Innovation Action

inteGRIDy

integrated Smart GRID Cross-Functional Solutions for Optimized Synergetic Energy Distribution, Utilization & Storage Technologies

H2020 Grant Agreement Number: 731268

WP10 – Project Management

D10.10 - Privacy Issues Report & Ethical monitoring

Document Info	
Contractual Delivery Date:	31/12/2018
Actual Delivery Date:	18/12/2018
Responsible Beneficiary:	POLIMI
Contributing Beneficiaries:	ATOS(3), ENG(2), ASSEM(1), E@W(1), AIGUASOL(0,5), UCY(1), PH(1), WVT(1)
Dissemination Level:	Public
Version:	1.0
Type:	Final Version

This project has received funding from the European Union's H2020 research and innovation programme under the grant agreement No **731268**. This report reflects only the author's view and the Commission is not responsible for any use that may be made of the information it contains.

Document Information

Document ID:	**D10.10 - Privacy Issues Report & Ethical monitoring**
Version Date:	21/12/2018
Total Number of Pages:	47
Abstract:	A document that will guide project consortium to comply with EU data protection and privacy principles and regulations along with issues on privacy and security.
Keywords:	*GDPR, DMP, security, privacy, ethics*

Authors

Full Name	Beneficiary / Organisation	Role
Giuliano Rancilio	POLIMI	Overall Editor
Mina Mirbagheri	POLIMI	Overall Editor
Maurizio Delfanti	POLIMI	Overall Editor
Marco Merlo	POLIMI	Overall Editor
Charis Galatsopoulos	CERTH	Contributor
Dimitris Trigkas	CERTH	Contributor
Javier Valiño	ATOS	Contributor
Jorge Landeck	VPS	Contributor
Giuseppe Rana	E@W	Contributor
Christos Roumkos	WVT	Contributor
Jim Fawcett	IWC	Contributor
Alberto Perez	AIGUASOL	Contributor
Massimo Fiori	ASSEM	Contributor
Massacci Enrico	ASSEM	Contributor
Vahid Vahidinasab	UNEW	Contributor
Adib Allahham	UNEW	Contributor
Damian Giaouris	UNEW	Contributor
Vasco Abreu	ENOVA	Contributor
Otilia Bularca	SIVECO	Contributor
Vasilis Mahamid	UCY	Contributor

Reviewers

Full Name	Beneficiary / Organisation	Date
Marilena Lazzaro	ENG	13/12/2018
Christos Roumkos	WVT	17/12/2018

Version history

Version	Date	Comments
0.1	31/10/2018	ToC
0.2	05/12/2018	Draft
0.3	13/12/2018	WP reviewed draft
0.4	17/12/2018	Quality reviewed version
1.0	21/12/2018	Final version to be released to the EC

Executive Summary

inteGRIDy is a H2020 innovation action European demonstration project and aims to integrate cutting-edge technologies, solutions and mechanisms in an integrated framework of tools connecting energy networks with diverse stakeholders, facilitating optimal and dynamic operation of the Distribution Grid (DG) fostering the stability and coordination of distributed energy resources and enabling collaborative storage schemes within an increasing share of renewables.

D10.10 is guiding inteGRIDy Consortium to comply with European Union's (EU) and national regulations on data security, privacy principles and ethical monitoring.

EU regulates in detail the issues of protection and management of data. The regulatory framework is constantly evolving, and its evolution is regularly to be checked to verify compliance. General Data Protection Regulation (GDPR) has entered into force in 2018, becoming the reference rule for protection of personal data in EU. Verifying the compliance with requirements imposed by this regulation is essential for inteGRIDy. GDPR requests that every process of collecting and managing personal data must clearly define what data are collected, who is collecting those, who will have access to data, how long the data will be stored, what is the purpose of data collection and storage. Furthermore, GDPR requests to define a data manager, entitled of the data management process, and to develop Data Protection Impact Assessment (DPIA) in case of clear risk for freedom and rights of people whose data belong.

EU regulation is implemented in national regulatory framework. Consequently, an analysis of the regulation in the countries involved in Pilots is necessary. This allows to understand if EU regulation is in place; if it causes any conflict with national framework; if national regulations present requirements more stringent than EU one.

In addition to regulation, there are some special requirements inteGRIDy must respect being a project within the framework of Horizon 2020. Therefore, it is requested to adhere to EC Open Research Data Pilot. This implies a certain regard in managing data, which materializes in constructing and keeping up-to-date a Data Management Plan (DMP) and providing open access to data, where possible. The up-to-date DMP version is in D10.14. Again, as activity funded by EU, inteGRIDy project must perform Ethics Appraisal Procedure. This allows to verify that, beside scientific merit, every research activity carried out are conducted in compliance with fundamental ethical principles. Procedures requested in Ethics Appraisal go from self-assessment, passing through screening, to ethical complete assessment in case personal sensible areas are involved in the project.

It appears therefore clear the importance of defining whether a project is dealing with personal data or not. Personal data means any information relating to an identified or identifiable natural person.

To define if personal data are processed in Pilots, a survey has been proposed to Pilot Leaders. The list of information asked to Pilots is reported in the following.

- Identification of Data Manager.
- Nature of the data collected, included type of data, duration of the storage, accessibility to data.
- Data security mechanisms in place.
- Definition of personal data collected.
- Data privacy.
- Transparency of the data management process.
- Certification achieved or pursued.

The answers to survey have been collected and are here presented to check compliance with rules by each Pilot. Eventual issues are listed, and a solution is proposed.

Table of Contents

Table of Figures

Table of Tables

List of Acronyms and Abbreviations

Term	Description
CNIL	Commission Nationale de l'Informatique et des Libertés
CNPD	Comissão Nacional de Proteção de Dados
DMP	Data Management Plan
DPD	Data Protection Delegate
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EC	European Commission
ECHR	European Convention on Human Rights
EU	European Union
EV	Electric Vehicles
FAIR	Findable Accessible Interoperable Re-usable
GDPR	General Data Protection Regulation
HDPA	Hellenic Data Protection Authority
OECD	Organisation for Economic Co-operation and Development
PET	Privacy-Enhancing Technologies
PL	Pilot Leader
RDPA	Romanian Data Protection Authority
SME	Small Medium Enterprises
WP	Work Package

1.Introduction

1.1 Scope and objectives of the deliverable

D10.10 report aims to guide inteGRIDy Consortium to comply with EU and national regulations on data security, privacy principles and ethical monitoring. It assesses data treatment processes in place within the Consortium to define the compliance with laws and principles of the project. An analysis and description of the regulatory framework is necessary. Furthermore, the description of Horizon 2020 context is useful to report the further requirements inteGRIDy must respect, being funded by European Commission (EC).

inteGRIDy includes processes of collection and management of both non-personal and personal data. A self-assessment and a screening of the possible issues related to data managed are proposed. By the means of a survey delivered to Pilot Leaders (PL), information related to data treatment are gathered and any issues are highlighted. In case of risks of non-compliance with rules, a solution is proposed and the situation is monitored.

The objective of D10.10 materializes when, after the examination with PL of every Pilot project, all issues are highlighted, a solution to each one is proposed and the situation are kept under monitoring. D10.11 will state the updated state of art.

1.2 Structure of the deliverable

Layout of this report can be outlined as follows.

After the Introduction, Chapter 2 describes in detail the EU and EC regulation on data management. It describes GDPR (2.1) and defines Personal Data (2.2). Then, it faces Data Security issue (2.3); it deals with Privacy Principles (2.4); it describes the fundamental of ethics and Ethical monitoring (2.5).

Chapter 3 describes DMP as a tool for assessing compliance with EU regulatory framework. The definition of the process, its purposes and the responsibilities of that within inteGRIDy framework are highlighted.

Chapter 4 is composed cooperating with PLs and deals directly with national regulation on data management. Each and every PL taking part to inteGRIDy has been interviewed and they have proposed the description of his own national regulatory framework, defining in particular the relevant rules for inteGRIDy. Eight paragraphs describe national regulation for eight countries involved in inteGRIDy Pilots. This process was necessary to define the level of implementation of EU regulation at a national level.

Chapter 5 represents the core of the process of interview of the organizations leading each Pilot. After a recap of the general framework in which inteGRIDy takes place, paragraph 5.1 describes a survey that T10.3 proposed to PLs. The answers to the survey are collected and presented in paragraph 5.2. In paragraph 5.3 and subparagraphs the main outcomes of the surveys on regulation compliance by Pilots are reported. Eventual issues on data management process by any Pilot are here listed and the solution is proposed.

Chapter 6 includes the conclusions.

1.3 Relation to Other Tasks and Deliverables

D10.10 is edited by T10.3 for guiding Consortium to comply with EU regulation on data security and privacy. This means it works in parallel with the development of DMP. Last version available of DMP is D10.14. This version is the main source of the survey proposed in this report. In particular, it works as an update of that survey, modified in order to comply with requirements of regulation.

D10.10 refers to WP4 work since it includes the inteGRIDy Security Access Control Framework. D4.6 will present the report of that framework.

Finally, this document also inherits the work on privacy and ethics started by the Consortium at proposal time, as section 5 in inteGRIDy proposal presented a preliminary approach to national regulations and pilot envisaged plans, that are further updated and extended in this report.

D10.10 is edited in M24 (End of 2018) and it will be updated by D10.11 in M48 (End of 2020).

2.EU legal framework for Data Management

inteGRIDy's proposed solutions do not expose, use or analyse personal sensitive data for any purpose. However, the inteGRIDy Consortium is aware of the privacy-related implications of gathering data. The Consortium is composed by entities experienced in working with these issues. In the following section, the framework in which inteGRIDy moves will be presented and analysed.

The operation of smart grids is related with the collection and use of data. EU legal framework concerning data management is evolving and improving to cope with the constantly increasing amount of data shared and used by businesses and service providers. The backbone of this regulation has been the Council of Europe's *Convention for the protection of individuals with regard to automatic processing of personal data* [COE81], signed in 1981. It defined as a legal imperative, the right to privacy. The *Data Protection Directive* or *ePrivacy Directive* (95/46/EC) [EUP95] regulated the processing of personal data within EU since 1995. In 2002, EU adopted *Directive on privacy and electronic communications* (2002/58/EC) [EUP02] to ensure right to privacy among Member States particularly in electronic communication sector. In 2018, after many years of discussion and after approval in 2016, *General Data Protection Regulation* (GDPR) [GDP16] entered into force. It repealed Data Protection Directive, becoming the main reference for data processing in EU and extra-EU data export.

Lastly, it has been announced that *ePrivacy Regulation* will repeal ePrivacy Directive and enter into force as *lex specialis* to GDPR. It will implement stronger rules for electronic communications and align the legislation in this field to the rules introduced by GDPR. The updated D10.11 will deal better with the definitive version of this regulation and its impact on inteGRIDy.

GDPR defines as a principle that data management can be only performed after explicit consent by individuals under observation. These individuals must be aware of the nature of data collected, the entity who is handling the data and with whom the data will be shared, the purposes for the use of these data and the duration of the storage. The consent must be specific (on data and on purpose), freely-given, unambiguous. Data protection by design and by default must be assured by data collector.

