PANTERA
Pan European Technology Energy Research Approach

Work Package 1

Deliverable 1.5

Data Management Plan

Grant Agreement No:	**824389**
Funding Instrument:	**Coordination and Support Action (CSA)**
Funded under:	**H2020 LC-SC3-ES-7-2018: Pan-European Forum for R&I on Smart Grids, flexibility and Local Energy Networks**
Starting date of project:	**01.01.2019**
Project Duration:	**48 months**

Contractual delivery date:	**28.02.2019**
Actual delivery date:	**28.02.2019**
Lead beneficiary:	**FOSS**
Deliverable Type:	**Open Research Data Pilot**
Dissemination level:	**Confidential, only for members of the consortium (including the Commission Services)**
Revision / Status:	**draft**

This project has received funding from the European Union's Horizon 2020 Coordination and Support Action Programme under Grant Agreement No. 824389

Document Information

Document Version:	1
Revision / Status:	draft
All Authors/Partners	[Venizelos Efthymiou / FOSS] [Christina Papadimitriou/FOSS] [Giorgos Papadopoulos/Suite 5] [Mohamed Shalaby/Derlab e.V.]
Distribution List	[All partners of PANTERA]
Keywords:	[Data management Plan, Ethics Requirements]

Document History

Revision	Content / Changes	Resp. Partner	Date
1	Initial draft	FOSS	08.02.19
2	Final version	FOSS	27.02.19

Disclaimer

Copyright Notice

Table of contents

Abbreviations

Acronym	Full name
APRR	Annually Periodic review reports
BIM	Business Innovation Manager
CA	Consortium Agreement
DMP	Data Management Plan
DER	Distributed Energy Resource
EMT	Executive Management Team
FAIR	Findable, Accessible, Interoperable, and Reusable
FPM	Framework Project Management
GA	Grant Agreement
GenA	General Assembly
ICT	Information & Communication Technologies
IMP	Innovation Management Plan
IMR	Interim management reports
LL	Living Lab
MS	Milestone
OA	Open Access
PC	Project Coordinator
PM	Project Manager
QAP	Quality Assurance Plan
S/T	Scientific/ Technical
SC	Steering Committee
SSL	Secure Sockets Layer
TL	Task Leader
TM	Technical Manager
ToC	Table of Content
PANTERA	Pan European Technology Energy Research Approach
WP	Work Package
WPL	Work Package Leader

Executive Summary

This deliverable presents the final version of the (open) Data Management Plan for the PANTERA project in month 2 of the project. This Data Management Handling Plan investigates the appropriate methodologies and open repositories for data management and dissemination and tries to offer through open access as much information generated by the PANTERA project.

Such information would be the public deliverables of the project, the scientific publications issued by the project consortium, white papers published, etc. These datasets are expected to be collected during the entire phase of the project and are therefore subject to change, considering also the definition of the PANTERA business models. The publishing platforms used are the project website, the OnlyOffice platform for long-term archiving (as proposed by E.C.), and the PANTERA platform. PANTERA platform and website can be accessed openly whereas OnlyOffice platform will be accessed by members only and serve their collaboration..

In addition to the data management plan, the scope of this document is to define the ethics management plan of the project. As this part of the work is handling with the ethics requirements of the project, we consider this section as the confidential part of the document.

1 Objectives of the report

1.1 Purpose of the Document

The PANTERA Data Management Plan is produced in the context of WP1, Task T1.7 Data management and ethics requirements.

The main objectives of the Data management plans are to clearly address issues such as the overall methodology for handling the scientific outcomes of the project, the specification of data types that the project generates and/or collects, the standards that will be used, the process of how this data will be exploited and/or shared/made accessible for verification and re-use, the data preservation and maintenance processes etc. The analysis is twofold covering both the ethics management process and the dissemination of data outcomes of the project.

In particular, the Data Management Plan is formulated in accordance with the H2020 guidelines regarding Open Research Data. In alignment with the EC Guidelines for Open Access (1. European Union, 2019), we clearly define how the scientific publications issued by the project consortium like white papers published, will be further disseminated to a wider audience.

On the other hand, the Ethics Management Plan is a core part of the project; thus the detailed plan on the way to handle data collected by the PANTERA partners during the development of the project is reported in this deliverable.

1.2 Scope of the Document

The scope of the document is to define the internal data management structure of the project and provide the associated methodology on the way to handle and further disseminate the data outcomes of the project.

The PANTERA Data Management Plan is produced in the context of WP1, Task T1.7 Governance, Coordination and Quality Assurance to serve as a data management manual of the project activities; considering this as the horizontal management activity of the project.

1.3 Structure of the Document

The document is divided into the following sections

- Chapter 2 defines the purpose of the document, its structure, and terms that are necessary to understand it.
- In section 3, we define the methodological framework towards handling the results collected or generated during the project. The overall analysis is inline (actually a summarized version) of the methodology proposed by E.C.
- In section 4, we define the tools to be used in order to ensure that the data will be exploited and/or shared/made accessible for verification and re-use along with the data preservation and maintenance processes
- In section 5, we list all publications and related data that is already or may be generated or collected during the project. For each result we provide - in accordance to the Data Management Guideline (European Commission, 2013) - a short description, the chosen way of open access, and a long-term storage solution.
- In section 6, the focus is on the Ethics management plan of the project, in line with the new GDPR legislation in Europe.

A summary of project activities towards the definition of the PANTERA Data Management Handling plan is provided as an outcome of the work.

2 Methodological Framework for Data Management Plan

A DMP (Data Management Plan) describes the data management life cycle for the data to be collected, processed and/or generated by a HORIZON 2020 project (1. European Union, 2019). As part of making research data findable, accessible, interoperable and re-usable, a DMP should include information about the handling of research data during and after the end of the project**Error! Reference source not found.**:

- What data will be collected, processed and/or generated? What kind of data will the project collect or generate? To whom might they be useful later on?
- Which methodology and standards will be applied? What metadata is required to enable data to be found and understood, ideally according to the particular standards of scientific discipline?
- Whether data will be shared/made open access?
- How data will be preserved (including after the end of the project)? How to archive and preserve the open datasets of the project? How funding bodies ensure that publicly funded research outputs can have a positive impact on future research, for policy development, and for societal change?

More specifically, for Horizon 2020 projects, a FAIR (Findable, Accessible, Interoperable, and Reusable) DMP template has been designed to be applicable to any project that produces, collects or processes research data (2. FAIR, 2013). The respective activities defined as part of the methodology, adopted also in PANTERA project are:

- Data Summary
- FAIR Data Principles
  - Making data findable, including provisions for metadata
  - Making data openly accessible
  - Making data interoperable
  - Increase data re-use (through clarifying licenses as defined during project period)
- Allocation of resources
  - Explain the allocation of resources
- Data Security
  - Address data recovery as well as secure storage and transfer of sensitive data
- Ethical Aspects
  - In the context of the ethics management plan of the project as defined in Section 6 of this document.
- Other Issues
  - Refer to other national/funder/sectorial/departmental procedures for data management if any

Figure 1 presents the FAIR data principles towards promptly disseminating the data outcomes of a research project.

