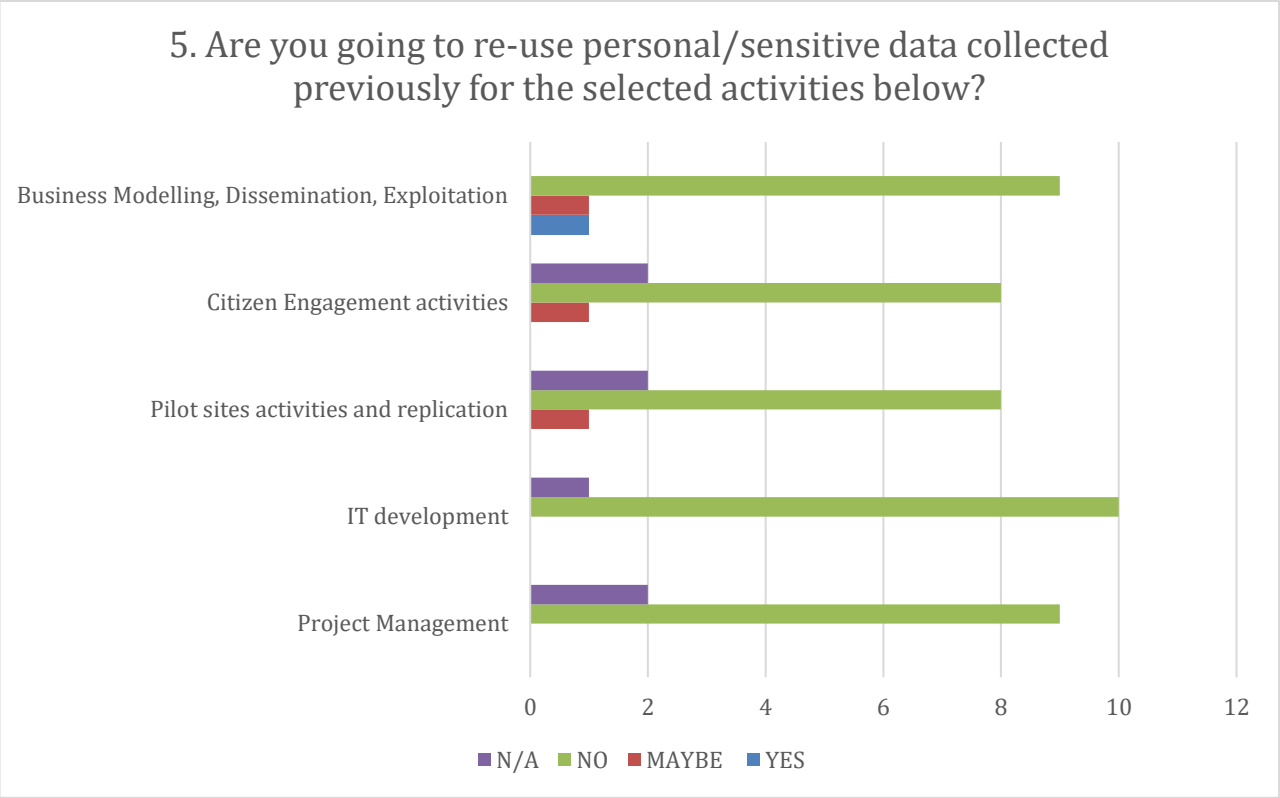


Figure 6 - Intention to re-use personal/sensitive data previously collected

4.1.5 Data sharing outside the Consortium

According to the GDPR (paragraph 3.2.1), 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 7shows only four affirmative answers in which the “IT development and Citizen engagement” activities are not involved. Two of them have been provided by EDP which also has explained that it will depend on the dissemination level.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement Nº 957810