Therefore, collection and management of data arise a series of issues to cope with. The following three pillars will be analysed in the Section.

- **Data Security**

Collected data must be safely managed and stored. Data protection by design and by default must be provided. This means that these issues must be faced within the phase of development of the business process. The data must be accessible only to entities defined in the request for consent of data collection and use. To do this, data will be stored in secure server systems. Data breaches must be notified to individuals under observation. If necessary, Privacy-Enhancing Technologies (PET) must be adopted to ensure protection from data breaches.

- **Privacy**

Since inteGRIDy does not deal with personal sensitive data, data processing must be anonymous and unobtrusive. To do this, data collected will be anonymised. Only key personnel from pilot partners will possess key for re-identification. No data will be sold or used for any purposes other than the current project. To ensure anonymity of data collection, privacy-preserving sensors will be used where necessary. Consent will be asked to users for every data collection operation. The consent procedure will be carefully determined and managed by Pilot-Specific Work Packages (WP) in order to comply with the regulation.

- **Ethical Monitoring**

Every information about data processing will be provided to individuals under observation. Written description of the pilots in which they are involved will be proposed and made available in their own language. The data stored will be only the relevant ones and they will be stored only for the period necessary to the project, communicated at the moment of consent.

2.1 EU Regulation 2016/679: General Data Protection Regulation

A description of the EU regulation on data management necessarily starts with an elaboration on the main code regulating the matter in the EU.

In January 2012, EC presented a proposal on the personal data protection and security. After a lengthy negotiation process, the legislative initiative resulted in the adoption of **EU Regulation 2016/679** [GDP16] of the European Parliament and Council of 27 April 2016 on the protection of individuals with regard to personal data treatment and free movement. This normative instrument, known as the **General Data Protection Regulation** and hereinafter referred to as **GDPR**, has been specially created to protect the citizens against the personal data treatment on a large scale by any type of entity.

The GDPR repealed the previous **Directive 95/46/EC** and, starting from 25 May 2018, is applicable in all EU Member States. However, it does not mean that all the regulations and requirements stated in the previous Directive were repealed. In fact, there are many situations of the previous Directive continuity, and some key definitions have not been affected.

However, the GDPR establishes more stringent rules regarding the treatment of special categories of personal data, for example, racial & ethnic origin, political opinions, religious or philosophical beliefs or information related to the health and sexual orientation. It establishes also the conditions under which the data treatment can take place. According to the Article 6 of GDPR (Lawfulness of Processing), the personal data treatment is allowed if at least one of the following situations occurs:

- data owner has given his consent to his personal data treatment for one or more specific purposes;
- data treatment is necessary for agreement celebration;
- data treatment is necessary for a legal obligation fulfilment;
- data treatment is necessary for the data owner vital interests defence;
- data treatment is necessary for the performance of functions of public interest.

Concerning the personal data transfer to third parties or international organizations, the criterion of ensuring the appropriate level of protection remains in place.

According to the Article 15 of the GDPR (Right of access by the data subject), the personal data owner has the right to require from the responsible for the data treatment the confirmation concerning the personal data that is being used and has the right to always access his personal data and the following information:

- the purpose of data treatment;
- the categories of personal data;
- expected period for the personal data retention;
- the existence of the right of the data owner to ask the responsible for the data treatment to change / erase or limit the personal data treatment.

According to the Article 17 of GDPR (Right to erasure), the personal data must be deleted if it is no longer necessary for the purpose for which it was collected or proceeded.

Moreover, the GDPR establishes rules on sanction law, significantly increasing the maximum penalty rates.

One of the novelties provided by GDPR is the introduction of the extra-territorial influence of the GDPR. For example, a company that is not situated in EU (for example is situated in USA) but sells the goods to a consumer in EU, is obliged to respect the GDPR rules. In addition to this, unlikely the previous Directive, the definition of consent began to demand an unequivocal positive act, ruling out the possibility of tacit consent. The GDPR allows the Member States to define the age at which children can have access, without the consent of their legal representatives, to the direct provision of information that varies between 13 – 16 years.

GDPR introduces the designation of Data Protection Officer (DPO) who replaces the previous control realised by control authorities. The DPO shall have the independent status within the organisation and shall be designated in accordance with its skills and knowledge of Law and data protection & security.

According to the GDPR, the majority of the organizations that treat or stores large amount of personal data, must appoint a Data Protection Officer (DPO). For what concerns the companies, they are required to designate a DPO only in case if they treat the sensitive data or data relating to criminal convictions and large-scale infringements (Articles 9 - Processing of special categories of personal data, and 10 - Processing of personal data relating to criminal convictions and offences). It is necessary to publish the contacts of the DPO and to inform the data holders of those contacts when giving them the information referred to the Articles 13 (Information to be provided where personal data are collected from the data subjects) and 14 (Information to be provided where personal data have not been obtained from the data subject) of GDPR.

The GDPR admits that associations or other representative bodies of companies can designate a common DPO. Also, within the same business group, it is possible to designate a single DPO, if he is easily accessible from each facility. The DPO does not need to have any certification to perform his duties. The DPO should be designated on the basis of its professional qualities and, in particular, its knowledge and skills in the field of law and data protection.

2.2 Personal data

Since GDPR applies on personal data treatment, a shared and unique definition of what is personal data appears necessary.

Paragraph 1 of Article 4 of GDPR defines personal data as follows: "'*personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*" [EUC18].

Given the definition above, in different circumstances, the same data could be personal or not. In a restricted bunch, data before not considered personal, can be used to narrow down the number of people to such an extent that an individual identity can be established. On the contrary, data that has been rendered anonymous in such a way the individual is no longer identifiable, cease to be considered personal data [EUC18].

Therefore, applicating the definition to inteGRIDy framework, a set of data describing personal energy consumption, even if gathered in a small group and even if not associated to a personal number, can become personal data if they allow to identify the individuals. Therefore, a specific consent is requested. Otherwise, anonymization of those data is enough to no more define them as personal data: specific consent is no more requested.

2.3 Data Security

Data security is provided by design and by default (GDPR, Article 25) in inteGRIDy, as regulation requests. The main references are the GDPR and the Article 4 of the Directive 2002/58/EC (ePrivacy Directive). The ePrivacy Directive states that every organisation providing a publicly available electronic communications service must ensure a level of security appropriate to risk presented. To do this, technical and organisational measures must be taken. Moreover, the provider of electronic communications service must inform the subscribers in case of risk of a breach in the security and of any possible remedies.

GDPR adds that the data protection measures required must be designed in the development of the business processes (security by design and by default).

Furthermore, DPIA must be conducted in case specific risks occur to the rights and freedom of data subjects (GDPR, Article 35).

All data collected in inteGRIDy are stored in data repositories where only authenticated personnel can access. Access to data is pilot-specific.

A methodical assessment of security risks followed by their impact analysis is performed. The personal information and data processed by the proposed system, their flows and any risk associated to their processing are subject to this analysis. inteGRIDy Security Access Control Framework is in charge of this procedure, that leads to the foresight and design of the appropriate countermeasures to risks.

The inteGRIDy Security Access Control Framework is included in WP4. D4.6 will present the report of this framework. Within this framework, the design and development of DPIAs will be performed. The key reference for designing DPIAs is the *Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems* [SGT12], developed for EC by *Smart Grids Task Force 2012-14*.

During the inteGRIDy project, responsibilities are clearly assigned for the overall management and control of research findings and the controlling of access rights. The person who is responsible on issues for data security directly informs to the quality board, the ethics helpdesk and the project coordinator.

2.4 Privacy Principles

Under the EU law, personal data is defined as "*any information relating to an identified or identifiable natural person*" [EUC18]. Hence, this section has investigated the EU legal framework for Privacy. It will list the laws in place, in particular:

- Charter of Fundamental rights of the EU (ECHR) [EUC12]: Article 7 and Article 8
- Directive 95/46/EC (Data protection Directive): Article 6-b and Article 7
- Directive 2002/58/EC: Article 5 Confidentiality of the communications
- Directive 2009/136/EC (Cookie Directive) [EUP09]: Article 4

The right to privacy is a highly developed area of law in Europe. All the Member States of the EU are also signatories of the European Convention on Human Rights (ECHR). Article 8 of the ECHR provides a right to respect for one's "private and family life, his home and his correspondence", subject to certain restrictions. The European Court of Human Rights has given this article a very broad interpretation in its jurisprudence.

The Organisation for Economic Co-operation and Development (OECD) issued its "Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy of Personal Data" [OEC99]. The seven principles governing the OECD's recommendations for protection of personal data are in following. All of these principles were incorporated into the EU Directive.

- Notice: data subjects should be given notice when their data is being collected;

- Purpose: data should only be used for the purpose stated and not for any other purposes;
- Consent: data should not be disclosed without the data subject's consent;
- Security: collected data should be kept secure from any potential abuses;
- Disclosure: data subjects should be informed as to who is collecting their data;
- Access: data subjects should be allowed to access their data and make corrections to any inaccurate data;
- Accountability: data subjects should have a method available to them to hold data collectors accountable for not following the above principles.

Directives generally do not directly apply in the EU and associated non-EU countries and need to be nationally implemented by each country through laws and regulations. As countries have some freedom in the implementation of directives, stricter requirements than those prescribed by the directives may apply in certain EU countries. Furthermore, the national data protection legislation is, in many respects, complemented or overlapped by sector specific legislation that also needs to be considered. Therefore, in order to get a clear and comprehensive picture of the data protection requirements, it is essential to check the national frameworks, national data protection laws, unfair competition legislation, telecommunications laws and any other local data protection regulations. As after Automatic Processing of Personal Data in 1981, EC realized that diverging data protection legislation amongst EU Member States impeded the free flow of data within the EU and accordingly proposed the Data Protection Directive.

A crucial aspect of the discussion around personal data processing and protection is related to the deployment of the offered services in a cloud computing environment, as additional risks have to be taken into consideration in this case. The majority of these risks fall within two broad categories: Lack of control over the data, Insufficient information regarding the processing operation itself (absence of transparency).

2.5 Ethical Monitoring

Ethics is an integral part of research, from beginning to end, for all activities funded by the EU. Ethical compliance is seen as fundamental to achieve research excellence. To assess compliance with ethics framework, every project undergoes Ethics Appraisal Procedure [EUC17]. It consists of a self-assessment procedure followed online. It highlights if any risky issue is present among the field faced by the funded research. After self-assessment, a screening is necessary only if there is at least one confirmed ethical issue. If establishing the ethics principles within the issues is considered complex, even a complete ethical assessment could be required.

The ethical framework is analysed in Article 34 of Grant Agreement. In addition, section 5 of the proposal is dealing in a more detailed way with ethics.

inteGRIDy's ethics helpdesk will be put in place for verifying the accomplishment of the requirements for EU funded projects, their impact to business actors and end users before being applied to the pilot sites. This helpdesk undertakes the responsibility for implementing and managing the ethical and legal issues of all procedures in the project, ensuring that each partner provides the necessary participation in inteGRIDy and its code of conduct towards the participants.

Ethical monitoring is reflected in the fact that project participants must be aware of the data collected, the entities that are collecting, the purpose data are collected for, the accessibility and timeframe of storage. Every pilot should provide information about how it is taking in charge this process.