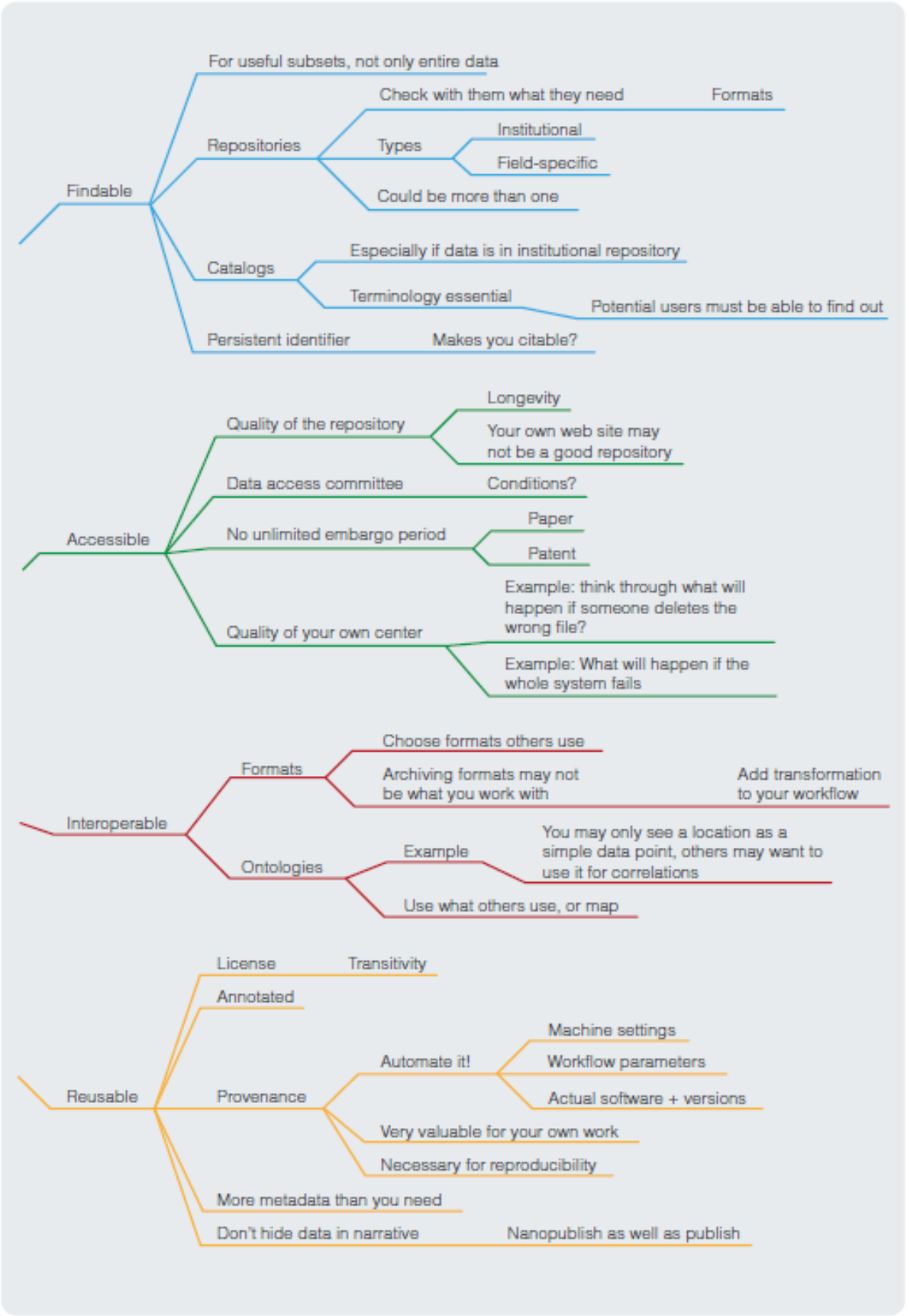

Figure 1 Research Data Management according to the FAIR principles (Source: Elsevier)

A DMP is required for all projects participating in the extended Open Research Data pilot and PANTERA will contribute towards this direction. Thus, a preliminary version of the Data Management Plan is provided early in the project, subsequently the DMP needs to be updated over the course of the project whenever significant changes arise, such as (but not limited to):

1. new data are generated
2. changes in consortium policies (e.g. new innovation potential, decision to file for a patent)
3. changes in consortium composition and external factors (e.g. new consortium members joining or old members leaving)

As previously indicated, the Data Management Plan is a living document that should be updated at a minimum in time with the periodic evaluation/assessment of the project. Any updates will be reported in the **project periodic report** as there is no plan for the updated version of this deliverable.

Along with the definition of the datasets, special focus is delivered at the selection of the platform to archive and preserve the datasets. When choosing a repository, it is important to consider factors such as whether the repository:

- Gives the submitted dataset a persistent and unique identifier. This is essential for sustainable citations – both for data and publications – and to make sure that research outputs in disparate repositories can be linked back to particular researchers and grants.
- Provides a landing page for each dataset, with metadata that helps others find it, tell what it is, relate it to publications, and cite it. This makes your research more visible and stimulates reuse of the data.
- Helps to track how the data has been used by providing access and download statistics.
- Responds to community needs and is preferably certified as a ‘trustworthy data repository’, with an explicit ambition to keep the data available in the long term.
- Matches particular data needs (e.g. formats accepted; access, back-up and recovery, and sustainability of the service). Most of this information should be contained within the data repository’s policy pages.
- Provides guidance on how to cite the data that has been deposited.

In addition, a main point of the DMP is the definition of the **open access** type over the data. Open Access (OA) refers to the practice of providing online access to scientific information that is free of charge to the end-user and reusable. 'Scientific' refers to all academic disciplines. In the context of research and innovation, 'scientific information' can mean:

- peer-reviewed scientific research articles (published in scholarly journals) or
- research data (data underlying publications, curated data and/or raw data).

Open Access (1. European Union, 2019) to scientific publications means free online access for any user. The 2 main routes to Open Access are:

A. Self-archiving / 'green' Open Access – the author, or a representative, archives (deposits) the published article or the final peer-reviewed manuscript in an online repository before, at the same time as, or after publication. Some publishers request that open access should be granted only after an embargo period has elapsed.

B. Open Access publishing / 'gold' open access - an article is immediately published in open access mode. In this model, the payment of publication costs is shifted away from subscribing readers. The most common business model is based on one-off payments by authors.

Research data refers to information, in particular facts or numbers, collected to be examined and considered as a basis for reasoning, discussion, or calculation. In a research context, examples of data include statistics, results of experiments, measurements, observations resulting from fieldwork, survey results, interview recordings and images. The focus is on research data that is available in digital form. Users can normally access, mine, exploit, reproduce and disseminate openly accessible research data free of charge. The next figure presents the process flow towards defining the open access type in scientific publications and research data.

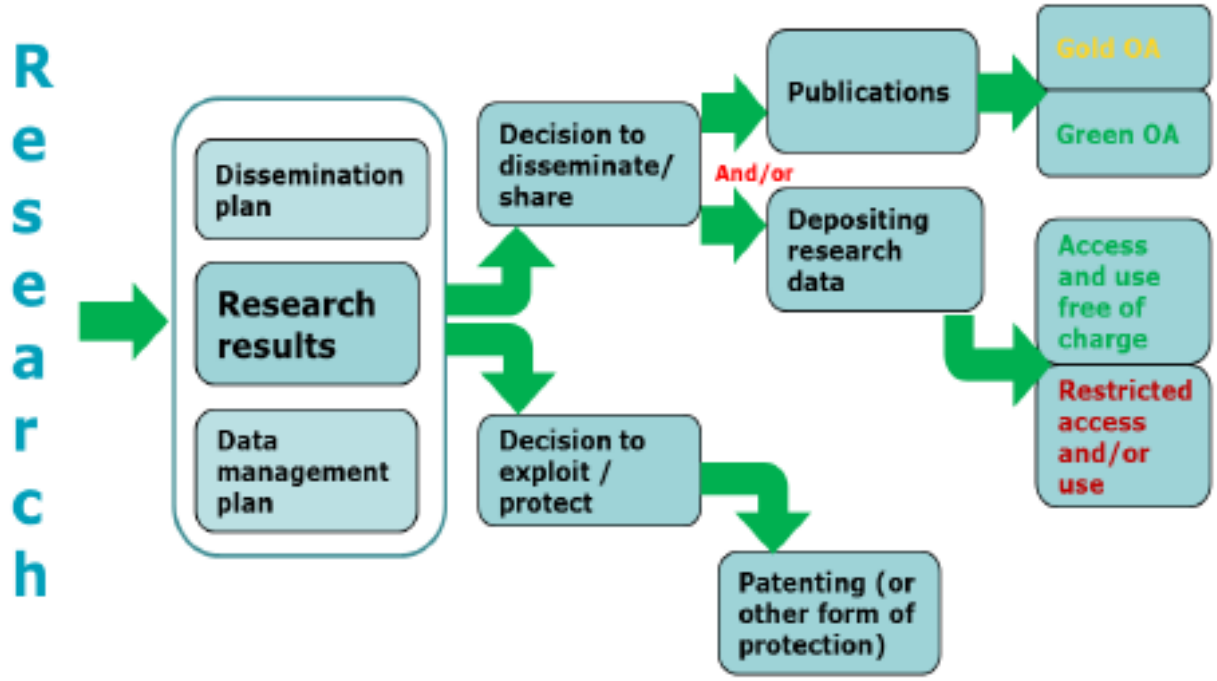

Figure 2 Open Access strategy for publications and research data

The open access mandate comprises 2 steps:

1. depositing publications in repositories
2. providing open access to them

These steps are explained in the following sections along with the definition of the ways for archiving and preserving the open datasets of the PANTERA project. A methodological process to handle the Data Management Process is provided as part of the framework towards the definition of the Data Management Plan.

2.1 DMP Management Process

We highlighted in previous section the main goals and objectives towards the definition of the PANTERA Data management plan along with some principles and guidelines.

Taking into account this preliminary analysis, the PANTERA Data Management Process is defined as a step-wise approach for each result generated or collected during the project runtime (3. CA, 2019). The following questions must be answered to classify the different datasets:

1. Does a result provide significant value to others or is it necessary to understand a scientific conclusion?

If this question is answered with yes, then the result is classified as public (granted for open access). If this question is answered with no, the result is classified as non-public. For example, code that is very specific to a platform (e.g. a database initialization) is usually of no scientific interest to anyone, nor does it add any significant contribution.

2. Does a result include personal information that is not the author's name?

If this question is answered with yes, the result is classified as non-public. Personal information beyond the name must be removed if it should be published according to the ethics management plan of the project.

3. Does a result allow the identification of individuals even without the name?

This is also a step managed by the ethics management plan of the project as we have committed in PANTERA project to establish anonymization techniques to conceal a single user's identity, e.g. abstraction, dummy users, or non-intersecting features. If this question is answered with yes, the result is classified as non-public.

4. Can a result be abused for a purpose that is undesired by society in general or contradict with societal norms and the project's ethics?

This is also a step managed by the ethics management plan of the project. If this question is answered with yes, the result is classified as non-public.

5. Does a result include business or trade secrets of one or more partners of the project?

If this question is answered with yes, the result is classified as non-public. Business or trade secrets need to be removed in accordance to all partners' requirements before it can be published.

6. Does a result name technologies that are part of an ongoing, project-related patent application?

If this question is answered with yes, then the result is classified as non-public. Of course, results can be published after patent has been filed.