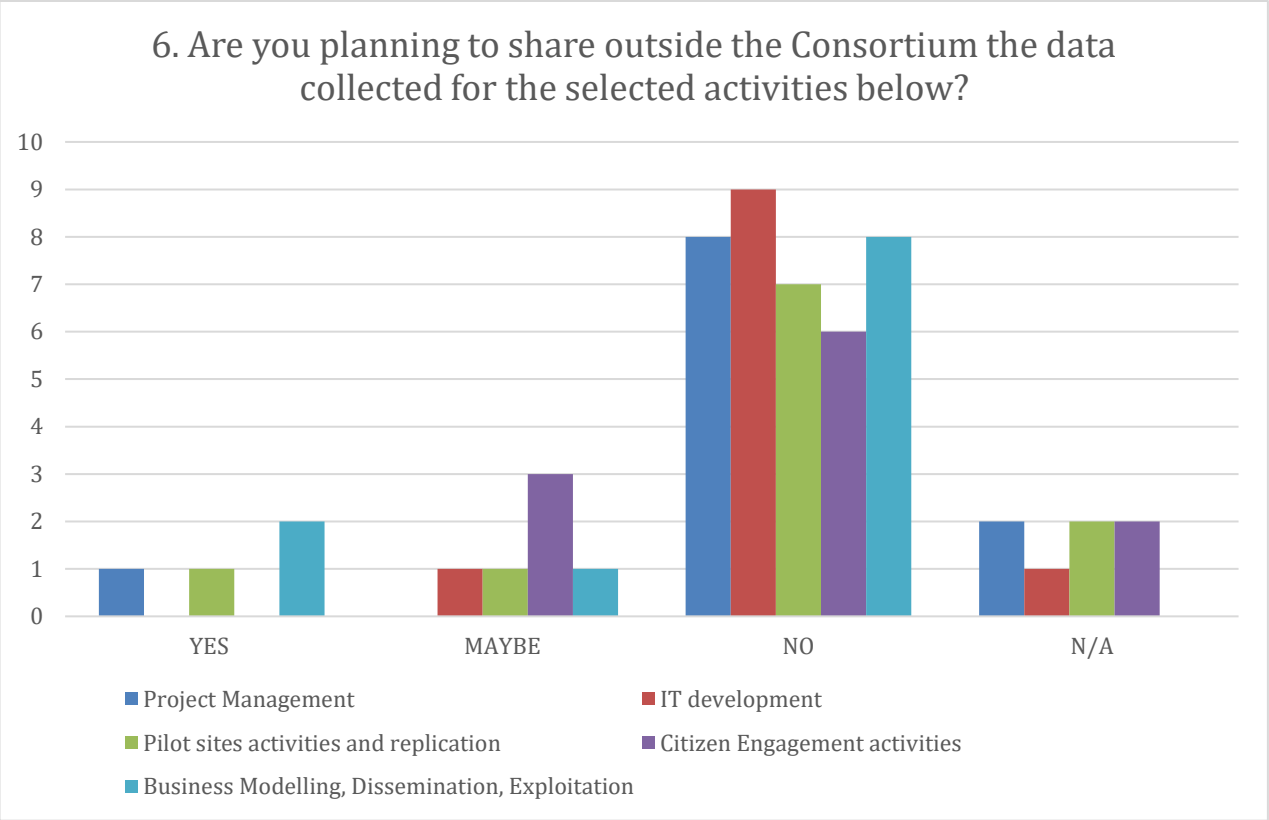


Figure 7 – Planning to share data collected outside the Consortium

In this context, the partner HANZE has also commented that the data will not be shared from its side, but they will probably be used for publications. HANZE has specified: "The data will not be a part of a publication, only aggregated results and conclusions that are based on it", whereas TNO has added: "In case of customer evaluation and/or auditing of the project we may share information with the appropriate organization within the Netherlands or EU. In terms of dissemination and communication activities we may share general project data (not personal) with conference & workshops organizers, magazines and journals editors and publishers and on social media according to the project's communication plan. In any case our strong preference is to share information perceived as open access and publicly available data. Also, whenever possible fully anonymized datasets will be considered (for example in case of a publication to journals and so on). In all situations sanction and export control regulations apply as established by the Dutch government and followed by TNO policy."