3.Data Management Plan

Following the definition of the main pillars of data management, this section examines the main tool adopted in inteGRIDy for verifying compliance with regulatory framework.

As a project in Horizon 2020 framework (starting from January 2017 on), inteGRIDy is by default part of the *Open Research Data Pilot* [OAI17]. The conditions to adhere to are of ensuring the accessibility to data and develop (and keep up-to-date) a DMP. This DMP shall comprise a description of:

- Handling of research data during and after the project.
- What data will be collected, processed or generated.
- What methodology and standards will be applied.
- If data will be shared /made open access/ how data will be curated and preserved.

A data set template has been disseminated to WP tasks leaders, in order to guarantee the fulfilment of the above criteria. Furthermore, some sections of the DMP are dedicated to data security and privacy within each pilot. Some surveys have been circulated among PL and have been answered. The answers gathered information about data security in each phase of data management, recognition of presence of personal data among collected, data privacy in each phase, auditing mechanisms and certifications achieved by pilots.

DMP assesses FAIR data management. Data management is FAIR, within Horizon 2020 framework, if data are:

- **Findable**, and univocally numbered, with provision of metadata.
- **Accessible** to audience openly. If some data cannot be shared, there should be proper explanation justifying it.
- **Interoperability** among users, researchers, projects. Data should be exchanged without difficulties among different boards.
- **Re-usable**, after being licensed conveniently. Data should be available to third parties, even after the end of the project.

A DMP involves also ethical aspects in the data management.

A DMP can therefore be mentioned as the main tool for assessing compliance with data security and privacy regulation within inteGRIDy. Its creation, developing and regular update, necessary for inteGRIDy board for being compliant with requirements of Horizon 2020, are consequently assessed by T10.3.

inteGRIDy has issued so far 3 differente releases of the Data Management Plan, namely D2.3, D2.4 and D10.14. These documents contain the methodology followed for data gathering and storing, distiguising per WP. It also covers the cyber-security and privacy aspects to be taken into account.

The Data Management Plan reports conducted an analysis of cyber security & privacy issues and consideration of guidelines for security measures. Cyber security and data protection within the EU present a high degree of market fragmentation and there is a variation of policies for the technologies developed. Although the NIS Directive and GDPR in 2018, address this matter, new legislations are needed for information exchange and cooperation on cyber security at cross-border level. Establishing the security of communication and control signals depends on two important measures:

- **Authentication** (who can talk to the device? e.g. communicating with a smart meter).
- **Integrity** (has the information been modified in transit? e.g. a man-in-the-middle attack between the interrogating party and the smart meter).

In addition, these reports also assessed, pilot per pilot, the level of cyber-security and privacy measures implemented and, therefore, that must be taken into account for the Data Management Plan. This was done through a survey requesting the following information:

- **Dataset description**: brief description of the dataset and data flows.
- **Data security** (acquisition, transmission/storage/access): mechanisms/protocols used or available to ensure secure data handling; certifications.
- **Personal data**: ways in which the collected or processed data can becomes personal or "sensitive" considering the recently adopted EU General Data Protection Regulation.
- **Data privacy** (acquisition, transmission/storage/access): mechanism/protocols used or available to ensure data privacy including encryption, anonymization, aggregation.
- **Auditing**: mechanisms used or available to record data processing and handling operations.
- **Certification**: applicable standards and sought certifications already in place or expected in the near future.

The following table summarizes this analysis. The colour code assessment tries to identify the level of awareness perceived for each topic mentioned in the survey Green means that the topic is well understood and addressed already; yellow means that, at least from our interpretation of the available information, the topic may require further consideration; grey means that the topic is not considered relevant.

Table 1. Preliminary Analysis of Cybersecurity and Privacy Survey

Question\Pilot	01	02	03	04	05	06	07	08	09	10
Data security (acquisition, transmission, storage, access)	●	●	●	●	●	●	●	●	●	●
Personal data	●	●	●	●	●	●	●	●	●	●
Data privacy (acquisition, transmission, storage, access)	●	●	●	●	●	●	●	●	●	●
Auditing	●	●	●	●	●	●	●	●	●	●
Certification	●	●	●	●	●	●	●	●	●	●

inteGRIDy Data Management Plan (DMP) is associated with categorisation of the type of data; relevant methodology & standards that apply; the handling, open access and usage; and the Implementation of the data plan. The dataset is assigned with the relevant references, metadata and standards as attributes before a decision on accessibility, storage and archiving is made. H2020 and UK Digital Curation Centre, Joint OpenAIRE and EUDAT webinar guides are followed as guidelines. The figure below shows the application of DMP to the inteGRIDy data generated, accessed and stored.

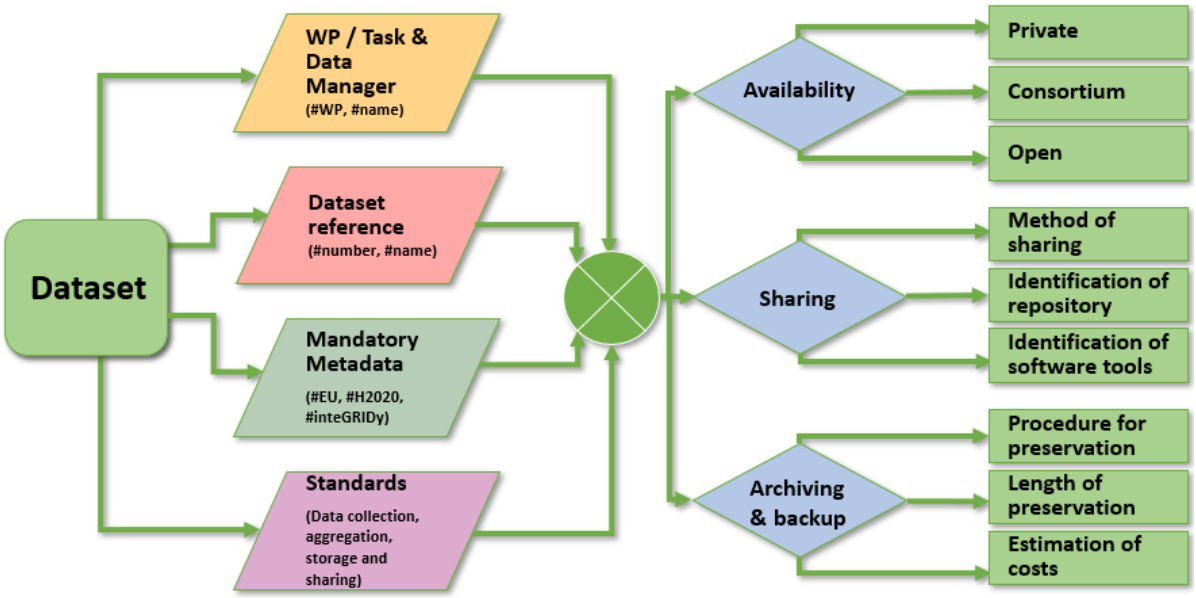

Figure 1. inteGRIDy Dataset Template

Table 2. Dataset Template

WP/Task & Data Manager	Work Package and/or Task numbers related to the dataset, and the Data Manager who takes responsibility.
Dataset reference/name	Dataset number and name
Availability	Private, Consortium or Open
Mandatory Metadata	European Union H2020 integrated Smart GRID Cross-Functional Solutions for Optimized Synergetic Energy Distribution, Utilization Storage Technologies inteGRIDy GA 731268
Dataset Specific Metadata	Keyword(s) that categorize data to make it linked/searchable
Data set description	Data description, origin, nature, scale, if it underpins a publication, who useful to, existence of similar data, possibilities for reuse.
Standards	Reference to existing standards in topic area governing data collection, aggregation, storage and sharing. Adaptation of data set to community standards to maximize interoperability with other researchers. Potential license restrictions. Discoverability. Need for aggregarion and anonymization.
Data sharing	How the data will be shared, identification of repository, existence of embargo period if any, identification of software or tools necessary for reuse. Data sets reused from other inteGRIDy tasks. Use of this dataset by third parties in the future.
Archiving and preservation (storage/backup):	The procedure for long-term preservation, length of preservation, an estimation of costs and how this will be covered.

As described in Figure 1 and Table 2, inteGRIDy collected, per each task in the project, the expected data description to be collected. This is especially relevant in WP6 and WP7, as tasks in those WPs correspond to inteGRIDy pilots.

Within the aspects included in those tables, the following items are relevan to the privacy and ethics analysis:

- **Availability and Data sharing**. This points to whether the dataset is open to third parties, restricted to project members or just used to the owner. This is a potential indicator of privacy issues.
- **Standards**. In case of need to preserve privacy, this field indicated the measures (in the form of adopted standards) taken so as to guarantee it.
- **Archiving and preservation**. How the dataset owner plans to make the data persistent and available to stakeholders while granting the privacy and security needs.

All in all, the Data Management Plan is a very good reference source for assessing the project needs in terms of privacy and security needs, with main items already identified.

4.National legal framework

This chapter will provide an overview of the national legal framework on topic. It will highlight the fact that every EU regulation must be implemented at a national level. An overview of the different level of detail of national regulations and eventual particular issues in any regulation at national level will be here presented. This chapter has been developed in cooperation with PLs and Data Manager of each pilot. These persons are responsible for the data management process carried out within the context of their Pilot.

In detail, the PL is the member designated within inteGRIDy Consortium to be the responsible of the pilot; the Data Manager is the figure who covers the role of the DPO for that pilot. They may be the same person.

4.1 Greece

The Hellenic Data Protection Authority (HDPA) is the National Supervisory Authority responsible for the protection of personal data and privacy of individuals.

Following the revision of the Greek Constitution in 2001, Article 9A was introduced to protect an individual's personal data against unlawful processing. It has also introduced for the first time the right to "informational disposition" as a distinct aspect of the right to privacy, which essentially means a person's right to know, control and decide when and whether his/her personal data are to be collected, processed, or used in any way.

Until the entry into force of the GDPR on the protection of natural persons with regard to the processing of personal data and on the free movement of such data in May 2018, the collection and use of personal data in Greece was regulated by:

- **Law 2472/1997** [GPA97]: it transposed Directive 95/46/EC on data protection (Data Protection Directive) into domestic law.

There were also certain special laws that regulated specific sectors, including:

- **Law 3471/2006** [GPA06]: it regulates the collection and use of personal data in the context of electronic communications and transposed Directive 2002/58/EC on the protection of privacy in the electronic communications sector (E-Privacy Directive).
- **Law 3917/2011** [KAR11]: it regulates the retention of collected/processed personal data and transposed Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (Data Retention Directive).

It is noted that Greece has not yet issued a national law implementing the GDPR.