7. Does a result break security interests for any project partner?

If this question is answered with yes, the result is classified as non-public.

This is a simple structural approach to determine the different data types defined as part of the DMP. The responsibilities of the PANTERA consortium partners towards disseminating the project outcomes are defined in the following section.

2.2 Responsibilities and Decision Making

The Data Management Plan presented in this deliverable aims to identify the project outputs to be disseminated as well as to decide on way and means of their Open Access (if applicable). To ensure it, a dedicated time slot will be reserved at each of the project plenary meetings and, if needed, at selected consortium audio conferences. EC and project reviewers will be informed about related work done and publications provided in the project management reports.

Individual responsibilities on data management in the project consortium are:

- Data Management Plan Leader (FOSS) – to prepare and lead related discussions at the relevant project meetings and to maintain the channels for dissemination of project outcomes.
- Scientific and Technical Project Manager (FOSS) – to identify data collected by the project and technical project outcomes eventually suitable for publication
- Dissemination leader (DERlab e.V.) – to identify publications suitable for publication in the considered repositories and maintain PANTERA inputs for the Open Access
- Each individual partner – to identify own project results suitable for publication

Moreover, each PANTERA partner has to respect the policies set out in this DMP. Datasets have to be created, managed and stored appropriately and in line with applicable legislation. Validation and registration of datasets and metadata is the responsibility of the partner that generates the data in the WP. Metadata constitutes an underlying definition or description of the datasets, and facilitate finding and working with particular instances of data.

Backing up data for sharing through Open Access repositories is the responsibility of the partner possessing the data.

Quality control of these data is the responsibility of the relevant WP leader, supported by the Data Management Plan Leader.

If datasets are updated, the partner that possesses the data has the responsibility to manage the different versions and to make sure that the latest version is available in the case of publicly available data.

Last but not least, all partners must consult the concerned partner(s) before publishing data in the open domain that can be associated to an exploitable result.

2.3 NOTIFICATION OF TREATMENT OF PERSONAL DATA

By taking into account the methodological framework, we issue the following notification according to art. 13 of EU Regulation 2016/679 of April 27, 2016 on the protection of individuals with regard to the processing of personal data and in compliance with the legislation on the processing of personal data, as well as on the free movement of such data.

2.3.1 Data Controller

The following organizations are partners of the PANTERA project. They act jointly as data controller.

- UNIVERSITY OF CYPRUS FOSS, Cyprus
- European Distributed Energy Resources Laboratories e.V., Germany
- RICERCA SUL SISTEMA ENERGETICO RSE SPA, Italy
- SINTEF ENERGI AS, Norway
- FIZIKALAS ENERGETIKAS INSTITUTS IPE, Latvia
- SUITE5 DATA INTELLIGENCE SOLUTIONS LIMITED, Cyprus
- UNIVERSITY COLLEGE CORK - NATIONAL UNIVERSITY OF IRELAND, Ireland
- UNIVERSITY COLLEGE DUBLIN, NATIONAL UNIVERSITY OF IRELAND, Ireland
- TECHNICAL UNIVERSITY OF SOFIA, Bulgaria

2.3.2 Internal responsible persons of PANTERA project

- <<George E. Georghiou, geg@ucy.ac.cy, Panepistimiou 1 Avenue P.O. Box 20537 1678, Nicosia >>, UNIVERSITY OF CYPRUS, FOSS, Cyprus
- <<Ata Khavari, ata.khavari@der-lab.net, a c/o Fraunhofer IEE Königstor 59 34119 Kassel / Germany >>European Distributed Energy Resources Laboratories e.V., Germany
- << Cabiati Mattia, mattia.cabiati@rse-web.it, Via Raffaele Rubattino, 20134 Milano >>RICERCA SUL SISTEMA ENERGETICO RSE SPA, Italy
- <<Andrei Morch, Andrei.Morch@sintef.no, Sem Sælands vei 11, 7034 Trondheim, >>SINTEF ENERGI AS, Norway
- <<Anna Mutule, amutule@edi.lv, Institute of Physical Energetics, Aizkraukles iela 21, Riga, LV-1006, Latvia>>FIZIKALAS ENERGETIKAS INSTITUTS IPE, Latvia
- <<Tasos Tsitsanis, tasos@suite5.eu, 95B Archiepiskopou Makariou III, 3020 Limassol, Cyprus,>> SUITE5 DATA INTELLIGENCE SOLUTIONS LIMITED, Cyprus
- <<Shafi Khadem, shafi.khadem@ierc.ie, College Rd, University College, Cork, T12 K8AF>>UNIVERSITY COLLEGE CORK - NATIONAL UNIVERSITY OF IRELAND, Ireland
- <<Claire Cullen, claire.cullen@ucd.ie, Belfield, Dublin 4, Ireland. Eircode: D04 V1W8>>UNIVERSITY COLLEGE DUBLIN, NATIONAL UNIVERSITY OF IRELAND, Ireland
- <<Rad Stanev, rstanev@tu-sofia.bg, Sveti Kliment Ohridski" 8, 1756 Studentski Kompleks, Sofia,>>TECHNICAL UNIVERSITY OF SOFIA, Bulgaria

The data may be processed by UNIVERSITY OF CYPRUS, FOSS and to this end instructed in compliance with current legislation.

2.3.3 Responsible of personal data protection and contact point

DPO of UNIVERSITY OF CYPRUS, FOSS, <<e-mail lefteri@ucy.ac.cy, tel: 00357 22894075>>

2.3.4 Purposes of processing legal basis, data categories and storage period

Data collection activities of the project (e.g. research data collection from H2020 participants) will be performed in collaboration with organizations that hold the type of information required for PANTERA. Each request for data will be accompanied by the collection of personal data for the person collaborating with PANTERA under the following notification:

You are invited to participate to the PANTERA project (Pan European Technology Energy Research Approach). PANTERA promises a pan-European multi-dimensional collaborative platform, capable of leveraging coherence and trust as a pull towards enhanced R&I in energy systems centred around an integrated grid active and responsive. Easy access, readymade tools, real data from projects with results build in case studies for exploitation / utilization, building of future scenarios and equally important an attractive environment for generating the vision of tomorrow through innovative tools and methods to be tailored for wider understanding and use.

For the purposes of the application of European and national legislation on the matter (EU Regulation 679/2016, from now on Regulation), we inform you that your personal data will be used for the following purposes.

	Legal basis of the treatment	Categories of personal data being processed	Period of retention of personal data
Purpose 1 **Storage of Project Proposal, Grant Agreement, Consortium Agreement, Financial Identification Form and relevant content.**	Execution of the PANTERA project including the administrative obligations (Article 6(1)(b) of the Regulation)	○ First name ○ Family name ○ Email ○ Affiliation ○ Phone number ○ Curriculum Vitae	Stored until the completion of all the project obligations after the project end, i.e., until 2027. The project end is in 2022 plus five years of obligations. For public administration, indefinitely due to the transparency and good functioning of the public administration.
Purpose 2 **Email distribution lists for PANTERA project**	Execution of the PANTERA project (Article 6(1)(b) of the Regulation)	○ First name ○ Family name ○ Affiliation ○ Email	Stored until the completion of all the project obligations after the project end, i.e., until 2027. Email distribution lists for the project.
Purpose 3 **Participation to meetings in EC premises.**	Execution of the PANTERA project Access to the buildings of European Commission in Brussels during coordination meetings (Art. 6(1)(b) of the Regulation)	○ First name ○ Family name ○ Affiliation ○ Email ○ Nationality, Identity Card number ○ Identity Card validation date	From the meeting announcement until the meeting date.

TABLE 1: Purposes of the processing of personal data.

For purposes 1, 2 and 3 the legal basis is the Art. 6(1)(b) of the Regulation, i.e., data processing is necessary for the performance of a contract to which the data subject is party.

This represents the current status at the best of our knowledge. Any modifications will be promptly communicated.

2.3.5 Nature of data provision

The provision of personal data is optional. The refusal to provide data, however, makes it impossible to execute PANTERA project or to provide PANTERA project services.

In general, failure to communicate and / or refusal to provide the personal data outlined above will make it impossible to participate to the project and attend the project events. For Purpose 3, failure to communicate and / or refusal to reply will make it impossible to attend coordination meetings with the European Commission.

2.3.6 Method of the treatment and profiling

Method of the treatment

The processing carried out for the purposes indicated above are carried out both on paper and digitally. In any case, automated instruments, including in-house databases such as excel, access, institutional database, address books of email tools, and external repository: OnlyOffice for which DERlab has enterprise license providing compliance with the Regulation, ISO privacy standard and GDPR. How can OnlyOffic comply with GDPR can be found:

https://www.onlyoffice.com/blog/2018/05/how-onlyoffice-complies-with-gdpr/

For Purpose 1, they are also stored in paper archives and digital format according to Table 1.
The access to the data acquired for the aforementioned purposes is allowed to duly authorised personnel of the Controllers.

Profiling

Data profiling will be not applied.

2.3.7 Categories of recipients

In relation to the purposes indicated above, personal data may be disclosed to the following categories indicated below, in particular they may be disclosed to European companies and / or persons who provide Project services, also external to the project Consortium, on behalf of the Data Controllers.

- For Purposes 2:

o to advisory board members,

o EC representative persons (EC project officers, and EC project reviewers).