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº 957810

4.1.6 Storage solution

Question 7 asks the partners: “If you are going to collect and process personal/sensitive data, please provide information on the storage solution. Will you store it on a cloud server? Which one? Will you use specific IT tools/solutions to process the data collected? If yes, which ones?” Below the partners’ answers are reported:

- CERTH - Key value and/or relational databases (such as PostgreSQL) will be used to store the data to be processed. The stored data will be hosted on local web server(s) at CERTH premises (protected by extended firewall filters). Sensitive personal information will be encrypted during database storage. CERTH will use both custom-made (developed and integrated in WP3, WP4, WP5, WP6) and commercial tools (e.g., Digsilent Power factory, Simapro - only for a specific subset of the stored data) to process data retrieved from pilot sites individuals.
-
- EDP - EDP will store it in a cloud server (private SharePoint for Consortium members).
- ENG - ENG will collect data coming from smart meters. Anonymization data will be used in order to avoid the connection with the data provider.
- EREF - N/A.
- ETRA - IANOS Enterprise Service Bus (ESB) is the component that will play the data transfer role in the iVPP among the components. This solution can be easily deployed in Google, Amazon Web Services (AWS) and Azure clouds services.
- NEROA - At this moment, on Ameland it is not yet determined how we exactly are going to store the data. The consideration at this moment is to build a physical server on the island itself and use this as the storage of the data. To gather and process the data, we either use Raspberry Pi’s or gather it through API’s.
- RINA - Within the scope of communication and dissemination activities, people interested in it (stakeholder or general public) are invited to subscribe to the IANOS newsletter and/or to join IANOS social channels. Whenever they subscribe to the newsletter, data are saved in SendinBlue which is a European mailing system and complies with the GDPR (the hosting servers on which SendinBlue processes and stores its databases are all located within the EU, on own servers, on Google Cloud

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement Nº 957810

or on AWS.). The cookie privacy statement of the project website refers to the law of the country where it is originated, in this case, the Dutch law.

- TNO - TNO cloud environment running on cloud or in-house servers; multi factor authentication and access rights controls apply.
- UBE - The datasets from the pilots that would be collected for the context of the IT developments that our company is going to conduct will be stored in the Company's drive. The IT tool that will be leveraged depends on the volume of that data. Either by using python or Apache Hadoop tool.
- VPS - VPS will only store energy measurements and other data acquired from IoT devices. No personal or sensitive data will be stored.

4.2 Processing and data collection

This paragraph reports the answers provided by the Consortium partners concerning the measures/techniques that they are going to implement for protecting the data collected and processed, especially against unauthorised access.

4.2.1 CERTH

- **Technical measures:** the data will be stored in secure data servers (both in terms of physical and cyber access).
- **Organizational measures:** databases access will be granted only to authorized users under specified usernames and passwords.
- **Encryption techniques:** according to each specific UC, hybrid (authenticated) encryption schemes will be used.
- **Anonymisation techniques**: generalization and pseudonymization schemes will be used to make data as less identifiable as possible.
- **Pseudonymisation techniques:** personal data (e.g. names) will be substituted by private identifiers where possible maximizing data confidentiality.

CERTH partner also added the following clarification to the question:

"IANOS will collect personal data[1]. Furthermore, any of this personal data from research participants will not be included in project deliverables and dissemination materials without prior informed consent. Moreover, the Ethical Advisory Board as defined in GA, will ensure that the project is proceeding in an ethically acceptable manner, i.e., aligned with national or European regulations relevant to data protection, transfer, privacy as well as informed consent. We have analysed all these relevant needs set out in the GA of the IANOS project and other EC documents such as Ethics and data protection[2] and Article 39 of the AGA – Annotated Model GA[3].

Regarding personal data transfer and processing among the 34 EU partners, IANOS Co-ordinator and Ethical Advisory Board confirm that all partners will process personal data under the GA in accordance with EU and national law on data protection (in particular, GDPR No 2016/679[4]) as well as the Universal Declaration of Human Rights and the Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data[5]."

