Innovation Action

H2020-SU-DS-2018-2019-2020 (Digital Security)

Topic: SU-DS04-2018-2020

PHOENIX

Electrical Power System's Shield against complex incidents and extensive cyber and privacy attacks

Deliverable D4.1
PRESS Framework Analysis

Authors	Elena Sartini (CEL), Luigi Briguglio (CEL), Carmela Occhipinti (CEL), Antonio Fiorentino (CEL), José Ramon Martinez (ATOS IT)
Nature	Report
Dissemination	Public
Version	1.1
Status	Deliverable
Delivery Date (DoA)	30/06/2020
Actual Delivery Date	30/06/2020

Keywords	Data Protection, Ethics, Privacy, Social Acceptance, EPES
Abstract	This deliverable will analyse the EPES related Privacy, Data Protection, Ethics, Security and Societal implications to be addressed by PHOENIX Project.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 832989

DISCLAIMER

This document does not represent the opinion of the European Commission, and the European Commission is not responsible for any use that might be made of its content.
This document may contain material, which is the copyright of certain PHOENIX consortium parties, and may not be reproduced or copied without permission. All PHOENIX consortium parties have agreed to full publication of this document. The commercial use of any information contained in this document may require a license from the proprietor of that information.
Neither the PHOENIX consortium as a whole, nor a certain party of the PHOENIX consortium warrant that the information contained in this document is capable of use, nor that use of the information is free from risk, and does not accept any liability for loss or damage suffered using this information.

	Participant organisation name	Short	Country
01	Capgemini Technology Services	CTS	France
02	THALES SIX GTS FRANCE SAS	TSG	France
03	THALES Research & Technology S.A.	TRT	France
04	SingularLogic S.A.	SiLO	Greece
05	DNV-GL AS	DNV	Norway
06	INTRASOFT International S.A.	INTRA	Luxemburg
07	Iskraemeco	ISKRA	Slovenia
08	Atos SPAIN SA [Terminated]	ATOS	Spain
09	ASM Terni	ASM	Italy
10	Studio Tecnico BFP srl	BFP	Italy
11	Emotion s.r.l.	EMOT	Italy
12	Elektro-Ljubljana	ELLJ	Slovenia
13	BTC	BTC	Slovenia
14	Public Power Corporation S.A.	PPC	Greece
15	E.ON Solutions Gmbh [Terminated]	EON	Germany
16	Delgaz Grid SA	DEGR	Romania
17	Transelectrica S.A.	TRANS	Romania
18	Teletrans S.A.	TELE	Romania
19	Centro Romania Energy	CRE	Romania
20	CyberEthics Lab	CEL	Italy
21	GridHound GmbH [Terminated]	GRD	Germany
22	Synelixis Solutions S.A.	SYN	Greece
23	ComSensus	CS	Slovenia
24	AALTO-KORKEAKOULUSAATIO	AALTO	Finland
25	Rheinisch-Westfälische Technische Hochschule Aachen	RWTH	Germany

26	Capgemini Consulting [Terminated]	CAP	France
27	ATOS IT Solutions and Services Iberia SL	ATOS IT	Spain
28	DNV GL NETHERLANDS B.V.	DNV-NL	Netherlands

ACKNOWLEDGEMENT

This document is a deliverable of PHOENIX project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement Nº 832989.
The opinions expressed in this document reflect only the author's view and in no way reflect the European Commission's opinions. The European Commission is not responsible for any use that may be made of the information it contains.

Document History

Version	Date	Contributor(s)	Description
V0.1	12-02-2020	CEL	Table of Content
V0.2	13-03-2020	CEL	Progress drafting
V0.3	20-04-2020	CEL	Progress drafting
V0.4	24-06-2020	CEL	Completion of first draft
V0.5	24-06-2020	CEL	Submission for peer review
V0.6	26-06-2020	CS, EMOT, and WP4 team	Integration of comments/feedbacks from peer reviewers and other WP4 Partners
V0.7	30-06-2020	CTS	Quality peer review
V1.0	30-06-2020	CEL and CTS	Submission
V1.1	30-06-2021	CEL	Resubmission – based on review feedback, fixed the references