- For Purpose 3:

o to EC security services to access EC buildings.

2.3.8 Data storage lifetime

As indicated in Table 1, for the protection of the rights of the data subjects, once the prescription terms have elapsed, the personal data will be deleted

2.3.9 Transfer of data to Extra EU countries

Personal data will not be transferred or stored outside European Union or to those countries that will not provide an adequate security level (EDPS, 2019).

2.3.10 Rights of the data subject

At any time, the data subject can ask the Data Controller for:

- confirmation of the existence of her/his personal data;

- access to her/his personal data and information relating thereto; the correction of inaccurate personal data or the integration of incomplete personal data; the erasure data (upon the occurrence of one of the conditions indicated in Article 17(1) of the Regulation and in compliance with the exceptions provided in paragraph 3 of the same Article); the limitation of the processing of her/his personal data (upon the use of one of the grounds indicated in Article 18(1) of the Regulation), the transformation into anonymous form or the blocking of personal data processed in violation of the

law, including those that are not necessary conservation in relation to the purposes for which the personal data were collected or subsequently processed.

These rights can be exercised addressing to: Data Protection Officer <<lefteri@ucy.ac.cy>>

If the data subject considers that her/his rights have been violated by Data Controller and / or by a third party, she/he has the right to submit a complaint to the relevant supervisory authority for the protection of personal data and / or to another competent supervisory authority pursuant to the Regulation.

3 Data Archiving and Preserving Infrastructure

Before providing the detailed analysis of the datasets/publications to be handled within the context of PANTERA DMP, we provide an overview of the platforms to publish our results openly. The following list presents the platforms selected to present the datasets/publications during the project and describes their concepts for publishing, storage, and backup.

3.1 PANTERA Project Portal

The partners in the PANTERA consortium decided early to setup its own project-related webpage. This webpage describes the mission and the general approach of the project and its development status. A dedicated section for downloads is used to publish reports and white papers. All documents are published using the portable document format (PDF). All downloads are enriched by using simple metadata information like the title and the type of the document. The webpage will be designed and developed by the partner of the consortium DERlab e.V. All webpage-related data will be backed on a regular basis (once per month). All information on the PANTERA website can be accessed without creating an account, though a private section will also be available linked with the OnlyOffice account of the project.

The PANTERA Project Portal will be available during the project runtime and will still be available for at least two years after the official project end.

Web link: https://pantera-platform.eu/

3.2 Research Gate

Along with the establishment of the project portal, the PANTERA ResearchGate channel will be established to promote the dissemination of scientific publications of the project. Open Access documents are published using the portable document format (PDF). All downloads are enriched by using simple metadata information like the title, a short description and the type of the document.

The PANTERA ResearchGate channel is managed by DERlab e.V., a partner of the consortium who periodically updates the material. The link for accessing the PANTERA Research Gate channel is:

https://www.researchgate.net/project/PANTERA

The aforementioned tools are defined as the platforms for accessing the project scientific results. Towards the wider dissemination of project outcomes and following the recommendation from E.C., we intend to use OnlyOffice service for datasets dissemination.

3.3 OnlyOffice Project Repository

OnlyOffice is an online office suit integrated with a collaboration platform to manage documents, projects, team and customer relation in one place. It provides the customer with the most secure way to create, edit and collaborate on business documents online and its 100%compatible with Microsoft Office formats. OnlyOffice was developed by Ascensio System SIA which was founded in 2008. The headquarter of Ascensio System SIA is in Latvia. (https://www.cmswire.com/d/ascensio-system-sia-o001877)

DERlab installed and maintains OnlyOffice environment on a virtual server. The virtual server is hosted by a German professional web hosting provider named Hetzner Online GmbH.

The users for OnlyOffice must have a username and a password in order to access OnlyOffice platform. The minimum requirements for the password are eight characters, capital and small letters, digits and special characters.

OnlyOffice repository is secured by SSL (Secure Sockets Layer) certificate which allows secure connections from the web server to the browser.OnlyOffice is used as the main repository for PANTERA project where PANTERA partners can share and edit the project documents between the consortium.

Web link: https://derlab-repo.net/

4 Datasets and Publications for DMP

In this section, a list of all existing or foreseeable results for dissemination is presented, separated into public deliverables, publications and open research data. For each result and in accordance to the FAIR data management guideline (2. FAIR, 2013) we provide a description, name the standards used for storage and metadata (to make data findable & interoperable), and define which open access platform is chosen.

Data Security aspects are also defined in this document, while the detailed ethics management policy of PANTERA project is defined in Section 6 which provides detailed analysis on the way to handle the datasets generated in the project. In summary, the PANTERA partners will comply with the ethical principles as set out in Article 34 of the Grant Agreement, which asserts that all project activities must be carried out in compliance with E.U. legislation towards data handling and preservation, aligned with the recent E.C. GDPR requirements.

4.1 PANTERA Project Public deliverables

We are considering the PANTERA Project public deliverables as part of the data management plan. The following table presents the list of public deliverables of the PANTERA project.

Deliverable Number[14]	Deliverable Title	WP number[9]	Lead beneficiary	Type[15]	Dissemination level[16]	Due Date (in months)[17]
D1.1	Project guidelines	WP1	1 - FOSS	Report	Public	2
D1.2	Risk management report	WP1	1 - FOSS	Report	Public	3
D1.4	Quality Assurance Plan	WP1	1 - FOSS	Report	Public	3
D1.6 – D1.8	Project progress reports	WP1	1 - FOSS	Report	Public	18, 36, 48
D2.1	Report on stakeholder's identification and interaction	WP2	3 - RSE	Report	Public	20
D2.2	Report on Enhanced collaboration opportunities	WP2	8 - NUID UCD	Report	Public	42
D2.3 – D2.4	Reports on interactions with European platforms and organizations	WP2	3 - RSE	Report	Public	24, 48
D3.1	Report on current status and progress in R&I activities: Technology	WP3	7 - UCC-IERC	Report	Public	18
D3.2	Report on RCS in EU-28	WP3	7 - UCC-IERC	Report	Public	22

D3.3	Report on community energy policy and barriers	WP3	7 - UCC-IERC	Report	Public	24
D3.4	Initial report on key challenges and bottlenecks	WP3	7 - UCC-IERC	Report	Public	38
D3.5	Roadmap to 2030	WP3	7 - UCC-IERC	Report	Public	46
D4.1	Content and topics for dissemination and networking activities	WP4	4 - SINTEF	Report	Public	9
D4.2 – D4.3	Reports on Identification of gaps and missing subjects	WP4	4 - SINTEF	Report	Public	12, 30
D4.4	Assessment of the defined topics; relevance, driving forces and trends	WP4	4 - SINTEF	Report	Public	33
D5.1	Workshop Format	WP5	2 - DERlab e.V.	Report	Public	3
D5.2 – D5.3	Reports on the outcomes of regional Workshops	WP5	2 - DERlab e.V.	Report	Public	24, 48
D5.4 – D5.5	Reports on the outcomes of Pan-European and Global Workshops	WP5	2 - DERlab e.V.	Report	Public	24, 48
D6.1	Report on identification/selection of stakeholders within the national/regional desks	WP6	5 - IPE	Report	Public	3
D6.2	Stakeholder consultation plans (one for each country/region)	WP6	5 - IPE	Report	Public	5
D6.3	Consolidated summary report of desk activities in the target regions	WP6	5 - IPE	Report	Public	22
D6.4	Catalogue of potential solutions to overcome acceptance barriers for each country	WP6	5 - IPE	Report	Public	26

D7.2	Report on the promotion of Key Midterm R&I Priorities for Smart Grids	WP7	9 - TUS RDS	Report	Public	48
D7.3	Report on Appropriate Funding Instruments to ensure Project Sustainability	WP7	6 - Suite5	Report	Public	42
D7.5	Report on Preliminary Business Development Activities	WP7	6 - Suite5	Report	Public	48
D8.1	Dissemination, communication and cooperation plan	WP8	2 - DERlab e.V.	Report	Public	3
D8.2	Promotion and marketing material	WP8	2 - DERlab e.V.	Websites, patents filling, etc.	Public	4
D8.3	PANTERA Collaboration Platform: European Hub for Smart Grids	WP8	2 - DERlab e.V.	Websites, patents filling, etc.	Public	48
D8.4	Report on Dissemination and communication Activities	WP8	2 - DERlab e.V.	Report	Public	48

Table 1 List of PANTERA Public Deliverables

The template for the management of public deliverables is provided:

Data set reference and name: The name and the ID of the deliverable

Data set description: A short description of the content of the deliverable

Standards and metadata: The type of the document format and any type of metadata associated with the content of the document.

Data sharing, archiving and preservation (including storage and backup): how data will be preserved, how to archive and preserve the open datasets of the project.

An overview of the public documents prepared so far by the consortium are presented:

4.1.1 Project visual identity, website and media coverage (T8.3)

Data set reference and name

Promotion and marketing material (Report D8.2)

Data set description

The purpose of this report is to briefly document the PANTERA website design and deployment, as well as the creation of PANTERA accounts in popular social media. The design and implementation of the PANTERA website falls under the activities of WP8 “Dissemination and Communication activities”. According to the DoA, the objectives of WP8 are (among others) to establish an effective online presence and to communicate the project outcomes to the intended audiences, in a way that is consistent with the project’s branding and scope.