4.2.2 EDP

- **Technical measures:** N/A
- **Organizational measures:** private SharePoint on an institutional server (EDP cloud server)
- **Encryption techniques:** N/A
- **Anonymisation techniques:** N/A
- **Pseudonymisation techniques:** N/A

4.2.3 ENG

- **Technical measures:** The tools and processes to be used will be selected according to the nature of the data and how it will be provided by the Data provider.

[1] Personal data means any information, private or professional, which relates to an identified or identifiable natural person (Section 39, Annotated Model Grant Agreement)
[2] https://ec.europa.eu/info/sites/info/files/5._h2020_ethics_and_data_protection_0.pdf
[3] https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/amga/h2020-amga_en.pdf
[4] https://eur-lex.europa.eu/eli/reg/2016/679/oj
[5] https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº 957810

- **Organizational measures:** Engineering follows a specific internal process for privacy management according to the GDPR. The process defines the governance structure, roles, risks, impact assessment and procedures related to the protection of personal data.
- **Encryption techniques:** Well-known encryption standards will be used, e.g., AES for symmetric key encryption and RSA for public-key systems.
- **Anonymisation techniques:** Techniques like noise addition, substitution or data aggregation will be considered. Anonymisation techniques will be applied before data transfer, if needed.
- **Pseudonymisation techniques:** Pseudonymised personal data will be considered as information about an identifiable natural person.

4.2.4 ETRA

- **Technical measures:** N/A
- **Organizational measures**: Every ingestion process is authenticated and authorized by a layer of security.
- **Encryption techniques**: Each credential per token or user has an authorization scheme to access a subset of platform data at three levels of security.
- **Anonymisation techniques:** The authorization scheme will allow the anonymization of the different tokens to be sent across the information exchange through the ESB.
- **Pseudonymisation techniques:** N/A.

4.2.5 NEROA

To protect the personal/sensitive data we will store most of the data locally (at the premises nearby the device). Reflex does not need to know WHO is ‘behind’ the data.
We will use the following principles to implement data protection:

- Local data; we will store as much as data locally and NOT in the cloud.
- The S2 interface will also make the data more abstract.
- Minimize the data exchange.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement Nº 957810

The exact security measures to protect the data will be determined and implemented during the project and will depend on the different use cases (Reflex and Monitoring for KPI).

4.2.6 RINA

- **Technical measures:** IANOS use an API connection with *Sendinblue* so people can registrate for the newsletter at the website, without saving any data in our backend.
- **Organizational measures:** only selected people in the organization have access to the personal data and their use is restricted exclusively to IANOS purposes. Passwords are not shared and common practices to preserve them are applied.
- **Encryption techniques:** Data is encrypted before being stored in the cloud (AWS or Google Cloud). Data is backed up at least once a week and, in some cases, (depending on how you use your data) more often.
- **Anonymisation techniques:** data are anonymized and while the website uses cookies, IANOS has obtained a data processing agreement with Google and the last numbers of your IP address have been masked. Furthermore, we don't allow Google to use the obtained information for other Google services (additional information can be found at https://ianos.eu/cookie-statement/).
- **Pseudonymisation techniques:** currently N/A.

4.2.7 TNO

- **Technical measures:** Two storage options will be considered (after consulting consortium partners and project's DMP):
    - *Option 1: SharePoint Online*

      Information is stored in Microsoft's SharePoint Online service. The data is located within the EU (Ireland and the Netherlands). Access to the information is possible worldwide based on a TNO account or a TNO partner account, but always on the basis of Multi Factor Authentication. Microsoft offers standard features to ensure the confidentiality, integrity and availability of the information. In addition, TNO makes a daily back-up of the information to a service in the Amazon S3 Cloud, also within the EU. Both for SharePoint Online and for the backup use is made of

encryption 'in transit' and 'at rest'. This option is typical for all project related information, unless otherwise specified (see below).