On 20 February 2018 a draft bill complementing the GDPR was published and made available for public consultation, which ended on 5 March 2018. The competent legislative committee is now evaluating feedback received during the public consultation procedure; an updated version is expected to be submitted soon to the Greek Parliament for approval. Noteworthy provisions of the draft bill include the following [MCK18]:

1. The minor age for consent is set at 15 years.
2. Provisions are introduced for Closed Circuit Television (CCTV) data processing.
3. Provisions are introduced regarding processing in the context of employment. Employees' heath data can only be collected directly from the employee and only if absolutely necessary for (a) evaluation of an employee's suitability for work; (b) compliance with a legal obligation; (c) establishment of an employee's social security rights. Special rules apply for psychological and psychometric tests and also for the processing of criminal records and genetic data.
4. Provisions are introduced regarding processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

5. Criminal sanctions are being introduced for breach of the GDPR provisions including imprisonment of up to five years and fine up to EUR 300,00. Stricter sanctions are envisaged if breach has an impact on national security.
6. A Data Protection Officer who violates his/her duty of confidentiality (as envisaged by the draft bill) can be sanctioned with imprisonment of up to five years and fine up to EUR 100,00.

4.2 The United Kingdom

In the United Kingdom, the Data Protection Act 1998 was replaced by the General Data Protection Regulation [GDP16] and Data Protection Act 2018 [PUK18], in May 2018. This legislation governs how personal data should be handled to protect individuals. Data Controllers are required to maintain personal information at an appropriate level of security to ensure compliance with the legislation.

Personal information is also protected by Article 8 of the Human Rights Act 1998 [PUK98]. The processing of personal information that may infringe this right will only be undertaken where it is lawful, proportionate and necessary to do so.

Organisations and their employees or representatives have a duty to ensure that personal information is not knowingly or recklessly misused, lost or destroyed. Personal information should be stored in secure locations and access restricted solely to relevant staff. A Privacy Notice should be issued at the time of collecting personal data and this will explain why the information is being collected, who the data may be shared with and for how long it will be retained.

Computer systems will be configured, and computer files created with adequate security levels to preserve confidentiality. Sensitive personal data should only be transferred by way of secure electronic transfer.

Personal data, defined as any information relating to an identified or identifiable natural person, should only be shared when the other party has a right to have the data. Data Exchange Agreements should be in place to describe what information will be shared and under what circumstances. It should only be used for the purposes specified and should not be further processed in a manner that is incompatible with those purposes.

Personal data cannot be transferred to a country outside the EU unless that country has an adequate level of protection for the rights of data subjects.

An individual's rights under Data Protection legislation are as follows:

- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure / right to be forgotten.
- The right to restrict processing.
- The right to data portability.
- The right to object.

Under the legislation, Privacy Impact Assessments should be completed at the start of any new project that involves the processing of personal data and are mandatory for any processing that is likely to result in a high risk to individuals' interests.

4.3 Spain

On the 6th of December 2018, the Organic Law 3/2018 on the Protection of Personal Data and guarantees of digital rights [BOE18] entered into force. It adapted the Spanish legislation to the EU GDPR. This Law regulates the relative protection of individuals regarding personal data handling and free movement of data.

This law repeals the previous Organic Law 15/1999 [BOE99] and Royal Decree-law 5/2018 [BOE02]. However, the provision 14 of the Organic Law 3/2018 states that articles 23 and 24 of the Organic Law 15/1999 are still in force.

The following provisions can be noted:

- The duty of confidentiality is included, both for the data controller and for anyone who intervenes in the process. This obligation is maintained even when the relationship with the person in charge or in charge of the treatment has ended.
- The explicit consent of the owner of the data is necessary in order to collect and use them.
- The owner of personal data has the right to know who is responsible to process his information, and must have access, easily and immediately, to them.
- In order to avoid discriminatory situations, it will not be possible to deal with data whose purpose is to identify the ideology, union affiliation, religion, sexual orientation, beliefs or racial or ethnic origin, even if the person affected gave their consent.
- Right to know what purpose the data are going to be used for and the use terms.
- Right to request the suspension of the processing of your data, the conservation and the portability of the same.

The figure of the Data Protection Delegate (DPD) is introduced. The DPD will act as the interlocutor or the person in charge of the treatment before the Spanish Data Protection Agency and the regional authorities of data protection. There is an obligation to appoint a DPD in three cases:

- If the data is processed by a public authority or body.
- If the main activities and operations of the data controller require regular and systematic large-scale monitoring.
- If the main activities and operations require large-scale processing of personal data related to crimes and convictions.

4.4 Italy

In Italy, as in all EU Member States, from 25 May 2018, GDPR is directly applicable, replacing entirely the previous rules (Italian Legislative Decree 30 June 2003, 196).

This Regulation applies to all Member States of the EU, as well as to all those who operate in the territory even if they do not have their registered office within EU, and its objective is to protect natural persons with regard to the processing of their personal data and to the free movement data protection.

The GDPR establishes that personal data shall be protected following some basic key processing principles; “personal data shall be:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);
- accurate and, where necessary, kept up to date;
- 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;
- processed in a manner that ensures appropriate security of the personal data.”

The new European regulation regulates, in particular, the “processing of personal data”, that is every operation performed with or without automated methods, concerning that data. Any intervention, from collection to registration, from storage to modification, from extraction to consultation, use, dissemination or any other form of making available, comparison or interconnection, limitation, cancellation or destruction is within the scope of the definition of data processing.

As part of the processing of personal data, in the EU Regulation two important figures are defined in addition to the natural person ('data subject'): the data controller and the processor. Very briefly, "controller" means the natural or legal person, which determines the purposes and means of the processing of personal data. "Processor" means a natural or legal person which processes personal data on behalf of the controller, typically when the amount of data is such that the controller must necessarily entrust other subjects for the management of the same.

It is clear that between the data controller and the data subject a well-defined and regulated relationship must be established; the instrument provided for by the GDPR is the so-called "consent" to treatment, meaning any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

As already mentioned, the GDPR has the objective of protecting personal data of the person concerned, and to do so has imposed specific obligations to the data controller, including providing the data subject with a concise, transparent and comprehensible information, with the aim of allowing the same to understand all its rights regarding the processing of its personal data.

Between the rights of the data subject we mention:

- access right;
- the right of rectification;
- the right to cancel;
- the right to limit the processing;
- the right to portability.

Finally, the European Regulation on personal data processing provides a special category, the "sensitive data", imposing a general prohibition of treatment of them while providing numerous exceptions. For the sake of completeness of information, sensitive data are considered personal data that reveal racial or ethnic origin, political opinions, religious or philosophical convictions, union membership, as well as genetic data, biometric data intended to identify univocal a natural person, data relating to the health or sexual life or sexual orientation of the person.

4.5 France

On May 25, 2018, the GDPR came into effect in France. Many formalities that were present with the previous responsible organization, the Commission Nationale de l'Informatique et des Libertés (CNIL), disappear. In return, the responsibility of the organizations is strengthened. They must now ensure optimal data protection at all times and be able to demonstrate it by documenting their compliance.

France implemented GDPR to repeal every previous regulation on personal data treatment. Some hints are suggested to organization from CNIL to comply with GDPR. The ones useful to understand the transition among the previous regulatory framework and the GDPR are listed in the following.

Until 2018, a "computer and freedoms correspondent" can be designated in France, who will act as DPO and will organize the actions to be taken.

To concretely measure the impact of the European data protection regulation that an organization is dealing with, it must start with a precise inventory of personal data processing. The development of a register of treatments allows the organization to take stock.

4.6 Portugal

4.6.1 Personal Data Management (Security & Privacy) in Portugal

In Portugal, the current Data Protection Law (**Law 67/98 of 26 of October**) continues to remain in force (even after 25 May 2018) in the topics that do not contradict the GDPR, until the national legislation implementing GDPR repeal it. In spite of the GDPR being an EU regulation, it presents a significant set of rules that require the national legislature to intervene.

There was proposed a draft **Law Nr. 120/XIII** on March 22, 2018 that guarantees the execution of the GDPR in order to provide the most appropriate solutions for the rights and freedoms protection of personal data owners in Portugal [PCM18]. However, it has not been officially accepted yet.

4.6.2 Legislative evolution of personal data protection in Portugal [CNP17]

In Portugal, the entity that deals with personal data protection is the National Data Protection Commission (in Portuguese "*Comissão Nacional de Proteção de Dados – CNPD*"). The CNPD controls and supervises the compliance of GDPR, as well as other legal and regulatory provisions concerning the personal data protection in order to defend the rights and freedoms of natural persons always when the personal data is proceeded.

The Commission began its first activity in January 1994. Its first designation was the National Commission for the Protection of Personal Computer Data (in Portuguese "*Comissão Nacional de Proteção de dados Pessoais Informatizados – CNPDPI*"). In 1976, the Portuguese Constitution defined the personal data protection as a fundamental right (Article 35 – Informatics usage). However, only 15 years later, the first data protection law was approved – **Law 10/91 of 29 April**, and there was created CNPDPI. The law has undergone some changes with **Law 28/94 of 29 of August**, which approved the measures to strengthen the personal data protection, when the Commission has already started operating.

In 1995, the **Directive 95/46/EC** of the EU Parliament and of the Council of 24 October, 1995 was published on the protection of individuals with regard to the personal data treatment and free movement in EU Member States. According to this directive, the Member States were given three years to transpose this directive into the national law.

In 1997, some changes were made in the Articles 35, in order to allow an adequate transposition of the Data Protection Directive. In the reformulated Article 35, the Commission has constitutionally consecrated its existence as an independent administrative entity.

In 1998, a new Personal Data Protection Law – **Law 67/98 of 26 of October**, transposing the Directive 96/46/EC, was approved, substantially enlarging the power range of the Commission, which has since passed to be called CNPD – National Commission of Data Protection.

At the same time, the Law 69/98 of 28 of October passed to regulate the protection of personal data in the telecommunications sector, transposing the so-called Telecommunications Directive (Directive 97/66/EC) and attributing the CNPD the competences in this area.

The EU Regulation **2016/679 of 27 of April** repeals the EU Directive **95/46/CE of 24 of October**. At the time being, the Portuguese Personal Data Protection Law (**67/98 of 26 October**) remains in force until the new Law (transposed from the EU Regulation 2016/679 of 27 of April) being accepted.

4.6.3 GDPR and its transposition to the Portuguese Law [PCM18]

The GDPR introduced several novelties in personal data treatment and privacy. Its transposition to the Portuguese law has been accomplished. Some peculiarities are listed in the following.

According to the Article 11 (Data Protection Officer functions) of the Portuguese Draft Law, the major functions of DPO are the following:

- to guarantee the execution of audits both periodic and non-scheduled;
- to sensitize the users of the importance of timely detection of security incidents and the need to inform the DPO immediately whenever malware has been detected;
- to ensure the relations with the data owners in matters covered by GDPR and national data protection legislation.

With regard to the accreditation and certification planned in the GDPR, it is attributed to the Portuguese Institute for Accreditation – the competence to accredit the certification bodies which are responsible for the certifying procedures.

With regard to the consent of minors to access the information society services, according to the Section V (Special provisions) of the Article 16 (Minors´ consent) of the Portuguese draft law, the age of 13 is considered to be appropriate, in line with others EU Member States. It is also determined that in case of the minors who are less than 13 years old, the consent must be provided by the respective legal representatives.