Document Reviewers

Date	Reviewer's name	Affiliation
26-06-2020	Francesco Bellesini	EMOT

26-06-2020	Miha Smolnikar and David Carro Santomé	CS

Table of Contents

Definitions, Acronyms and Abbreviations 5
Executive Summary 8
1. Introduction 10
1.1. Relation to Project work 10
1.2. Structure of the document 11
2. Privacy and Data Protection Requirements 12
2.1. Privacy and Data Protection legal framework 12
2.2. Privacy Methodology 15
2.3. Privacy and Data Protection potential concerns 17
3. Ethics and Social Requirements 20
3.1. Ethics and Social Framework 20
3.2. Ethics and Social Methodology 22
3.3. Ethics and Social potential concerns 24
4. Security Requirements 25
4.1. Security legal framework 25
4.1.1. The Directive on Security of Network and Information System 25
4.1.2. Cybersecurity Act 29
4.2. Security Methodology 29
4.3. Security potential concerns 31
5. Compliance rules and Governance policies 32
6. Conclusions 36
7. References 37

Definitions, Acronyms and Abbreviations

AMI	Advanced Monitoring Infrastructure
API	Application Programming Interface
CA	Consortium Agreement
Charter	Means the Charter of Fundamental Rights of the European Union
Consortium	Means the consortium created by the execution of the CA
Convention 108	Convention for the protection of individuals with regards to the processing of personal data
CSIRT	Computer Security Incident Response Team
DMP	Data Management Plan
DoA	Description of Actions
DPA	Data Protection Authority
DPO	Data Protection Officer
EC	European Commission
EC-GA	European Commission Grant Agreement
ECHR	European Convention of Human Rights
ECSO	European Cyber Security Organization
EPES	Electrical Power and Energy System
ERx	Ethics Requirements x
ETHRx	Ethics Threats x
ETSI	European Telecommunications Standards Institute
EU	European Union
FAIR	Findable, Accessible, Interoperable and Re-usable
GDPR	EU General Data Protection Regulation no. 2016/679
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force

LSP	Large Scale Pilot
MNGT	Data derived from management activities
NIS Directive	Directive on Security of Network Information System EU 2016/1148
OEP	Operator of Essential services
Partners	Means the PHOENIX partners as indicated within the CA
PC	Project Coordinator
PET	Privacy Enhancing Technology
PHOENIX	Electrical Power System’s Shield against complex incidents and extensive cyber and privacy attacks
PLC	Programmable Logic Controller
PM	Project Manager
PMT	Project Management Team
POPD	Protection of Personal Data
PRx	Privacy Requirements x
PTHRx	Privacy Threats x
Project	Means the PHOENIX Project
Prosumption	Production by consumers
QEG	Quality Evaluation Group
QMR	Quarterly Management Report
QUEST	Data derived from DMP questionnaire
RTU	Remote Terminal Unit
SCADA	Supervisory control and data acquisition
SGAM	Smart Grid Architecture Model
SRx	Security Requirements
STHRx	Security Threats x
TEST	Data derived from test
TFEU	Treaty of Functioning of the European Union

THREAT	Data derived from threats analysis
TL	Task Leader
TM	Technical Manager
WP	Work Package
WPL	Work Package Lead
WPMP	Work Package Management Plan

Executive Summary

The present deliverable D4.1 – PRESS Analysis Framework aims to provide a comprehensive regulatory framework to the PHOENIX project, paying particular attention to privacy and data protection as fundamental rights (as well as requirements), ethics, security and other social concerns (i.e. societal acceptance).

In light of the above, having in mind the structure of the Project as a whole, the present document will recall the analysis presented within deliverables pertaining to WP9 concerning the Ethics Requirements, as well as chapter 7 of deliverable D1.1 – Identification of existing threats and data privacy requirements. Moreover, the present document will reflect parts of the ongoing activities of monitoring and assessment performed within Task 1.4 - Data Privacy & GDPR requirements Analysis, already partly reflected in D1.1 – Identification of existing threats and data privacy requirements.