- *Option 2: SharePoint in TNO Data Center*

  Information is stored in the SharePoint service of TNO. The data is located in one of the two data centers contracted by TNO in the Netherlands. The equipment installed in these data centers is owned by TNO and is managed exclusively by TNO. Access to the information is possible worldwide based on a TNO account from the TNO network, or via TNO telecommuting facilities based on Multi Factor Authentication. TNO offers standard facilities to safeguard the confidentiality, integrity and availability of the information, including at least daily backup of the information to the data center other than where the service itself is active. This option will be considered for personal (pseudoanonymized) data that may be collected – though at this stage we do not anticipate to do so.

It remains to be seen whether we would need to use software for processing (personal) data that is not provided by TNO on actual TNO servers. If indeed this is to be the case we will evaluate and arrange for a processor agreement with the software supplier.

- **Organizational measures:** Apply access rights controls; in particular access to personal (pseudo-anonymized) data will be limited to the researchers "on need to know basis"; when sharing between consortium partners, project's DMP is applicable; the project's repository (Microsoft Teams) will also be used according to the guidelines as specified by the project coordinator. Only reports and deliverables specified as public will be shared on website and other communication channels as identified by the project's communication plan. Open software and tools will be shared via platforms are identified by the project's exploitation guidelines (such as for example GitHub[6]).
- **Encryption techniques:** When personal data are transmitted electronically to a receiver outside TNO, the data can be encrypted using the SURF File Sender[7]. Unless otherwise explicitly specified the project's repo facilities will be used.
- **Anonymisation techniques:** For IT development we will use anonymisation techniques such as *randomization* or *generalization* according to opinion 05/2014 on

[6] https://github.com/
[7] http://www.surf.nl/en/surffilesender-send-large-files-securely-and-encrypted

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº 957810

Anonymisation Techniques as a result of the working party on data protection of individuals (see also article 29).

- **Pseudonymisation techniques:** If applicable, encryption with secret key.

4.2.8 UBE

- **Technical measures:** N/A
- **Organizational measures:** N/A
- **Encryption techniques:** N/A
- **Anonymisation techniques:** In case that we will collect data including information regarding specific consumers' personal information, those will be removed from the dataset in order to ensure anonymity of the data owner.
- **Pseudonymisation techniques:** As a pseudonymization technique will be used the masking technique, which allows the part of the dataset which is crucial to be hidden with random characters or other data.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº 957810

5 Cyber security regulations, guidelines, and standards

5.1 Cyber security legislation and guidelines in EU

- **COM (2017)477 – EU Cyber security Agency and Information and Communication Technology cybersecurity certification (“Cyber security Act”)**

For enhancing the preparedness to cyber-risks, EU has adopted a first cyber security strategy in 2013 which reports a set of actions for achieving a coherent international cyberspace policy.

The strategy was drafted by the EU Agency for Network and Information Security (ENISA) which is the cyber security competence centre in Europe. The agency helps the EU and EU member states to prevent, detect, and respond to information security issues.

On 13 September 2017, the European Commission published its “cyber security package”, a set of initiatives aimed at strengthening resilience, deterrence, and the defence of the Union in the face of cyber-attacks. These measures included a proposal for a regulation on ENISA and certification of cybersecurity information technologies and communications (Cyber security Act – COM (2017) 477) [2]. The Regulation gives ENISA a permanent mandate and strengthens its role in prevention, advice, and cooperation. The Cyber security Act has a second component which is to create a European cyber security certification framework in which ENISA plays an essential role. The Cyber security Act was adopted in April 2019 and, among its objectives, it introduced the first EU certification scheme for ICT digital products, services, and processes. Moreover, a European Cyber security Certification Group was established in order to promote the implementation of the certification framework.

- **Directive Network and Information Security Directives (NISD)**

The NIS Directive introduces the security requirements as legal obligations for operators and suppliers of some key digital services. The directive can be considered an essential step for improving the attention toward the risk management in the light of the rapid proliferation of connected devices. The directive also requires the European Commission to

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement Nº 957810

review it periodically. Thus, a new legislative proposal was presented in December 2020 after a consultation opened in July. It covers the fields of cyber security and critical infrastructures protection. The legal framework considers the increased digitalisation of the market, keeping in line with the Commission's priorities to make European member states ready for the digital age [18].