When determining the penalties for non-compliance of GDPR, the Portuguese Data Protection Entity, CNPD takes into account, the criteria established in Article 39 (Penalty determination) of the Portuguese Draft Law:

- The economic situation of the agent in case of a natural person, or the turnover and the annual balance in case of the legal person;
- The size of the entity, taking into account the number of employees and the nature of the services provided;
- The continuing nature of the infringement.

In accordance with Article 33 of the GDPR (Communication of a personal data breach to the data subject), in the event of breach of personal data, the communication procedures to the supervisory authority must be the following: The DPO shall notify the competent control authority (in Portuguese case: CNPD) within 72 hours about the breach of the data.

According to the Article 52 (Disobedience), whoever fails to comply with the obligations set by GDPR and the Portuguese Draft Law, after exceeding the period established by the CNPD for compliance, shall be punished with a prison sentence of up to one year or with a fine of up to 120 days.

According to the Section VIII (Final and transitional provisions) of Article 64, the Portuguese Draft Law nr. 120/XIII was approved in the Council of Ministers on March 22, 2018 and shall enter into force on the day following its publication.

4.7 Romania

The Romanian Data Protection Authority (RDPA) is National Supervisory Authority for Personal Data Processing [DPA17] and the applicable legislation is:

- Law 190/2018 [DPA18] measures of applying 2016(UE)/679 GDPR [GDP16].
- Law no. 129/2018 [NAP18] for amending and supplementing the Law no. 102/2005 on the establishment, organization and functioning of the National Supervisory Authority for Personal Data Processing, as well as for repealing the Law no. 677/2001 on the Protection of Individuals with regard to the Processing of Personal Data and the Free Movement of such Data.
- Law no. 677/2001 [PPD01] on the Protection of Individuals with regard to the Processing of Personal Data and the Free Movement of Such Data, amended and completed.
- Law no. 506/2004 [ELC04] on the processing of personal data and the protection of privacy in the electronic communications sector.

- Law no. 298/2008 [ELC08] on the retention of data generated or processed in connection with the provisions of publicly available electronic communications services or of public communications networks and for the amendment of Law no. 506/2004 on the processing of personal data and the protection of private life within the electronic communication sector.

Following 25th of May 2018 when GDPR came into force in the EU, the Romanian Parliament and the RDPA initiated acts to implement data protection in Romania.

Law No. 129/2018 [NAP18] for amending and supplementing the Law No.102/2005 regarding the establishment, organization and functioning of the National Supervisory Authority for Personal Data Processing, and for repealing the Law No 677/2001 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data was published on 19 June 2018 in the Official Gazette of Romania No. 503/19 June 2018. Under Law No. 129/2018 [NAP18], the powers of the RDPA to oversee the implementation of the GDPR in Romania have been strengthened, with the RDPA being granted the right to conduct unannounced investigations at controller or processor premises; in cases of obstruction, the RDPA is entitled to obtain a judicial authorization from a Bucharest Court of Appeal judge to enter such premises, without any prior summoning. Furthermore, under Law No. 129/2018, the maximum number of employees of the RDPA was increased from 50 to 85. The representatives of the RDPA has the right to conduct investigations on the spot both or request end by datacontroller/ processor during working hours. Also, Law No. 129/2018 sets the administrative fine, its applications and certain corrective measures.

Law No. 129/2018 repeals, as of 25 May 2018, Law No 677/2001 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

Below, the list of the most relevant principles and the national legislation Law no. 677/2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data:

- Grounds for processing
- Sensitive Personal Data
- Data Quality Principle
- Data Retention
- Data Subject Rights
- Data Transfer
- Notification Obligations
- Security

The Romanian Parliament also adopted Law No. 190/2018 [DPA18] on the measures for implementing the GDPR (Law No. 190/2018), effective as of 31 July 2018, and relating to the measures necessary for the implementation of certain provisions of the GDPR at national level, such as: processing of genetic, biometric or health concerning data, processing of a national identification number, processing of personal data in an employment context, or the sanctions procedure applicable to public authorities in case of a GDPR breach. Law No. 190/2018 allows the public authorities to appoint a sole data protection officer, and provides for such authorities, acting as controller or processor, to face a two-tier sanctioning system, which includes an initial written warning and remedy plan to be completed in no longer than 90 calendar days.

In addition, the RDPA enacted Decision No. 99/2018 [DEC18] (effective as of 25 May 2018) which allowed for further GDPR implementation measures to be adopted into Romanian law. Decision No. 99/2018 repealed 17 regulations issued by the Romanian Ombudsman between 2002 and 2015, which at that time allowed for the implementation of the Data Protection Directive 95/46. Also, RDPA Decision No. 133/2018 [DCE18] allows a data

subject to draft a complaint in either the Romanian or English language for submission to the RDPA, in relation to an alleged breach of the GDPR provisions.

4.8 Cyprus

The GDPR is a EU law which became directly applicable law in Cyprus, like in all other Member States of the EU, on 25 May 2018. In Cyprus, the GDPR gives national data protection authorities greater powers of enforcement, with the potential for significant fines for regulatory infringement and increased litigation risk arising from aggrieved data subjects.

The GDPR provides for certain areas where Member States could determine and further set exceptions within the articles of the GDPR. Because of this, Cyprus has put in place a GDPR implementation law. Cyprus' Protection of Natural Persons Against the Processing of Personal Data and the Free Movement of this Data Law 125(I) of 2018 [CHR18], in some manner implements elements of the GDPR, and in another, it could be viewed as ancillary and supplementary to it. The legislation enacted by Cyprus sets out particular rules for certain processing situations and creates criminal offences for infringement of statutory provisions.

The data protection legislation in Cyprus takes into account the protection of information provided by both natural persons and legal entities on the Cypriot territory. The local authorities have created the legislation with the purpose of providing a legal framework which will protect the legal rights of the natural persons and legal entities in Cyprus. It provides a comprehensive image on the ways in which personal data can be collected, processed and transferred. The main authority which controls the enforcement of the data protection law is the Office of the Commissioner for Personal Data Protection.

The legislation provides a clear understanding on what personal data means, which represents all types of information related to the private life of a person, such as the home address or personal phone number, the bank account, e-mail address and many others.

The legislation also prescribes definitions of the "sensitive data". The term refers to personal information related to a persons' ethnicity, political orientation, health, sexual orientation or religion.

Legal entities which act as data controllers in Cyprus are required to register with the Office of the Commissioner for Personal Data Protection and the procedure is compulsory for all types of data controllers. The respective entity must provide details on the business address, the main reasons for which the data must be collected, the period in which such information will be collected and many others. Data can be collected in Cyprus only if the respective companies or institutions provide evidence referring to the persons' consent on such actions.

5.Data Treatment in Pilots

The scope of this report and of the procedure adopted is, as already described, guiding inteGRIDy project and the Consortium to comply with EU regulation on data protection and privacy principles, along with facing issues in these fields encountered from pilots.

EU regulation asks businesses dealing with electronic communications to ensure data security by design and by default. This means, as previously mentioned, that the risks involved in data management must be recognized in design phase. Convenient procedures and mechanisms must be put in place to prevent and cope with menaces.

Privacy principles must be guaranteed in managing data. Since no personal data are involved in inteGRIDy, the level of risk is low. In any case, accessibility to data will be kept as restricted as possible. This implies a relationship among the type of data and its storage facility, implemented in inteGRIDy archives by design. As described in D10.14, if speaking of accessibility, there are five types of data. To each category of data is dedicated a storage facility designed on purpose. In detail, *Private data* are stored locally by organisational assets. *Consortium data* are stored in common space hosted by ATOS IT services. Open data will be stored in three different facilities. The project website http://integridy.eu/, managed by ATOS, is the first asset for serving public dissemination. Atos repository is used for scientific publications discoverable in the mode of “green” open access publishing. Open data repositories selected by each task leader will be used to host large and re-usable data sets.

This way of subdividing data based on their accessibility, along with protocols used for guaranteeing data security, is used to comply with privacy principles stated by EU regulation.

As stated before, inteGRIDy is interested in spending the largest effort to carry on the project within an ethical framework. This is, as said, a requirement for every EU funded project. Ethics is checked by assessments involving the pilots’ and the task forces’ operation. To comply with regulation for EU funded projects, the inteGRIDy project is consulting Ethics experts e.g. for assessment phase. Transparency in the process of data collection and management is the pillar of inteGRIDy compliance with ethical principles.

5.1 Survey to Pilots

To check the compliance of the pilots with rules and principles stated previously in this document, WP10 have circulated surveys to PL. The aim is updating data already collected during D2.3 and D10.14 accomplishment and gather some other information needed for defining pilots’ compliance with EU regulation.

The template of the survey circulated is shown in Table 3.

Table 3. Template of survey to pilot projects

Pilot & Data Manager	
Dataset description: *(brief description of the dataset and data flows. Type of data, accessibility of data, timeframe of storage)*	
Data security (acquisition, transmission/storage/access): *(mechanisms/protocols used or available to ensure secure data handling; certifications)*	

Personal data: *(ways in which the collected or processed data can become personal or "sensitive" considering the recently adopted EU General Data Protection Regulation)*	
Data privacy (acquisition, transmission/storage/access): *(mechanism/protocols used or available to ensure data privacy including encryption, anonymization, aggregation)*	
Data management process transparency: *(mechanisms used or available to notify individuals whose data is collected about: entities collecting data, purpose, type of data stored, accessibility of their data, timeframe of storage)*	
Certification: *(applicable standards, regarding both privacy and cybersecurity, and sought certifications already in place or expected in the near future)*	

Each cell of the table has been filled to return the following information.

Dataset description: it aims to gather information on what kind of data are collected, where they come from, who they will be accessed from, how long they will be stored. This is to define the nature of data collected.

Data security (acquisition, transmission/storage/access): it aims to describe the security protocols and mechanisms used in every step of the management process. It is useful to define the compliance of the process with principles of security by design and by default requested. On the other hand, it can be used to identify undetected risks by Pilot managers.

Personal data: since personal data are the most sensible to EU security and privacy regulation, this cell gathers information on whether or not a pilot is dealing with personal data. Personal data are the ones allowing to identify the individual under study. It is known by PL that energy consumption data in a small group can become personal data. On the contrary, anonymous or anonymized data are no more personal data. GDPR requires consent freely-given, in "opt-in" form and unanmbiguous in case of collection of personal data. No consent needed otherwise.

Data privacy (acquisition, transmission/storage/access): it aims to define accessibility to data by third parties in every phase of the process. If any mechanism for guaranteeing only partial accessibility or anonymization of data is in place, it must be declared here. This cell aims to define the compliance of the process with privacy principles.

Data management process transparency: it aims to define if any mechanism to guarantee awareness of people whose data is collected is in place. Transparency of the process is the main tool for guaranteeing ethical monitoring. This cell is stating whether the Pilot is complying with ethics framework of inteGRIDy.

Certification: it aims to define if any standard is followed in the framework of the Pilot. Compliance with a standard and achievement of a certification could by itself indicate the compliance of the Pilot with regulation.

Once received, the answer to surveys are analysed to check compliance to rules. The accomplished surveys and any eventual comment are listed in the following paragraph.