As per its structure, the core of the present deliverable is composed by 3 pillars (Chapter 2 (*Privacy and Data Protection Requirements*) Chapter 3(*Ethics and Social Requirements*), and Chapter 4 (Security Requirements)), each of them dedicated to identify those requirements regarding that specific topic, whereby it will be illustrated (i) the regulatory framework, (ii) the methodology to identify the requirements and (iii) the assessment of the requirements illustrating potential threats or concerns. Then Chapter 5 (*Compliance rules and Governing policies*) provides the PHOENIX project with a practical set of compliance rules and governance policies for each requirement identified and described in the 3 pillars. These compliance rules and governance policies will be implemented by the DevSecOps process among the whole project lifecycle.

The structure and the outcomes of the document is illustrated in the Figure 1.

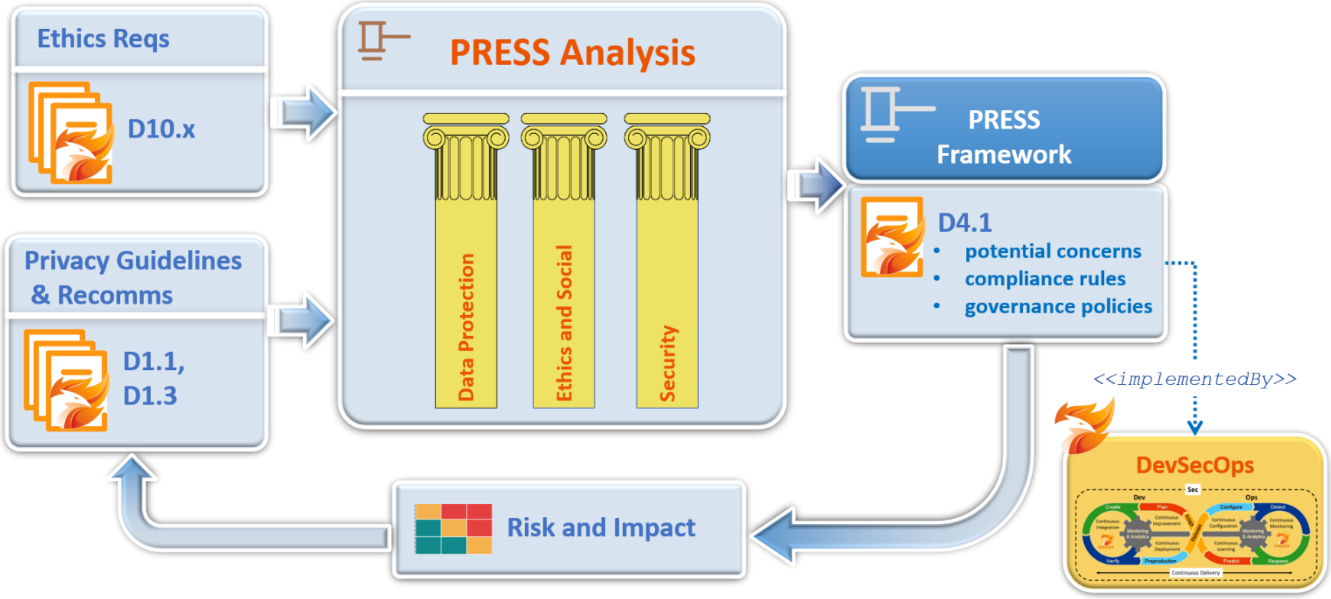

Figure 1: PRESS Framework Overview

It should also be noted that each chapter, or pillar, of the document shall be read in conjunctions with the others, which therefore cannot be read and analyse as separate and independent among each other, but rather aiming at providing a complete and over comprehensive picture of the regulatory framework.

1. Introduction

The PHOENIX Project focuses on the protection of the European end-to-end EPES (from energy production to prosumption) via prevention, early detection and fast mitigation of cyber-attacks against EPES assets and networks and from (intentional and unintentional, internal and external) human activities, while protecting the utilities and end-users' privacy from data breaches by design. The challenge of the Project is to provide a cyber-shield armour to European EPES to survive coordinated, large scale cybersecurity and privacy incidents; guarantee the continuity of operations and minimize cascading effects in the infrastructure itself, the environment and the end-users at reasonable cost. The Project aims to produce a complete EPES security and privacy protection framework, validated by real world scenarios by the means of 5 Large Scale Pilots (hereinafter "**LSPs**").