- **Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security**

The National Institute of Standards and Technology Interagency Report (NISITR) 7628 Guidelines for Smart Grid Cyber Security offers an analytical framework that can be used to develop smart grid related characteristics, risks, and vulnerabilities. The report is rich of technical information which makes it difficult to read and apply as much to encourage the development of ICT tools with this aim [19].

5.2 Cyber security standards

The cyber security standards guarantee the safeguard of information exchange among many actors in the energy automation systems. The technical security standards provide specific technology solutions for satisfying the security needs concerning organizations and technologies used. Some of the fundamental cyber security standards related to the energy sector are reported below:

- **IEC 62351 standard: Power systems management and associated information exchange – Data and communication security.**

IEC 62351, defined by the International Electrotechnical Commission Technical Committee responsible for the development of standards for computer exchange (IEC TC 57), has filled a void in the cyber security field and opened the way for existing unsecured communication protocols. By applying this standard, for example, to the 60870-5-101/-104, DNP3 and IEC 61850 protocols, energy systems can achieve end-to-end safety. The set of standards defines the need for encryption and access control through authentication and authorization.

- **IEC 62443 standard: Security for industrial automation and control systems.**

The aim of IEC 62443-4-2 standard is to guarantee the safety of the industrial plant. Together with confidentiality, availability, and integrity, the standard has the remarkable advantage of mitigating the risks associated with interferences and accidental damage.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº 957810

- **IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems.**

IEC 61508 governs the functional safety of programmable electronic systems of electrical, electronic, or programmable electronic systems.

- **ISO/IEC 270xx: Information Security Management System.**

ISO/IEC 270xx: includes a series of standards for the information security management such as ISO/IEC 27001:2013 and ISO/IEC 27002:2013. Some of them are addressed to specialized sectors, such as the ISO/IEC 27019, based on ISO/IEC 27002:2013 applied to process the control systems used by the energy utility industry for monitoring the production, transmission, storage, and distribution.

- **IEEE 1686: Intelligent Electronic Devices (IED) Cyber Security Capabilities.**

IEEE 1686 defines the functions which must be provided in IED to fix critical infrastructure from access, operation, and configuration point of view.

- **IEEE 1711.2-2019: IEEE Standard for Secure SCADA Communications Protocol (SSCP).**

This standard defines a cryptographic protocol known as SSCP that protects the integrity and, optionally, the confidentiality of asynchronous serial communications. Due to the elevated concern of cyber security in the power industry, the standard is addressed to the security need to protect the serial links communications in the substations.

- **IEEE C37.240: Cyber Security Requirements for Substation Automation, Protection and Control Systems.**

IEEE C37.240 provides a balance of the cyber security measures between technical and economic feasibility. In this way, the risks expected at the substation can be addressed. At the same time, it has to guarantee the access to the legitimate activities.

- **CEN/TR 17167: Communication system for meters.**

The standard 7 of EN 13757 series specifies transport and safety services relating to communications systems for meters. The standard is purposed to protect consumer data and guarantee relative privacy [20].

Technical Report CEN/TR 17167 contains additional information to the requirements reported in EN 13757-7, concerning the non-regulatory requirements and meter communication itself as well [21].

- **IEEE P1402: IEEE Draft Guide for Physical Security of Electric Power Substation.**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº 957810

IEEE P1402 is a guide which describes recommended practices for the physical security of electric power substations. It is designed to address several threats, including unauthorized access to substation facilities and vandalism.

5.3 Cyber security recommendations for IANOS

After analysing the legislative framework on cybersecurity and the fundamental standards for energy automation systems, it is possible to identify a set of high-level security requirements that must be implemented in the IANOS architecture. The following table reports these requirements.

Table 3 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. 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.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº 957810

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 4 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. The following practical guidelines will be refined during the course of the project, as soon as technological improvements occur. Each guideline/recommendation is associated to the impacted high-level requirement described before.