5.2 Answers to survey

Surveys have been submitted to Pilots, whose answers are listed here below:

Table 4. Isle of Wight Pilot answers to the survey

Pilot & Data Manager	**Isle of Wight - Tom O'Reilly (Siemens)**
Dataset description: *(brief description of the dataset and data flows. Type of data, accessibility of data, timeframe of storage)*	Lifetime total KW/hrs, Time of day, cooling set points and dead bands, pumping set points and dead bands, fan KWH, Air Handling Unit Kw, Fan Coil Units KW, Variable Frequency Drives % output, Variable Frequency Drives KWH, Variable Speed Drives % output, Variable speed Drives KWH, Temperature, Pressure, (ON/OFF) status or stage, Flow rate of air, Alarm state, Current Power demand (kW), Energy consumption (kWh), Revolutions per minute (RPM), N2EX market prices, Ancillary Market Prices
Data security (acquisition, transmission/storage/access): *(mechanisms/protocols used or available to ensure secure data handling; certifications)*	The Siemens system will establish a secured communication link the virtual server hosted by AWS. A VPN terminator will be deployed within IOW infrastructure which will create IPSec VPN tunnel and provide a layer of security to the connectivity between Siemens and the subsystem. White-lists will be implemented to ensure only those servers and devices that should be able to talk to one another can, and no others.
Personal data: *(ways in which the collected or processed data can becomes personal or "sensitive" considering the recently adopted EU General Data Protection Regulation)*	None
Data privacy (acquisition, transmission/storage/access): *(mechanism/protocols used or available to ensure data privacy including encryption, anonymization, aggregation)*	User access is built around CAS and uses the following security access control methods: Authentication, Authorization & Encryption. Authentication, validation of the credentials (i.e. password) determines the authenticity of the user.
Data management process transparency: *(mechanisms used or available to notify individuals whose data is collected about: entities collecting data, purpose, type of data stored, accessibility of their data, timeframe of storage)*	None

Certification: *(applicable standards, regarding both privacy and cybersecurity, and sought certifications already in place or expected in the near future)*	Centralised certificate management process to manage device certificates is not part of the solution.

Table 5. Terni Pilot answers to the survey

Pilot & Data Manager	**Terni – DPO: Giovanni Gaudino (dpo@asmterni.it)**
Dataset description: *(brief description of the dataset and data flows. Type of data, accessibility of data, timeframe of storage)*	In Terni Pilot site, real time data are collected from the field and sent to the internal server at ASM LAN. Main data stored/collected in the KRW are: microgrid load profiles requested by the DSO; measurements from microgrid (loads, generators and storage system); microgrid optimization plan as computed by CMP.
Data security (acquisition, transmission/storage/access): *(mechanisms/protocols used or available to ensure secure data handling; certifications)*	Devices and CMP authenticate and authorise each other's by means of their static IP address. Data collected from the field layer are transferred to the CMP over internet, most probably a secure VPN tunnel will be used.
Personal data: *(ways in which the collected or processed data can becomes personal or "sensitive" considering the recently adopted EU General Data Protection Regulation)*	Processed and stored data can be considered as personal data since they represent personal behaviours and sensitive information. Data leak causes the sharing of microgrid personal data.
Data privacy (acquisition, transmission/storage/access): *(mechanism/protocols used or available to ensure data privacy including encryption, anonymization, aggregation)*	Field devices cannot handle encrypted data, so encryption/decryption must be done by the DSO server. Moreover, data are stored in DB located in the local private network not accessible to unauthorised personnel
Data management process transparency: *(mechanisms used or available to notify individuals whose data is collected about: entities collecting data, purpose, type of data stored, accessibility of their data, timeframe of storage)*	In Terni, there is only one individual responsible for the pilot who is already aware of the data gathering during the project, by a previous agreement. For this reason, notification will not be implemented.
Certification: *(applicable standards, regarding both privacy and cybersecurity, and sought certifications already in place or expected in the near future)*	Devices and CMP authenticate and authorise each other's by means of their static IP address, moreover, a VPN tunnel will be implemented.

Table 6. San Severino Marche Pilot answers to the survey

Pilot & Data Manager	**San Severino Marche - Massimo Fiori (ASSEM)**
Dataset description: *(brief description of the dataset and data flows. Type of data, accessibility of data, timeframe of storage)*	**The Pilot 3 data set will include, in detail:** • the **power profiles collected on active users** (PV and hydro plants, etc). These data will be accessible to the DSO and will be archived over a long period of time (years). • **measurements collected on MV network** (active and reactive power flow, voltage profiles, currents, etc.). These data will be accessible to the DSO and will be archived over a long period of time (years). • **power exchange of energy storage systems** involved in the pilot project. These data will be accessible to the DSO and the end user involved and will be archived over a medium period (months) for the user, and over a long period of time for the DSO (years). • **weather data acquired by a web service provider** (solar radiation, humidity, temperature, etc.). These data will be accessible to the DSO and will be archived over a long period of time (years). • **historical time series relevant to the MV and LV load on the network.** These data will be accessible to the DSO and will be archived over a long period of time (years). • **electrical parameters of electrical MV lines and HV/MV transformers.** These data will be accessible to the DSO and will be archived over a long period of time (years). • **grid topology, in terms of network structure, substations and lines localization.** These data will be accessible to the DSO and will be archived over a long period of time (years). • **data collected from electrical market.** These data will be accessible to the end user and will be archived over a short period of time (days).
Data security (acquisition, transmission/storage/access): *(mechanisms/protocols used or available to*	The data collected by the distribution network and by active users are transmitted following the IEC 60870-5-104 protocol through the LTE network which provides dedicated APN

ensure secure data handling; certifications)	and SIM authentication. The data of the Zhero system are transmitted by the UNE webserver to the ASSEM workstation through an API catalogue. The data of the Zhero system in the field (user side) are transmitted to the UNE webserver through the encrypted Modbus TCP / IP protocol in https. Weather data is collected using a REST protocol.
Personal data: *(ways in which the collected or processed data can become personal or "sensitive" considering the recently adopted EU General Data Protection Regulation)*	Only the data collected and processed within the pilot related to production facilities and / or the Zhero system can be considered as *personal data* under the GDPR, if related to natural persons. Within the pilot, instead, the *particular (sensitive) data* in accordance with the GDPR is not present.
Data privacy (acquisition, transmission/storage/access): *(mechanism/protocols used or available to ensure data privacy including encryption, anonymization, aggregation)*	Data privacy will be assured through anonymization and aggregation.
Data management process transparency: *(mechanisms used or available to notify individuals whose data is collected about: entities collecting data, purpose, type of data stored, accessibility of their data, timeframe of storage)*	Adequate consent to personal data treatment will be acquired every time the obligation, in accordance to the provisions of the GDPR, will occur.
Certification: *(applicable standards, regarding both privacy and cybersecurity, and sought certifications already in place or expected in the near future)*	None

Table 7. Barcelona Pilot answers to the survey

Pilot & Data Manager	Sport Centre Claror Barcelona, Gas Natural Fenosa
Dataset description: *(brief description of the dataset and data flows. Type of data, accessibility of data, timeframe of storage)*	Dataset in the pilot includes: – Indoor conditions: Temperatures, Relative Humidity. – Energy consumption/generation: active/reactive power, gas consumption, photovoltaic generation, battery power – Equipment status: SOC of battery

	– Energy demand: inlet/outlet water temperature, water flow rate. Those variables will be sent in time steps of 15 minutes or hourly. To be defined.
Data security (acquisition, transmission/storage/access): *(mechanisms/protocols used or available to ensure secure data handling; certifications)*	Data is stored in AWS Europe complying ISO27002 and the regulation of data protection in Spain. • ISO 27017: It provides guidance on the information security aspects of cloud computing, recommending the implementation of cloud-specific information security controls that supplement the guidance of the ISO 27002 and ISO 27001 standards. This code of practice provides additional information security controls implementation guidance specific to cloud service providers. • ISO 27018: It focuses on protection of personal data in the cloud. It is based on ISO information security standard 27002 and provides implementation guidance on ISO 27002 controls applicable to public cloud Personally Identifiable Information (PII). It also provides a set of additional controls and associated guidance intended to address public cloud PII protection requirements not addressed by the existing ISO 27002 control set. Security of the data depends on its classification level and exposure.
Personal data: *(ways in which the collected or processed data can becomes personal or "sensitive" considering the recently adopted EU General Data Protection Regulation)*	There will not be any data form individuals collected in the project, only aggregated data from Sport Centre
Data privacy (acquisition, transmission/storage/access): *(mechanism/protocols used or available to ensure data privacy including encryption, anonymization, aggregation)*	As stored in AWS, it will comply with ISO27002 and the regulation of data protection in Spain. General Data Protection Regulation (GDPR): It is complied by AWS on May 25, 2018. Sensitive data (passwords, etc) will be encrypted. Access mechanisms need to be defined guaranteeing that data is only accessed by

	those authorized.
Data management process transparency: *(mechanisms used or available to notify individuals whose data is collected about: entities collecting data, purpose, type of data stored, accessibility of their data, timeframe of storage)*	There will not be any data form individuals collected in the project, only aggregated data from Sport Centre
Certification: *(applicable standards, regarding both privacy and cybersecurity, and sought certifications already in place or expected in the near future)*	Following EU regulation

Table 8. St. Jean de Maurienne Pilot answers to the survey

Pilot & Data Manager	**Pilot : St Jean de Maurienne, France** **Data Manager: Sylvain Berlioz (INNED)**
Dataset description: *(brief description of the dataset and data flows. Type of data, accessibility of data, timeframe of storage)*	Pilot Energy Management Data including aggregated energy consumption and forecast, PV and Hydro power plants energy production and forecast. Measurement data is collected and stored locally and transferred to a platform server using a broadband connection.
Data security (acquisition, transmission/storage/access): *(mechanisms/protocols used or available to ensure secure data handling; certifications)*	Applied EU defined security policies in accordance with best practices of the country concerned.
Personal data: *(ways in which the collected or processed data can becomes personal or "sensitive" considering the recently adopted EU General Data Protection Regulation)*	In France, the National Commission of Informatics and Civil Liberties (CNIL) are in line with EU recent regulation. We will follow then these requirements and practices [CNI16]
Data privacy (acquisition, transmission/storage/access): *(mechanism/protocols used or available to ensure data privacy including encryption, anonymization, aggregation)*	Applied EU defined privacy policies in accordance with best practices of the country concerned.
Data management process transparency: *(mechanisms used or available to notify individuals whose data is collected about: entities collecting data, purpose, type of data stored, accessibility of their data, timeframe of storage)*	Respecting transparency rules of the National Commission of Informatics and Civil Liberties CNIL guide [CNI18].