1.1. Relation to Project work

The general indications for the Project deployment have been defined in the European Commission Grant Agreement (EC-GA), the Description of Action (DoA) and the Consortium Agreement (CA). The present deliverable **D4.1 – PRESS Framework Analysis** – as well as the other deliverables – does not replace any of these established agreements and Project deliverables, and Partners should abide by the order of precedence reported in Table 1.

Table 1: Order of precedence of PHOENIX agreements and deliverables

1	European Commission Grant Agreement (EC-GA)
2	Commission Rules
3	Consortium Agreement (CA)
4	Project Handbook
5	D10.1: H – Requirement No.1
6	D10.2: H – Requirement No.2
7	D10.3: H – Requirement No.3
8	D10.5: POPD – Requirement No.5
9	D10.4: POPD – Requirement No.4
10	D10.6: POPD – Requirement No. 6
11	D10.8: POPD – Requirement No. 8
12	D7.1 – LSP Data Management Plan
13	D1.1 - Identification of existing threats & data privacy requirements

1.2. Structure of the document

The document is divided into the following chapters:

Table 2: Structure of D4.1 – PRESS Framework Analysis

	Chapter title	**Summary**
Chapter 1	Introduction	It provides a brief explanation on the objectives of the PHOENIX Project, the present deliverable and on the structure of the present document.
Chapter 2	Privacy and Data Protection Requirements	It provides the analysis of the regulatory framework on Privacy and Data Protection, allowing to identify relative requirements, potential concerns and applicable rules and policies.
Chapter 3	Ethics and Social Requirements	It provides the analysis of the ethics and regulatory framework on Ethics and Social Acceptance, allowing to identify relative requirements, potential concerns and applicable rules and policies.
Chapter 4	Security Requirements	It provides the analysis of the regulatory framework on Security, allowing to identify relative requirements, potential concerns and applicable rules and policies.
Chapter 5	Compliance rules and Governance policies	It provides the overall and integrated view of the compliance rules and governance policies to be implemented by the Project during its whole lifecycle.
Chapter 6	Conclusions	It provides the conclusions of this deliverable and the follow up of its outcomes.
Chapter 7	References	It provides the list of references used for the preparation of this deliverable.

2. Privacy and Data Protection Requirements

The results and the outcomes of the PHOENIX Project might impact (either positively or negatively) some of the fundamental rights recognised at EU and national level within the Member States.

In particular, considering that the Project deals with smart grid and the development of a cyber-security shield against cyber threats, it appears necessary to preliminary analyse privacy and data protection as fundamental rights, which in light of their status have been declined within EU and Members States legislation. Consequently, the protection of privacy and personal rights become specific legal requirements that the Project must comply with, during the Project itself, but also in terms of outcomes.

Without prejudice to the above, in any case attention will be paid also to those other fundamental rights that might be impacted by the PHOENIX Project, as provided within the Charter of Fundamental Rights of the European Union (hereinafter, the "**Charter**").

As a consequence, in the present chapter, after an introduction on privacy and data protection as fundamental rights, it will be then briefly recalled the principles of the GDPR that will be identified as "privacy requirements" that will be satisfied by the implemented IT solutions, having regard also to the provisions set forth within the EU Directive 2019/944 (the "**Electricity Directive**"). Moreover, considering the interdependencies of this deliverable with others Project's documents and reports, the same chapter will refer to chapter 7 of D1.1 – Identification of existing threats and data privacy requirements where a first set of general requirements/set of recommendations concerning privacy and smart grid had been formulated already at month 6 of the Project (i.e. February 2020) but that today, in light of the progress and development of the PHOENIX IT architecture can be refined.

2.1. Privacy and Data Protection legal framework

The identification of the privacy and data protection requirements whose compliance will characterize the PHOENIX Project during its life, as well as its outcomes, should start considering the following.