Table 4 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.	SR1

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº 957810

It is also recommended that the IANOS components should be released with their test reports, in order to provide evidence of the security level.	
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

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº 957810

6 Conclusions and next steps

The document provides a clear overview of the current regulations regarding the ethical issues and cyber security requirements related to the IANOS research field. The main guidelines for data protection are described in the GDPR, which can be considered the most significant regulation of the last 20 years in this context. Moreover, D1.10 introduces several directives and cyber security standards at the European level related to the energy sector and recommendations applicable to the project.

The survey circulated among the IANOS partners has proved a power instrument for identifying a first version of the 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 elaboration of the survey has shown that some of the partners already have an idea of the measurements and techniques that they intend to use for this scope; in other cases, the procedures will be clearer during the project, in the light of the development of the activities.

The deliverable points out that the partners will make a limited use of personal and sensitive data in the project lifetime as well as their processing. Moreover, they will mostly take information from individuals inside their own organizations, without involving external ones. Concerning the data storage, the partners have mentioned different cloud solutions such as Google cloud and AWS.

There is not the intention of sharing data outside the Consortium, if not for the research scope, such as publications and conference presentations. In this regard, the ways in which the data will be shared should be better defined and described in the next versions of the document (D1.11 and D1.12).

The last section of the document provides a set of high-level security requirements that must be implemented in the IANOS architecture in order to avoid potential threats. . In the next version of the deliverable, related cyber security challenges and relevant specific measures concerning different aspects of IANOS VPP platform (edge-level gateways and devices and cloud platforms and data and multiple energy actors) will be considered.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº 957810

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] European Commission, «Directive on security of network and information systems,» 2016. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/nis-directive.

[3] European Parliament and Council, «Cyber security Act – COM (2017) 477,» 2017. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:0477:FIN.

[4] European Parliament and of the Counci, «DIRECTIVE (EU) 2019/1024 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL,» 2019. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.172.01.0056.01.ENG.

[5] European Parliament and Council, «REGULATION (EU) 2018/1807 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL,» 2018. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº 957810

[6] European Commission, «Clean energy for all Europeans package,» 2019. [Online]. Available: https://ec.europa.eu/energy/topics/energy-strategy/clean-energy-all-europeans_en.

[7] European Parliament and Council, «Directive (EU) 2018/844 amending Directive 2010/31/EU on the energy performance of buildings and Directive 2012/27/EU on energy efficiency,» Official Journal of the European Union, 2018.

[8] European Parliament and Council , «Directive (EU)2018/2002 amending Directive 2012/27/EU on energy efficiency,» Official Journal of the European Union, 2018.

[9] European Parliament and Council, «Directive (EU) 2018/2001 on the promotion of the use of energy from renewable sources,» Official Journal of the European Union, 2018.

[10] European Parliament and Council, «Regulation (EU) 2018/1999 on the Governance of the Energy Union and Climate Action,» Official Journal of the European Union, 2018.

[11] European Parliament and Council, «REGULATION (EU) 2019/941 on the risk-preparedness in the electricity sector,» Official Journal of the European Union, 2019.

[12] European Parliament and Council, «Regulation (EU) 2019/942 establishing a European Union Agency for the Cooperation of Energy Regulators.,» Official Journal of the European Union, 2019.

[13] European Parliament and Council, «Regulation (EU) 2019/943 on the internal market for electricity,» Official Journal of the European Union, 2019.

[14] European Parliament and Council, «Directive (EU) 2019/944 on common rules for the internal market for electricity,» Official Journal of the European Union, 2019.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº 957810

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

[16] 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.

[17] 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.

[18] 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.

[19] National Institute of Standards and Technology Interagency Report (NISITR), «Guidelines for Smart Grid Cyber Security».

[20] CEN Standard, «EN 13757-7:2018: Communication systems for meters - Part 7: Transport and security services,» 2018. [Online]. Available: http://store.uni.com/catalogo/en-13757-7-2018/.

[21] CEN/TR 17167, «Communication system for meters,» 2018. [Online]. Available: https://standards.iteh.ai/catalog/standards/cen/c766700b-a458-4487-b877-73b257be66d2/cen-tr-17167-2018.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº 957810