The project visual identity will consist of a project logo, general guidelines, as well as a presentation template, a document template and a project brochure/flyer.

The public website will be created and maintained by DERlab. It will serve as a basic tool for external communications and it will be updated regularly. The website will be suitable for different levels of interest and expertise: it will be attractive for both scientists and generally interested persons.

To ensure dissemination of the project activities and results to the wide public, several activities will be performed including media coverage by using dedicated PR platform for press releases, social media (e.g. dedicated professional LinkedIn account, Twitter, Facebook, YouTube channel), DERlab public activity report and dedicated newsletter.
The website will integrate the proposed European Hub for smart grids described in Task 8.1.

Standards and metadata

The report document is stored in the cross-platform portable document format (PDF). Metadata is added manually and includes the title, the partner organizations, and keywords that classify this report (PANTERA Website, Social Media Channels, etc)

Data sharing, archiving and preservation

The document will be published openly on the PANTERA webpage (following E.C. review and approval). The repository is backed on a regular basis by DERlab. The document will be added to OnlyOffice for long term preservation until the end of the project

4.1.2 PANTERA Collaboration Platform: Pan-European Hub for Smart Grids (T8.1)

Data set reference and name: PANTERA collaboration Platform: European Hub for Smart Grids (D8.3)

Data set description: The purpose of this report is to briefly document the PANTERA platform design and deployment. Within this task the aim is to update the existing database by integrating further research infrastructure available and enhance its functionalities, creating the proposed European Hub for smart grids. The Database of DER and Smart Grid Research Infrastructure contains systematic information on research infrastructure and related assets, testing capabilities and services of research institutes and organizations worldwide focusing on Distributed Energy Resources (DER) and Smart Grids. This database will also provide information with respect to provisional users’ access to specific research infrastructure or testing facilities available within Europe. New sections will be added to enhance the visibility of the Smart Grids: services, expertise, job market, scientific events announcements, studentships and internships, research opportunities, project collaboration offers, and a community forum. This will create a live science market place type webpage and the way to global hub for Smart Grids in the electrical energy domain.
Part of the dataset is the user registration data entered in the portal, allowing users to create accounts in order to be able to introduce additional project information in the platform or to gain the

needed privileges in order to be able to access specific research infrastructure or testing facilities available within Europe, as mentioned above.
Standards and metadata: The report document is stored in a cross-platform portable document format (PDF). Metadata is added manually and includes the title, the partner organizations, and keywords that classify this report (PANTERA platform, PANTERA webpage references, Social Media Channels)

Data sharing, archiving and preservation (including storage and backup): The document will be published openly on the PANTERA webpage (following E.C. review and approval). The repository is backed on a regular basis by JRC.
Any personal data collected from the PANTERA Platform and/ or the PANTERA portal, will be processed, in respect to the privacy policy, that will be made available in a dedicated page of the project portal/ platform and cited in Annex IV of the current deliverable.

Standards and metadata: The report document is stored in a cross-platform portable document format (PDF). Metadata is added manually and includes the title, the partner organizations, and keywords that classify this report (PANTERA platform, PANTERA webpage references, Social Media Channels)

4.2 Research Datasets

The analysis covers the datasets that set the inputs/ outputs of the project.

4.2.1 PANTERA Project – Datasets

We are presenting different data types to be considered as part of the Data Management Plan following the early identification of PANTERA datasets in WP1.

We are providing a typical template for datasets presentation within the context of DMP.

Data set reference and name: The name of the dataset **Data set description:** A short description of the content of the dataset **Standards and metadata:** The format utilized for making the datasets publicly available **Data sharing:** How the dataset will be preserved during the project period **Data archiving and preservation (including storage and backup):** How to archive and preserve the datasets of the project

An indicative example of open dataset is presented in the following section

<u>Available smart Grid project information and enhancements</u>

Data set reference and name

Available smart Grid project information and enhancements

Data set description

To be used as an input for the needs of PANTERA, project information already available will be exploited. A good example is data of Smart Grid Projects collected by the Joint Research Centre (JRC). The JRC started its data collection effort in 2010 with the launch of a survey that collected quantitative and qualitative data about smart grid projects in Europe, supplemented by additional

questionnaires and active search. All project info, including project name, state of development, Organization info, country of deployment, main application and funding details, will serve as an excellent basis for the creation of the PANTERA Collaboration Platform. Other than data available by JRC, additional smart grid project information sources will be verified, validated and used based on the project needs.
Enhancing the already available data in order to include details of technologies used, solution types, maturity and profitability levels as well as types of customers for all projects, is part of the targets of the PANTERA project. Identifying the mechanisms to be able to retrieve that information in order to make them part of the envisioned Pan-European Hub for smart grids will be handled throughout the project lifetime.

Standards and metadata
The data will be stored in a platform-independent format (e.g. XML or JSON). Any names or features that may be used for single user identification are removed at the data source layer and thus anonymous time-series data will be available. Part of the metadata extracted from the raw streams of data will be made also available, thus we need first to define the list of metadata generated in the project.

Data sharing
User-related data that may lead to single user identification will not be published. Only abstract data and statistics will be made openly accessible. Any anonymous user data (e.g. statistics) will be published openly. The access is free for everyone and without restrictions.

Archiving and preservation (including storage and backup)
The data types defined above are stored in project-related databases, which are hosted by the project partners. Considering privacy and security concerns, partner of the consortium restrict access to private information by following the security policy as defined in the project (Section 6). Databases are backed on a regular basis by each partner. The user statistics as defined for the DMP will be added to OnlyOffice for long term preservation during or at the end of the project.

4.3 PANTERA Scientific Publications

Along with the dissemination of project deliverables and datasets, we are considering as part of the Data Management Plan, further dissemination of project scientific publications.

There are no publications submitted yet by the consortium partners in scientific papers and conference events, though an indicative template for the management of scientific publications is presented; considering a draft publication prepared for the dissemination of PANTERA framework.

4.3.1 PANTERA Project Research Paper

Data set reference and name

PANTERA Project Research Paper

Data set description

This is a full report paper titled e.g. “PANTERA Paper” published by the partner of the consortium e.g. FOSS

The objectives of this publication are:

- To highlight the goal and the main objectives of the proposed framework

- To provide a blue print of the architecture defining the role of the different software components
- To present the demonstration environment of the project
- The overall framework as defined in the paper is in line with the definition of the PANTERA holistic framework as examined in the project.

Standards and metadata

The document is stored in the cross-platform portable document format (PDF). Metadata is added manually and includes the title, the partner organization, and keywords that classify this research paper. For indexing linked references, citable DOI numbers are added by the publisher.

Data sharing

This research paper is published in e.g. OnlyOffice. This is a green access publication and thus available for mass dissemination with no further publication restrictions. The paper will be available in ResearchGate channel of the project.

We presented above the project outcomes (public deliverables by the project consortium, research datasets, white papers published) towards communicating and spread the knowledge of project results to all interested communities and stakeholders. The overall methodology is linked with the definition of open repositories for data management and dissemination as defined in previous section. The next section is about the definition of the ethics management plan of the project.

5 Ethics Management Plan

Apart from the Data Management Plan as reported in previous section (with the main focus on the dissemination of project outcomes), we specify in this deliverable the ethics management plan. The definition of a concrete ethics management plan is part of the management work in the project; to address any concerns about handling personal or private data.

Towards this direction, the detailed methodology about ethics management is documented in this section (aligned with the recent E.C. GDPR requirements), further defining the means and mechanisms to be considered in order to be fully compliant with national and E.U. legislation.

5.1 Methodology

The PANTERA consortium is aware of the ethical, privacy and data protection issues which could be raised by the activities performed in the scope of the project, since it involves data collection. Thus, from the very beginning the consortium has decided to invest time and effort in order to ensure that the outcome of the Ethical Monitoring of the project will meet all the respective ethical rules and requirements. The methodology followed towards this direction comprises of 6 steps, which are analyzed below (see **Figure 3**).

Figure 3 PANTERA Ethical Monitoring Methodology

5.1.1 Legislation Overview

The first step of the overall approach was to investigate and study the laws which are associated with the activities of the project, namely the directives of the EU, for example the Charter of Fundamental Rights of the European Union, the European Convention on Human Rights, which

have been taken into consideration. Concisely, the legislation with which the PANTERA framework has to conform includes:

i. *European Union – ePrivacy Directive 2002/58/EC*
ii. *DIRECTIVE 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*
iii. *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*

5.1.2 Research in HORIZON 2020

The second step of the proposed framework includes a thorough investigation about the ethical guidelines for research projects in EU. Horizon 2020 must comply with ethical principles and relevant national, EU and international legislation, for example the European Code of Conduct for Research Integrity. This investigation has revealed the major concerns around data protection and privacy.

Ethics is dealt extensively in the Horizon 2020 legislation:

i. Horizon 2020 Rules for Participation: Ethics Reviews (Article 14)
ii. Horizon 2020 - Regulation of Establishment: Ethical principles (Article 19)
iii. Model Grant Agreement: Ethics (Article 34)
iv. The document “H2020 Programme Guidance How to complete your ethics self-assessment, Version 5.2 12 July 2016” summarizes the main information about the compliance with H2020 Ethic requirements.