Certification: *(applicable standards, regarding both privacy and cybersecurity, and sought certifications already in place or expected in the near future)*	REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) The Regulations, contrarily to the Directives, are directly applicable into the Member States. This Regulation shall apply from 25 May 2018

Table 9. Nicosia Pilot answers to the survey

Pilot & Data Manager	**Pilot: Cyprus demonstration site (two different sites: 1) Microgrid at University of Cyprus, 2) dispersed prosumers within Cyprus)** **Data Manager: EAC (DSO) with FOSS (University of Cyprus)**
Dataset description: *(brief description of the dataset and data flows. Type of data, accessibility of data, timeframe of storage)*	Metering data (residential households and university campus) for both consumption and PV generation. Weather data (solar irradiance, indoors and outdoors temperature etc). Energy prices. Data are saved in servers of EAC and University of Cyprus and securely transmitted to online platform. Real-time acquisition and storage of data is possible, but provision of data in 15-minute intervals will be used
Data security (acquisition, transmission/storage/access): *(mechanisms/protocols used or available to ensure secure data handling; certifications)*	Each prosumer will have access to its own data by getting a security code to the data monitoring system. From EAC side, only authorized persons will have access to the data. Web management systems are secured according to the best practices. Regarding cyber security, the governing law 22(III)/2004 should be respected (referring to cyber-attacks).
Personal data: *(ways in which the collected or processed data can becomes personal or "sensitive" considering the recently adopted EU General Data Protection Regulation)*	All relevant data of the pilot sites are completely anonymized, so they cannot become personal or "sensitive"

Data privacy (acquisition, transmission/storage/access): *(mechanism/protocols used or available to ensure data privacy including encryption, anonymization, aggregation)*	Data anonymization process for all gathered data of prosumers. Encryption of all transmitted data and secure transmission of all relevant data
Data management process transparency: *(mechanisms used or available to notify individuals whose data is collected about: entities collecting data, purpose, type of data stored, accessibility of their data, timeframe of storage)*	-
Certification: *(applicable standards, regarding both privacy and cybersecurity, and sought certifications already in place or expected in the near future)*	None

Table 10. Lisbon Pilot answers to the survey

Pilot & Data Manager	**Pilot: Microgrid demonstration site at Campo Grande City Hall building, Lisbon** **Data Manager: ENOVA (Administration) with VPS (Technology)**
Dataset description: *(brief description of the dataset and data flows. Type of data, accessibility of data, timeframe of storage)*	Pilot Energy Management Data including aggregated and disaggregated energy consumption and forecast, PV energy production and forecast, EV charging consumption and forecast. Measurement data (typically 15 min readings) is collected and stored locally (on a number of concentrators) and transferred to a cloud server using a broadband connection. Commands follow a symmetric path.
Data security (acquisition, transmission/storage/access): *(mechanisms/protocols used or available to ensure secure data handling; certifications)*	Monitoring network, essentially a wired solution, uses a secure proprietary protocol to transfer data to the cloud server. Local access to data concentrators protected by basic authentication (username/password). Web based management system services secured in accordance with best practices using https. User's accesses limited by functionality (profile) and basic authentication.
Personal data: *(ways in which the collected or processed data can becomes personal or "sensitive" considering the recently adopted EU General*	Monitoring data may be susceptible to be considered personal, in particular disaggregated electrical energy consumptions, although it is being collected on a public building and with the exception of

Data Protection Regulation)	the EV charging doesn't refer to personal consumptions. Yet, this matter will be further analysed in detail and the necessary development to protect the privacy of the works and users of the building will be done in accordance with the EU Directive on Data Protection.
Data privacy (acquisition, transmission/storage/access): *(mechanism/protocols used or available to ensure data privacy including encryption, anonymization, aggregation)*	Disaggregated data is available only to authenticated end users; no anonymization is in place yet.
Data management process transparency: *(mechanisms used or available to notify individuals whose data is collected about: entities collecting data, purpose, type of data stored, accessibility of their data, timeframe of storage)*	There is no acknowledgment or notification mechanisms because the data collected is so far not considered personal or sensitive.
Certification: *(applicable standards, regarding both privacy and cybersecurity, and sought certifications already in place or expected in the near future)*	At this time, we are not looking for any particular certification but that might change during the course of the project.

Table 11. Xanthi Pilot answers to the survey

Pilot & Data Manager	**Pilot 8: Optimum Distributed Control of RES-Enabled Islanded Grids Local Storage Xanthi.** **Data Manager: CERTH/CPERI, SUNLIGHT**
Dataset description: *(brief description of the dataset and data flows. Type of data, accessibility of data, timeframe of storage)*	Energy production data from each of the three microgrids, microgrid consumption data, Energy Management Data, state of charge of the batteries, hydrogen storage, energy forecasting data, electrical signals, electrochemical signals and several control signals. The data is collected and stored locally. The data exchange between the microgrids and the control station is implemented with the existing wired local network. There is the feasibility for authorized users to communicate with control station remotely.
Data security (acquisition, transmission/storage/access): *(mechanisms/protocols used or available to ensure secure data handling; certifications)*	Data that is collected from the microgrid subsystems are not personal data but can be considered sensitive for CERTH and SUNLIGHT, hence they are password protected. Web management systems are secured according to the best practices. Transmitted data over MQTT protocol are

	protected with TLS/SSL secured communication channels.
Personal data: *(ways in which the collected or processed data can becomes personal or "sensitive" considering the recently adopted EU General Data Protection Regulation)*	Pilot 8 is a RES islanded smart microgrid. In such cases, the interaction with the end user is minimal. The collected data from each subsystem of the grid cannot be considered as personal data. Operators of the system are authorized personnel from SUNLIGHT and CERTH.
Data privacy (acquisition, transmission/storage/access): *(mechanism/protocols used or available to ensure data privacy including encryption, anonymization, aggregation)*	Data is acquired in each subsystem by using metering devices and is transmitted using a secure protocol. The data is collected and stored locally. Local access protected by basic authentication (username/password).
Data management process transparency: *(mechanisms used or available to notify individuals whose data is collected about: entities collecting data, purpose, type of data stored, accessibility of their data, timeframe of storage)*	No personal data management is employed in the pilot. Acquired or stored data can only be accessed from authorized personnel from SUNLIGHT and CERTH.
Certification: *(applicable standards, regarding both privacy and cybersecurity, and sought certifications already in place or expected in the near future)*	No certification is needed due to lack of personal-sensitive data.

Table 12. Ploiesti Pilot answers to the survey

Pilot & Data Manager	**Pilot: Ploiesti, Romania demonstration site (8 residential consumers and 2 commercial buildings** **Data Manager: ELECTRICA (DSO)**
Dataset description: *(brief description of the dataset and data flows. Type of data, accessibility of data, timeframe of storage)*	Residential Consumers: Pilot Energy Management Data including energy consumption {P, Q, U, Up and Down Time, SAIDI}. Measurement data is collected and transferred to a server via a 3G/Ethrenet communication protocol. The communication with DSO is carried out through the current communication infrastructure.
Data security (acquisition, transmission/storage/access): *(mechanisms/protocols used or available to ensure secure data handling; certifications)*	Each consumer will have access to its own consumption data via a security code. Considering DSO, only authorized persons will have access to the data. Web management systems are secured

	according to the best practices. Regarding cyber security, the Romanian Government Decision No 271/2013 approving the Cyber Security Strategy in Romania should be followed.
Personal data: *(ways in which the collected or processed data can becomes personal or "sensitive" considering the recently adopted EU General Data Protection Regulation)*	The processing of personal data is governed by the Processing of Personal Data as described in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) As the number of consumer's involved in Ploiesti Pilot is small, i.e. 8, an Informed Consent with each consumer is signed.
Data privacy (acquisition, transmission/storage/access): *(mechanism/protocols used or available to ensure data privacy including encryption, anonymization, aggregation)*	Data is acquired by the DSO using its metering devices and is transmitted anonymized via 3G communication as data is received by Elelectrica. According to The National Supervisory Authority For Personal Data Processing in Romania, Law nr 677/2001 should be respected.
Data management process transparency: *(mechanisms used or available to notify individuals whose data is collected about: entities collecting data, purpose, type of data stored, accessibility of their data, timeframe of storage)*	Informed consent with each consumer is signed.
Certification: *(applicable standards, regarding both privacy and cybersecurity, and sought certifications already in place or expected in the near future)*	Electrica has all the required certifications for data handling.

Table 13. Thessaloniki Pilot answers to the survey

Pilot & Data Manager	**Pilot: Thessaloniki demonstration sites:** **1) Demand Response in residential buildings with smart meters and Battery Energy Storage Systems (BESS),** **2) Demand Response in commercial building with smart meters and BESS.** **Data Manager: WVT (Utility), SUNLIGHT (SME) with CERTH (Research Centre)**
Dataset description: *(brief description of the dataset and data flows)*	WVT has already developed an advanced metering infrastructure (AMI), so smart meters can measure and record actual energy consumption from all the buildings at

	constant time intervals of 5 minutes. Further occupancy and environmental monitoring equipment will be utilized in the commercial building use case. The data gathered will be aggregated at a gateway at the building level and forwarded to the back-end WVT analytics system over a secure network through wired or wireless communication. AMI consists of three basic components: smart metering devices at the user end, two-way communication path between the end-user (HAN) and WVT and automated software and operation centre for data processing. A database known as Meter Data Management System (MDMS) is utilized by WVT to store and manage the collected data. This system includes analytical tools which enable different sections of operation and management system to interact with it and collect the required data.
Data security (acquisition, transmission/storage/access): *(mechanisms/protocols used or available to ensure secure data handling; certifications)*	Based on the current installation of the WVT infrastructure, only authorized persons have access to the dataset collected at the back-end WVT analytics system. Web management systems utilized are secured according to the best practices.
Personal data: *(ways in which the collected or processed data can becomes personal or "sensitive" considering the recently adopted EU General Data Protection Regulation)*	All the pilot participants (around 100 residential buildings and around 20 people working on the commercial building) will be properly informed and educated on the planned activities of the pilot trials, and further asked to sign an Informed Consent Form prior to the pilot realisation.
Data privacy (acquisition, transmission/storage/access): *(mechanism/protocols used or available to ensure data privacy including encryption, anonymization, aggregation)*	In order to meet the requirements in terms of data privacy, the solutions to be deployed will be compliant with respective legislation in Europe. The most popular wired technology in Europe is Power Line Communications (PLC), which refers to the use of the existing power lines for the signal transmission and includes the broadband PLC (B-PLC) and narrowband PLC (NB-PLC) standards. The basic benefit of this technology is that there is no need for new infrastructure. As for the wireless technologies, they are divided into three categories: (i) the point-to-point (mobile communication), point-to-multipoint (star topology) and radio mesh networks. In Greece, the main technologies that have been used for smart metering data

	transmission are the power line communication NB-PLC and wireless technologies over GPRS and GSM. Since the collected data contains critical personal as well as business information, the storage facilities should be disaster proof and all required back up and contingency plans for different scenarios should be carefully designed for them. Data are sent from the smart meter through a secure Cloud Service to the back-end WVT MDMS database system , which is using MySQL, which offers enterprise-grade security features including network access control, Firewall, Enterprise Authentication, Enterprise Encryption & Transparent Data Encryption to ensure data is protected against external attacks and misuse of information while helping WVT achieve regulatory compliance.
Data management process transparency: *(mechanisms used or available to notify individuals whose data is collected about: entities collecting data, purpose, type of data stored, accessibility of their data, timeframe of storage)*	Adequate consent to personal data treatment will be acquired every time the obligation, in accordance to the provisions of the GDPR, will occur.
Certification: *(applicable standards and sought certifications already in place or expected in the near future)*	A certification from the Commissioner for Data Protection is to be acquired regarding the data editing from the prosumers on the basis of the submitted application. WVT, being a utility company, has already all the required certifications for data handling.

5.3 Findings and outcomes

After collection of the answered surveys, main outcomes are reported.

5.3.1 Data managers

As requested by regulation, an individual/firm is defined as data manager.

5.3.2 Datasets description

For what concerns dataset, most of the data collected are obviously energy/power or energy/power-related data. Energy consumption, production or forecast are main energy/power data. Related to those, some datasets include also data of the auxiliaries of the core plant, e.g. batteries, EV, hydrogen storage logs. Other datasets are related to market, e.g. market prices. Finally, weather data are present, e.g. temperature, irradiance, wind speed logs. No data are in principle personal, but relatives to group of users, to plants, to firms or to ambient conditions.

5.3.3 Data security

Most of datasets are protected by a form of identification of accesses (ID + password). Repositories online where storage takes place have data protection planned by design. Different data transmission protocols are used. Most of them have encryption and/or data

transmission permitted for authenticated data only. Anyway, Pilots are aware they must respect national directives and rules for each phases of data treatment.

5.3.4 Personal data

Most of the data are not considered personal and cannot arise any doubts. Some data can present a risk of identification of the related individuals. For those data, either specific consent is requested, or anonymization process is applied.

Personal data are in origin present for Pilots 3, 5, 6, 7 and 9.

Anonymization procedures are in place in 6

Specific consent is asked to individuals involved in Pilot 3 and 9.

Further development of data treatment to comply with regulation will take place in Pilot 5 and 7.

Specifically, the survey highlighted an issue in Pilot 7. They are performing collection of data that can be defined personal data (disaggregated energy consumption data on a public building, including EV charging data) without neither performing anonymization nor asking for specific consent. The PLs will be notified of this issue and an update on it will be provided in D10.11.

5.3.5 Data privacy

Anonymization and aggregation of data is the main tool for provision of privacy within inteGRIDy framework. These are the most suitable methods, and they can be used since inteGRIDy has not the aim of analyzing personal behavior and attitudes. Accessibility to data is regulated by default within inteGRIDy framework, and data are clustered in Open, Consortium and Private.

5.3.6 Transparency of data treatment

As previously described, in case of personal data in use, specific consent is asked to all the individuals involved. This is the tool for guaranting notification and awareness of people under study, therefore achieving transparency of the process.

The situations as of now still not completely detailed (Pilot 5 and Pilot 7), will be assessed and will be referred about their update on D10.11.

5.3.7 Certifications

Most of the Pilots are not pursuing a specific standard or certification. In any case, the responsible of data treatment possess the certifications needed to perform it.

6. Conclusions

The document was aimed to guide the Consortium comply with EU regulation on data protection, privacy principles and ethical monitoring. The regulation has been implemented in every country involved in inteGRIDy. After a detailed description of the regulations, the answers to a survey proposed to PLs have been listed. The responses are checked to verify compliance of every Pilot to regulation.

The outcomes of the analysis with PLs are listed in the following.

Some personal data are involved in Pilot projects of inteGRIDy. Two main paths are used to overcome this issue. The first is anonymization of the data. The latter is submission of a specific consent.

Anonymization of data appears the less demanding solution. Nonetheless, it implies a loss of information that can be of use. In this case, specific consent can be requested.

In particular, energy consumption data on a small group of users can lead to identification of the individuals. A consent compliant with GDPR (no “opt-out”, freely-given, unambiguous consent) is submitted to users at the beginning of experimentations. This is the case for Pilots 3 and 9. In other cases, Pilot responded that the subject will be further analysed with development of the pilot. This is the case for Pilot 5 and 7. Other Pilots responded there are no personal data so far involved in their projects. They are aware of the definition of personal data.

Apparently, Pilot 7 (Lisbon) will need a review of its protocols in data treatment. It is treating data that could be defined as personal data, yet it is asking no consent and it is not performing any anonymization process. Data collected are aggregated of energy consumption data on small buildings. These buildings are municipally owned, and the manager is involved in inteGRIDy. Nevertheless, a further check within the development of the Pilot is already planned by PLs. They will be notified of this issue and update of this situation will be provided in D10.11.

For Pilot 5 and 7, monitoring of the evolution of their issues will be regularly performed from M24 on. This is in charge of T10.3 in a shared effort with the PLs.

Data security mechanisms are up and running in the majority of Pilots. Every category of data is collected and stored in repositories assuring the access of only authorized individuals and organizations.

Privacy of data is guaranteed in most of projects by anonymization processes. The cases in which this process is not in place ask for specific consent to individuals under study.

Anyway, the data management process is under regular surveillance in inteGRIDy framework by means of DMP. Latest version of DMP is D10.14.

Ethical framework is assessed within inteGRIDy. No involvement in risky issues is present.

Data accessibility is maintained as open as possible. The FAIR protocol is followed.

What follows can be stated as final remarks.

inteGRIDy Consortium is just partially involved in personal data collection. Where personal data are treated, two main paths are pursued by Pilots to comply with rules. Anonymization allows personal data to be considered no more personal. Otherwise, a specific consent request compliant with GDPR can be submitted to individuals involved.

Data security mechanisms are in place and tested. All the data gathered are clearly defined and so are the purposes. Accessibility to data for different categories of users is guaranteed and data are classified in three clusters: Open data, data accessible to Consortium, Private data.

Any issues arising within the timeframe inteGRIDy is taking place will be faced by Consortium in a manner compliant to laws and respectful of principles of the project. PLs involved in situations that could arise issues will be notified, and the evolution of each situation will be monitored.

7.References

[BOE02] Boletín Oficial del Estado, Real Decreto-ley 5/2018, accessed on December 17, 2018, https://www.boe.es/boe/dias/2018/07/30/pdfs/BOE-A-2018-10751.pdf

[BOE18] Boletín Oficial del Estado, Ley Orgánica 3/2018, accessed on December 17, 2018, https://www.boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf

[BOE99] Boletín Oficial del Estado, Ley Orgánica 15/1999, accessed on December 17, 2018, https://boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf

[CHR18] Cyprus House of Representatives, Law 125(I) of 2018, accessed on December 17,2018 http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/2B53605103DCE4A4C225826300362211/$file/Law%20125(I)%20of%202018%20ENG%20final.pdf

[CNI16] Commission Nationale de l'Informatique et des Libertés, Plus de droits pour vos données !, accessed on December 13, 2018, https://www.cnil.fr/fr/plus-de-droits-pour-vos-donnees

[CNI18] Commission Nationale de l'Informatique et des Libertés, Conformité RGPD : comment informer les personnes et assurer la transparence ?, accessed on December 13, 2018, https://www.cnil.fr/fr/conformite-rgpd-information-des-personnes-et-transparence

[CNP17] Comissão Nacional de Protecção de Dados, História da CNPD, accessed on November 23, 2018, https://www.cnpd.pt/bin/cnpd/historia.htm

[COE81] Council of Europe (1981), Convention for the protection of individuals with regard to automatic processing of personal data, accessed on December 13, 2018, https://rm.coe.int/1680078b37

[DCE18] Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal, Decizia nr. 133 din 3 iulie 2018 privind aprobarea Procedurii de primire și soluționare a plângerilor

[DEC18] Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal, DECIZIE nr. 99 din 18 mai 2018 privind încetarea aplicabilităţii unor acte normative cu caracter administrativ emise în aplicarea Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date

[DPA17] Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal, Website Homepage, accessed on December 13, 2018, https://www.dataprotection.ro/

[DPA18] Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal, Law no. 190/2018 on the measures for the application of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), https://www.dataprotection.ro/servlet/ViewDocument?id=1520

[ELC04] Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal, Law no. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector, https://www.dataprotection.ro/servlet/ViewDocument?id=173

[ELC08] Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal, Law no. 298/2008 on the retention of data generated or processed in connection with the provisions of publicly available electronic communications

services or of public communications networks and for the amendment of Law no. 506/2004 on the processing of personal data and the protection of private life within the electronic communication sector

[EUC12] European Commission, Charter of Fundamental Rights of the European Union, accessed on November 22, 2018 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

[EUC17] European Commission (2017), Cross cutting issues, accessed on November 22, 2018, http://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/ethics_en.htm

[EUC18] European Commission (2018), What personal data is?, accessed on December 3, 2018, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

[EUC95] European Commission, Directive 95/46/EC

[EUP02] European Parliament (2002), Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, accessed on December 13, 2018, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32002L0058

[EUP09] European Parliament, 2009/136/EC, accessed on November 22, 2018, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:EN:PDF

[EUP95] European Parliament (1995), Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, accessed on December 13, 2018, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[GDP16] European Commission, 2016(UE)/679 General Data Protection Regulation, accessed on November 22, 2018 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[GPA06] Greek Parliament, Law 3471/2006, accessed on December 17, 2018, http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/LEGAL%20FRAMEWORK/LAW_%203471_06EN.PDF

[GPA97] Greek Parliament, Law 2472/1997, accessed on December 17, 2018, https://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/LEGAL%20FRAMEWORK/LAW%202472-97-APRIL010-EN%20_2_.PDF

[KAR11] Karageorgiou & Associates Law Firm, Data protection in Greece: key issues, accessed on December 17,2018, https://kalaw.gr/wp-content/uploads/Overview_Greece_2011.pdf

[MCK18] Baker McKenzie, GDPR National Legislation Survey, 4.0, accessed on December 17,2018, https://tmt.bakermckenzie.com/-/media/minisites/tmt/files/2018/08/gdpr_national_legislation_survey_4_aug2018.pdf

[NAP18] Law no. 129/2018 [NAP18] for amending and supplementing the Law no. 102/2005 on the establishment, organization and functioning of the National Supervisory Authority for Personal Data Processing, as well as for repealing the Law no. 677/2001 on the Protection of Individuals with regard to the Processing of Personal Data and the Free Movement of such Data, https://www.dataprotection.ro/servlet/ViewDocument?id=1502

[OAI17] OpenAire (2017), What is the EC Open Research Data Pilot?, accessed on November 29, 2018, https://www.openaire.eu/what-is-the-open-research-data-

pilot

[OEC99] Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, The Organization for Economic Co-Operation and Development.

[PCM18] PRESIDÊNCIA DO CONSELHO DE MINISTROS, Proposta de Lei n.º 120/XIII, accessed on November 22, 2018, http://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c324679595842774f6a63334e7a637664326c756157357059326c6864476c3259584d7657456c4a535339305a58683062334d76634842734d5449774c56684a53556b755a47396a&fich=ppl120-XIII.doc&Inline=true

[PPD01] Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal, Law no. 677/2001 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data, amended and completed, https://www.dataprotection.ro/servlet/ViewDocument?id=174

[PUK18] Parliament of the United Kingdom, Data Protection Act 2018, accessed on December 17,2018, http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf

[PUK98] Parliament of the United Kingdom, Human Rights Act 1998, accessed on December 17,2018, https://www.legislation.gov.uk/ukpga/1998/42/contents

[SGT12] Smart Grids Task Force 2012-14 (2014), Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems, accessed on November 15, 2018, https://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

http://www.integridy.eu