5.2 Legislation Overview

The PANTERA project must abide by the European laws and directives as well as the national laws of the countries that are involved in other activities of the project. In this section, the reference to the new GDPR legislation is reported.

- ***E.U. legislation for General Data Protection Regulation- EU 2016/679***

Data Collection, Storage, Processing and data protection
In April 2016 the GDPR (2016/679) was finally approved by the EU Parliament. The regulation is on the on the protection of natural persons with regard to the processing of personal data and on the free movement of such data enforcement date: 25 May 2018 - at which time those organizations in non-compliance will face heavy fines. It replaces the Data Protection Directive 95/46/EC. The GDPR harmonizes data privacy laws across Europe, protects and empowers all EU citizens’ data privacy and reshapes the way organizations across the region approach data privacy.

Towards defining the detailed procedure for data collection, storage, protection, retention and destruction in the project the General Data Protection Regulation (GDPR) - is described below. The GDPR applies generally to processing the personal data of data subjects residing in the Union, regardless of the company's location. It also applies to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not. Very important: the GDPR strengthens Data Subjects rights and imposes strong penalties on breaches, dealing with personal data.

The GDPR introduces newly:

- Right to be Forgotten (Article 17)

The "right to be forgotten" entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure, as outlined in article 17 of GDPR, include the data no longer being relevant to original purposes for processing, or a data subjects withdrawing consent.

- Right to data portability (Article 20)

GDPR introduces data portability - the right for a data subject to receive the personal data concerning them, which they have previously provided in a 'commonly use and machine-readable format' and have the right to transmit that data to another controller.

- Privacy by Design (Article 23)

Privacy by design is part of a legal requirement with the GDPR. At its core, privacy by design calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition. Article 23 calls for controllers to hold and process only the data necessary for the completion of its duties (data minimization), as well as limiting the access to personal data to those needing to act out the processing.

- Penalties (Chapter 8)

Under GDPR, organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater). This is the maximum fine that can be imposed for the most serious infringements e.g. not having sufficient customer consent to process data or violating the core of Privacy by Design concepts. There is a tiered approach to fines e.g. a company can be fined 2% for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting impact assessment. It is important to note that these rules apply to both controllers and processors -- meaning 'clouds' will not be exempt from GDPR enforcement.

- Data Protection Officers

Currently, controllers are required to notify their data processing activities with local DPAs. Under GDPR it will not be necessary to submit notifications / registrations to each local DPA of data processing activities, nor will it be a requirement to notify / obtain approval for transfers based on the Model Contract Clauses (MCCs). Instead, there will be internal record keeping requirements, as further explained below, and DPO appointment will be mandatory only for those controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences. Importantly, the DPO:

- Must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices

- May be a staff member or an external service provider

- Contact details must be provided to the relevant DPA

- Must be provided with appropriate resources to carry out their tasks and maintain their expert knowledge

- Must report directly to the highest level of management

- Must not carry out any other tasks that could results in a conflict of interest.

The GDPR differentiates between roles: data processor and data controller (Chapter IV).

A controller is the entity that determines the purposes, conditions and means of the processing of personal data, while the processor is an entity, which processes personal data on behalf of the controller.

Essential legal principles of privacy in the GDPR are:

- Data Sovereignty

Data sovereignty is the concept that information which has been converted and stored in binary digital form is subject to the laws of the country in which it is located.

- Self Determination

The individual decides on the disclosure and use of his personal data (that explicitly covers the collection, storage, process and disclosure of personal data).

- Autonomy – (the way of handling personal data within the rights granted)

Enabling individuals to extent their privacy and protect them against interferences.

Main aspects of these principles are:

1. Subject of data sovereignty: Personal Data
2. Being holder of rights

a. Clear and specific right to inform – before, during and after the data process

b. Consent requirement

c. Right to correction

d. Right to erase

e. Right to restrict data process

f. Right to appeal – Not being object of pure automatic data process that have legal effect

3. Data controller and processor as holder of obligations

a. Fulfilling principles of data processing

b. Obligation to inform in intelligible and easy language, transparently with the key facts presented

4. Principles of data processing (Art. 5 GDPR)

a. Lawful, fairly and transparent data process

Personal data in GDPR:

According to Art. 4 I GDPR any information related to a natural person or 'Data Subject' that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, bank details, and posts on social networking websites, medical information, or a computer IP address.

Important is the relative meaning of personal data in context of the term identifiable. Art.4 sec. 1 GDPR differs between information referring directly and indirectly to an identifiable person. Relevant are two categories of data: Personal data and non-personal data. As the first term has already been mentioned, the second category can be divided into two further kind of data:

Anonymous data: Anonymous data are information that do not contain any information about a natural person. The person-related information has been cleared from the datasets. Such data do not fall under the scope of the GDPR and are not relevant in the legal assessment.

Pseudonymous data: Pseudonymisation of personal information is a procedure where person-related information is replaced by non-identifiers in order to ensure that these informational cannot be assigned to natural persons anymore.

GDPR Principles relating to processing of personal data are (Article 5):

Lawful, fairly and transparent data process

The data process is bound to the data protection principles, which represent the fundament on which the data process is executed. The data protection principles can be found in Art. 5 GDPR.

Data minimization

According to Art. 5 GDPR, data minimization requires that data are only processed due to a legitimate purpose at the time of collection. The data process shall be restricted to the minimum amount necessary to fulfil the pursuit purpose of the data process. According to this definition, the data process has to be appropriate, substantial and restricted to the minimum amount necessary.

Purpose limitation principle

Processing personal data is only allowed with prove of a particular, explicitly determined and lawful purpose and not for any other purposes afterwards.

Compatible further processing

Nevertheless, it is not excluded to process data on the base of different purposes. For processing personal data, it is recommended to gain the respective consent. Besides, according to Article 6 IV GDPR, processing data for a purpose other than the original purpose requires to be compatible, and vice versa not incompatible, with the original purpose. With regard to the wording of Art. 6 IV GRPD, "further processing" implies that subject is the extension of the current data process and not a new data process independent of the previous data processes. A new data process requires a new legal basis, whereas the extension of the current data process does not require a new legal basis, but a reasonable justification according to Art. 6 IV GDPR. Decisive criterion is compatibility. Insofar, the further processing of data is not restricted to the pure compatibility, but the decisive criterion whether data process derives from the original purpose.

Accuracy

Accuracy according to Art. 5 sec. GDPR means that personal data have to be objectively correct and if necessary to be updated. Thereby objectively correct means that all information about a person have to match with reality.

Restriction of storing data

In order to avoid long term storing, personal data have to collected and stored as long as it is necessary for the respective purpose. This constitutes a time limit for storing personal data. Whenever the purpose is reached, all personal data have to be erased from the data storage.

Integrity and Confidentiality

The data controller has to guarantee the safety and security of personal data during the data process. Thereby, he is fully responsible and so, according to this principle, obligated to implement suitable technical and organizational measures in order to prevent unintentional harm of personal data.

Lawful data processing

The GDPR strengthens the conditions for consent, as the request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

Further information can be found at the European Commission Webpage (https://www.eugdpr.org/ . The new legislation is standard all-around Europe.

While the laws establish some core principles both at European and National level, they do not establish clear lines for the field of research. The PANTERA consortium will abide by the above mentioned legislation and will act with respect to the rights of any human being that is involved in the project either as a participant or not. The Horizon 2020 rules define the ethical principles that PANTERA will follow throughout its lifecycle.

5.3 Ethical & Social Issues

This section describes the ethical and social issues that have been identified concerning the platform and the implementation of the PANTERA framework. These issues have been classified into four categories, which are analyzed below.

5.3.1 Privacy Control

The platform supervisor will provide to all people participating, detailed information about the undertaken procedures and the data handled. In this way, the users will get access and control over their own data whenever they want in order to ensure a crystal clear view on the way PANTERA handles personal data. Their initial interest has been stated and they will be further asked to sign a consent form (ANNEX II).

The conditions for consent have been strengthened under the new GDPR legislation, and thus the request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

5.3.2 Data Management

During the implementation of collaborative activities within the PANTERA framework, information about participants and their interaction with the platform will be collected, transmitted, shared, stored

and processed. According to the definition of the EU Directive 2016/680 and the recent GDPR legislation, these are personal data and their security must be ensured.

Ethical guidelines will be delivered in order to be adopted as well as, detailed information will be provided on the informed consent procedures that will be implemented in the project to inform platform users

5.3.3 Transparency

PANTERA framework will ensure the collection, storage, protection, of data collected by Research organizations or individuals, who will take part in the process of the project. Any breach or leak of data to irrelevant parties (e.g. supervisors, managers) may lead to transparency issues.

To that end, PANTERA Project would provide the necessary feedback in order to minimize the impact of that risk or any other similar. Furthermore, the Project in collaboration with platform coordinators will inform participants and relevant authorities on the details, the scope and the purposes of the data collection process in order to get an Ethical approval consent signed by them.

In addition, the PANTERA Project would ensure that data will be used only within the goals and objectives of the project. The goal of the project is not to use data for other reasons and this point will be also marked on the information content to be delivered on platform users.

5.3.4 Behaviour

The PANTERA consortium has taken into consideration the fact that some people may change their behavior and/or their professional performance when they know that they are being monitored. For that reason, the project's purpose and intentions have been made perfectly clear to all participants. In addition, the selection of the participants is based mainly on their high interest and willingness to participate in PANTERA project, pointing out that the participation in the project does not result in more work for the involved end users.

Furthermore, all participants will sign a consent form (ANNEX II) that will connect both sides (platform users and consortium members) with a form of a "confidentiality contract". In any way, the platform users are able to opt out of the project and the details are specified as part of a special document attached as part of the ethical plan (must be ensured that the employees have a real possibility to opt out of the project).

The ethical scope of the PANTERA project has received significant consideration from the very beginning, and as the projects unfolds and evolves it will be one of the aspects that will guide all the procedures. The ethics of the PANTERA framework will be carefully treated throughout the lifecycle of the project so that ethical risks will be appropriately addressed.

6 Conclusions

The objective of the document is to report the steps for data management which are to be followed during the execution of PANTERA project. The scope of the document is twofold: to define the detailed data management plan towards the dissemination of project outcomes and to report the detailed ethics management plan; specifying the ethics handling and preservation activities.

The current document gives a preliminary information about the data types used and generated by the project consortium partners including focus on the means of sharing data captured by PANTERA framework and further specifies the methods of data storage thus providing general view over the complete data management life cycle. As this report is generated at the early stage of the project execution is considered as a living document which will be further updated during the project life time if needed.

7 References

1. European Union. (2019). *Data Management*. Retrieved from ec.europa.eu: http://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-data-management/data-management_en.htm
2. FAIR. (2013). *FAIR Data Management in Horizon 2020.*
3. CA. (2019). *PANTERA Consortium Agreement.*

8 Annex

8.1 List of figures

8.2 List of tables

8.3 Annex I – Ethics Manual Documentation

8.3.1 Scope of the ethics manual

The current Ethics Manual has been produced by the PANTERA consortium towards the diffusion and establishment of all the ethical guidelines that should be taken into consideration during the platform implementation, where final users will be involved, and data collection is going to take place. The manual will be constantly updated throughout the whole duration of the project based on new ethical issues or problems that may arise. The final version of the ethics manual will provide all the needed information and guidelines for the topics addressed by the proposed framework.

This document is intended, first of all, for all the project staff that will participate in the platform preparation and realization. Software developers, managerial and technical staff members should carry all their activities in accordance with the guidelines outlined here. Secondarily, the manual is directed to all the people involved in the project and especially to final users, who are the ones actually participating in the platform and may want to be further informed about the guidelines adopted by the project.

8.3.2 Platform infrastructure

For the need of the platform realization and assessment, existing databases will be utilized and further enhanced, by integrating further research infrastructures available and by improving its functionalities. The main goal of this project is to provide easy access to the details of past and ongoing Smart Grid Research activities. Information captured in the PANTERA platform, project specific details or user registration data, will be handled according to the definition of the EU Directive 2016/680 and the recent GDPR legislation.

Based on the recent legislation, there is no mandate to contact the local ethical committees about the project activities. Nevertheless, the consortium will be fully transparent to external ethical committees and disseminate any ethics related issue through the PANTERA local partners.

It is essential to protect the rights and the privacy of all the participants. To that end, this Ethics Manual has been composed by the PANTERA consortium including all the necessary ethical and privacy guidelines in order to inform all involved parties towards preserving the privacy of the user, protecting his/her personal data and limiting the risk of interception to the minimum. This document will be constantly updated throughout the whole duration of the project.

8.3.3 Legislation

The PANTERA project must abide by the ethical rules of the EU. More specifically, the legislation that the PANTERA framework has to conform with is:

- *European Union – Directives 2002/58/EC & 2016/680 & new GDPR legislation*
- *Horizon 2020 Ethics Legislation (mentioned in 6.1.2)*

8.3.4 Guidelines

8.3.4.1 Personal Data

Personal Data (GDPR reference) must be:

- processed fairly and lawfully;
- collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that appropriate safeguards are established;
- adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality').

8.3.4.2 Acquisition and storage of human related information

- No sensitive personal data should be collected. In no case more personal data should be collected than the necessary ones, according to the requirements of European and National legislation.
- No personal data should be centrally stored, but they should be scrambled where possible and abstracted in a way that will not affect the final project outcome.
- No data should be collected without the explicit written consent of the occupants under observation (group-based and individual scenarios).
- No data collected should be sold or used for any purposes other than the current project.
- A data minimization policy should be adopted at all levels of the project and should be supervised by the respective ethical/privacy component. This will ensure that no data which is not strictly necessary to the completion of the current project will be collected.
- Any shadow (ancillary) personal data obtained during the course of the research should be immediately cancelled. However, this kind of ancillary data should be minimized as much as possible. Special attention should also be paid to complying with the Council of Europe's Recommendation R(87)15 on the processing of personal data for police purposes, Art.2 :
    - "The collection of data on individuals solely on the basis that they have a particular racial origin, particular religious convictions, sexual behavior or political opinions or belong to particular movements or organizations which are not proscribed by law should be prohibited. The collection of data concerning these factors may only be carried out if absolutely necessary for the purposes of a particular inquiry".
- The burden for enrolled subjects should not be superior to that imposed by participation in standard market research.
- The research to be conducted should be in full compliance with the principles and guidelines of ethics for research projects in Horizon 2020 framework.

8.3.4.3 Collection of data from participants

The platform supervisor or his/her representative must provide participants from whom data related to themselves are collected with at least the following information, except where he/she already has it:

- the identity of the controller and of his/her representative, if any;
- the purposes of the processing for which the data are intended;
- any further information such as
    - the recipients or categories of recipients of the data,
    - whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,
    - the existence of the right of access to and the right to rectify the data concerning them

in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing.

Overall, derived from the GDPR regulation ((EU) 2016/679) PANTERA commits to perform a clear process towards managing any possible ethical concerns related to Data Management, namely.

1. The research to be conducted will be carried out in full compliance with the principles and guidelines of the PANTERA Grant Agreement, Article 34 on Ethics and Research Integrity.
2. PANTERA will assign dedicated “Data Controllers” and “Data Processors” as soon as the platform design is ready and name them personally.
3. The Data Controllers must:
    a. guarantee that the collected data will be only used for the purposes of the project and they will not be sold or used for other activities.
    b. guarantee that no personal or sensitive data will be centrally stored. In addition, data will be scrambled where possible and abstracted in a way that will not affect the final project outcome.
    c. guarantee that no data collected will be sold or used for any purposes other than the current project
    d. guarantee that any ancillary data obtained during the course of the research will be immediately cancelled. However, the plan is to minimize this kind ancillary data as much as possible. In particular the names of the research participants will not be made public and their participation will not be communicated to. Any incidental findings will be kept strictly confidential and erased from files under request from the enrolled subject.
    e. inform the participants about all data that will be collected and the purpose of that;
    f. provide their personal contact data to the participants and will be available to further explanation on the data collection and management;
    g. implement appropriate technical and organizational measures (e.g. PET technologies) to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing
    h. ensure that no data will be collected without the explicit written consent of the participants
    i. describe the way the data is supposed to be handled in a detailed way and set the consent forms for the end users to participate in the demonstrator.
4. Data Processors will ensure that:
    j. Collected data will be saved on secured servers,
    k. will not be available to anyone outside the project’s team;
    l.

8.3.4.4 Rights of Participants

Taking into account the most recent legislation, the information that must be made available to a Data Subject when data is collected has been strongly defined and includes;

- the identity and the contact details of the controller and DPO
- the purposes of the processing for which the personal data are intended
- the legal basis of the processing
- where applicable, the recipients or categories of recipients of the personal data
- the period for which the personal data will be stored, or if this is not possible, the criteria used to determine this period
- the existence of the right to access, rectify or erase the personal data;
- the right to data portability
- the right to withdraw consent at any time
- and the right to lodge a complaint to a supervisory authority

Overall,

- Participants will have the right to access their personal data.
- Participants will be able to revoke their participation at any point, if they wish, without any consequences. He/she can exercise his/her right to access, correct and delete his/her data at any moment also rectify or erase the personal data.
- Participants will enroll the platform in a voluntary basis and support activities of the project to the extent of their availability for their participation in PANTERA Project.

Moreover, every participant has the right to obtain from the platform Supervisor without constraint at reasonable intervals and without excessive delay or expense:

- confirmation as to whether or not data relating to him/her are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,
- communication to him/her in an intelligible form of the data undergoing processing and of any available information as to their source,
- knowledge of the logic involved in any automatic processing of data concerning him/her;
- as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Manual, in particular because of the incomplete or inaccurate nature of the data;
- notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking, unless this proves impossible or involves a disproportionate effort.

The participant has the Right to Object:

- at any time on compelling legitimate grounds relating to his/her particular situation to the processing of data relating to him/her, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the platform, may no longer involve those data;
- to object, on request and free of charge, to the processing of personal data relating to him/her which the platform user anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

8.3.4.5 Data Confidentiality and Security

- Any person acting under the authority of the data processor, including the processor himself/herself, who has access to personal data must not process them except on instructions from the controller, unless he/she is required to do so by law.
- The controller must implement appropriate technical and organizational measures (e.g. PET technologies) to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.
- Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

The regulation provides specific suggestions for what kinds of security actions might be considered “appropriate to the risk,” including:

- The pseudonymization and/or encryption of personal data.
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data.
- The ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident.
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

Especially for pseudonymization, we are adopting the principles of the new GDPR legislation towards keeping the de-identified data (tokenized datasets) separately from the “additional information,” then the GDPR permits data handlers to use personal data more liberally without fear of infringing the rights of data subjects. This is because the data only becomes identifiable when both elements are held together.

8.4 Annex II – PANTERA Participant's Consent Form

PANTERA Participant´s Consent Form

Name of Participant:

E-mail:

Purpose of the project

This data collection is part of research activities within the larger context of a research project from the Energy field named **PANTERA -** Pan European Technology Energy Research Approach. For more information see the PANTERA Website: *https://www.pantera-platform.eu//*. The research to be conducted aims to be in full compliance with EU REGULATION 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and Directive *2002/58/EC* (*ePrivacy Directive*) and the most recent GDPR regulation.

Purpose of Research: The PANTERA project will provide a Pan-European Hub for smart grids by improving existing databases and by integrating further research infrastructure available into it. Such improvements on systematic information of research infrastructures and related assets, will augment the visibility of the Smart Grids for all interested stakeholders.

In this context, it is necessary to collect data about project details like project name, state of development, organization info, country of deployment, main application, funding details services, expertise, job market, scientific events announcements and the IT infrastructure for a community forum, etc.

To this end, you are asked to participate as a platform user in PANTERA project and provide project relevant information in the platform, in order to be able to analyze this data and extract some statistics and indicators. That information will further facilitate the demonstration of the benefits of Smart Grid research activities and foster continuous information, experience, knowledge and best practices exchange among all participants.

Participants will be able to quit the platform at any point, if they wish, without any consequences. In addition, the participants can exercise their right to access, correct and delete his/her data at any moment.

Duration of the Research Activities: The Research Activities last from January 2019 to December 2022.

Risks or Inconveniences: No risks are foreseen. You are only requested to be available to participate.

Privacy and Confidentiality: As a voluntary participant in the PANTERA platform your recorded data will not include any personal identification; hence it will not be possible to identify you afterwards. Information will be held and used on an anonymous basis only for the purpose of the project PANTERA on research servers at DERlab e.V. (Germany) (or JRC) for processing.

Benefits: The result of the platform utilization is to develop a multi-functional collaborative platform as an interactive forum of all the partners through which all activity will be conducted making use of readymade tools for analysis, scenario building, case study synthesis and generation of useful replication ideas for growth and expansion.

Data destruction: After the end of the project the data will be only accessible to the European Commission until a 5 year period has passed. After this period the data will be destroyed.

Contact persons: Your participation is voluntary, consent can be refused, and withdrawal is possible at any time per email to either the scientists in charge **XXX XXX (email xxx@xx.xx, phone +XXXXX) or XXXX (XXX, email** XXXX**, Phone XXXXX).** You can also obtain information and ask for rectifying it. If you decide to exercise your rights, including the withdrawal from the project, please contact the PANTERA scientists in charge, and they will explain the best way for you to exercise them or stop taking part.

In the next pages of this document is the consent form for the data collection through measurements in your workplace is provided.

Voluntary Participation Form for the needs of PANTERA project

1. Participant's Questionnaire

I have been informed about the purpose, the expected duration and the procedures of the project	**Yes**	**No**
I have been informed about the potential benefits of the project.	**Yes**	**No**
I have been informed about my right to deny participating or to quit from the project and about the corresponding consequences.	**Yes**	**No**
I have been informed that participation in the project will not result in more work due to my participation in the evaluation phase	**Yes**	**No**
I have been informed about the contact person in case that I have questions and queries about the project.	**Yes**	**No**
I have been given a copy of my consent.	**Yes**	**No**
I had adequate time to make my decision concerning my participation in the project.	**Yes**	**No**
I comprehend that I can quit from the project at any time without having to justify my decision.	**Yes**	**No**
I have been informed about potential effects, difficulties and dangers	**Yes**	**No**
I have been informed about the security of the project data and results.	**Yes**	**No**

I have been ensured about the confidentiality of my personal information. Publications of the project results do not allow the personal data recognition, due to the principle of anonymity.	**Yes**	**No**
I have been ensured that the data will be used within the scope of the project and no incidental findings are expected within the project.	**Yes**	**No**
I have been informed that no extra work is required through my participation and the overall involvement is part of my daily activities	**Yes**	**No**

I agree to participate in the project.	**Yes**	**No**

Date: _____ Signature:_____

* A simpler version of the consent form is available for the control group (baseline group) of users participating in the project.

8.5 Annex III – PANTERA Participant's Opt Form

PANTERA Participant´s Opt Out Form

Complete this form to opt-out (decline participation in) the PANTERA project.

Please print or type clearly.

Section 1: Participant Information

Name of Participant: _____

E-mail: _____

Section 2: Participant Acknowledgement and Signature

By signing this form, I have exercised my rights as the PANTERA Participant to OPT OUT of the project without any consequences.

I have read the information and understood the above form; I hereby confirm my election to NOT participate in the PANTERA project.

Date: _____ Signature: _____

8.6 Annex IV – PANTERA Privacy Policy

PERSONAL DATA PROTECTION

DESIGNATIONS

Partners / partnership: In the following text, “partner” / “partnership” designate partner institutions / organisations participating in **PANTERA** and likely to collect data within the framework of the project, namely ***University of Cyprus (FOSS), European Distributed Energy Resources Laboratories e.V. (DERlab e.V), Ricerca Sul Sistema Energetico – RSE SPA (RSE), Sintef Energi AS (SINTEF), Fizikalas Energetikas Instituts (IPE), Suite5 Data Intelligence Solutions Limited (Suite5), University College Cork – National University of Ireland, Cork (UCC-IERC), University College Dublin – National University of Ireland, Dublin (NUID UCD), Technical University of Sofia (TUS RDS).***

Supervisory Authority: independent public authority established by a member State under article 51 of the GDPR. The Supervisory Authority will be updated in the next periodic report as soon as JRC agrees with PANTERA on their cooperation. The list of Supervisory Authorities is available here: https://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm

The **PANTERA** project partners carefully treat all data collected as confidential and strictly use it under the framework of **PANTERA** project activities in compliance with the EU legal regulations and the H2020 Programme rules.

All data collected and managed under the activities of the **PANTERA** project, namely accounts, newsletter subscribers, event registrations, surveys of any kind, is in strict compliance with the new Regulation (EU) 2016/679, General Data Protection Regulation.

The partnership appointed **Mr.** CHARALAMBOUS ELEFTHERIOS having been elected among the partnership to act as DPO, to act as **PANTERA** Data Protection Officer.

WHO IS CONCERNED BY THIS NOTICE?

This notice is addressed to the following public:

- All partners participating in the **PANTERA** project;
- respondents to surveys;
- registered participants in events;
- account owners in the exchange areas of the project website;
- newsletter subscribers of any outsourced database application.

FOR WHAT PURPOSES DOES THE PANTERA PROJECT STORE YOUR DATA?

Project partners collect data to perform their legal obligations as an EU co-funded project.

The scope of the data collected is the minimum necessary for each purpose, avoiding as much as possible personal information. However, no personal information is collected without the knowledge and consent of the target audience.

No data will be shared with third parties outside the project and the European Commission, other than the external providers or used for unintended purposes without the express consent and prior notification to the interested individuals. When personal data is collected, the purpose will be clearly expressed.

The data collected within the framework of the **PANTERA** project will be retained by the project partners and the H2020 Programme until 31/12/2027. Once the retention period has passed, the **PANTERA** project partners, potential sub-contractors / external providers will take adequate measures to delete all personal data collected within the project or extend their use, after receiving respective consent by the data providers, as part of the post-project exploitation activities of the project

WHAT ABOUT COOKIES AND TRACKING TECHNOLOGIES?

The **PANTERA** web platform collects and stores information using cookies and similar tracking technologies to track web behaviours. We use this information to provide analytics of only statistical nature.

WHAT ARE YOUR LEGAL RIGHTS AS DATA SUBJECT?

Every person may directly require from an organisation holding information about them the data to be corrected (if they are wrong), completed or clarified (if they are incomplete or equivocal), or erased (if this information could not legally be collected).

Anyone may oppose that information about them is used for advertising purposes or for commercial purposes;

They may also oppose to information concerning them being disclosed to a third party for such purposes. The persons concerned should have the possibility of exercising their right to oppose the disclosure of their data to a third party at the moment the data is collected. The use of automatic calling machines or faxes for advertising purposes is prohibited unless the person has given their prior consent.

If you believe that the processing of your personal data constitutes a violation of the legislation in force, you have the possibility to lodge a complaint with the supervisory authority concerned. (check here: https://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm)

List of the data subject rights as stated in the Chapter 3 of the GPDR:

- Transparency and modalities
- Information and access to personal data
- Rectification and erasure
- Right to object and automated individual decision-making

WHAT TYPE OF DATA IS COLLECTED AND HOW?

The project partners store data of different types and in several ways:

E-mail, postal and telephone contacts;
Newsletters subscription;
Event registrations;
Surveys;
Contact forms;
Data collected through the **PANTERA** web site;

WHO CAN YOU CONTACT FOR QUESTIONS REGARDING DATA PROTECTION?

For questions or concerns regarding the collection of your personal data within the **PANTERA** project, please contact the Data Protection Officer: **(**lefteri@ucy.ac.cy**)**