First, smart grid and smart meters belong to complex IT infrastructures that, to properly functioning, require not only to gather, collect and analyse data, but also to exchange the same data with other IT infrastructures (and ultimately with competent and responsible individuals appointed to monitor and potentially intervene on the same). In that respect, considering the source (i.e. household premises, electric vehicle power grids etc.) from which such data will be gathered/collected/extracted it is possible that among those data also personal information, i.e. personal data[1], might be included in the information exchange cycle. Assumed that, it should also be considered that the main objective of PHOENIX is to develop a cyber-shield able to protect the smart grid infrastructure from human and non-

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

human cyber threats, intentional or unintentional, able to early detect and avoid (or mitigate in the worst-case scenario) threats/attacks directed towards smart grid, considered by the EU as critical infrastructure. As a consequence, it appears that it is utterly important for PHOENIX and its Partners to develop technology solutions able to protect, on one side, the cyber-security of the smart grid infrastructure and, on the other side, the privacy and the protection of the personal data injected in the smart grid, which might be then analysed to protect the same smart grid by the PHOENIX infrastructure. In other words, it is necessary that the PHOENIX Project performs what is called a balancing operations among two (apparently) conflicting interests: privacy and data protection from one side, and security on the other side.

The second element to take into consideration is represented by the fact that privacy and data protection rights are two fundamental rights recognized either at European level and at International level. In particular, the inclusion of the protection of personal data in EU primary legislative texts such as the Treaty of Functioning of the European Union (hereinafter "**TFEU**"), as well as the Charter, enabled the same EU to provide for effective legislative instruments (*e.g*. among the other, GDPR) to protect personal data.

However, before to go deep into the analysis of GDPR in terms of source of "requirements" it is necessary to preliminary explains the concepts of privacy and data protection.

In particular, even if there is not an over comprehensive and generally accepted definition of "privacy", the right to privacy (i.e. the right to a "private life") was recognised at international level already in 1966, within the International Covenants of Civil and Political Rights, in article 17[2], as well as within the Convention for the protection of individuals with regards to the processing of personal data (hereinafter, "**Convention 108**"), and in article 8 of the European Convention of Human Rights (hereinafter, "**ECHR**"). At EU level the right to privacy has been elevated to fundamental right with the Charter as well as in article 16 of the TFEU. Moreover, in the same Charter besides the right to privacy as described in article 7 article 8 expressively recognised the right of data protection.

The importance of privacy and data protection as fundamental rights can be understood if these two rights are considered as "*prerequisite to exercise other fundamental freedoms, such as freedom of expression, freedom of peaceful assembly and association, and freedom of religion*"[3]. Which are also protected and recognized as fundamental rights in articles 11 and 12 of the Charter. Moreover, in more general terms, it is also possible to say that the respect of data protection and privacy rights entail also the respect of the principle of non-discrimination (recognized as fundamental right in article 21 of the Charter).

This last consideration is particularly true when considering which are the interests, the values, protected by the right to privacy and data protection rights (which for the sake of clarity are not the exactly the same). Indeed, it is possible to say that the scopes of these two rights are different. Privacy (even if there

[2] https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

[3] pag. 19 of the Council of Europe , European Court of Human Rights , European Data Protection Supervisor , European Union Agency for Fundamental Rights (EU body or agency) "Handbook on European Data Protection Law", 2018 Edition, https://op.europa.eu/en/publication-detail/-/publication/5b0cfa83-63f3-11e8-ab9c-01aa75ed71a1/language-en.

is not a unanimous definition generally accepted) can be considered as providing for a general prohibition of interference in the private life of an individual (with of course, certain limitations). On the other hand, the protection of personal data, can be instead intended as a complete system of rights, to be balanced and to be exercised and activated only when personal data, i.e. information that can identify (directly or indirectly) a person, are processed. This means also that data protection rules and requirements shall be complied with even when the processing operation having as object personal data do not interfere with the privacy of the individual.

Having in mind this introduction, and the scope and the objectives of the Project, it is now necessary to focus the attention on the legislative requirements in terms of data protection adopted at EU level. As it is notorious, the first legislative instruments that was issued by the EU to regulate this subject matter was Directive 95/46/EC. However, in consideration to the technological development as well as having regard to the legislative instruments used (a directive, which leave a certain margin of discretion to Member States in implementing it) in 2018 was issued the EU General Data Protection Regulation no. 2016/679 (hereinafter "**GDPR**").

As of today, GDPR is the most relevant EU legislative source in terms of providing those rules and principles that should be respected when, upon the occurrence of certain conditions, personal data are processed.

For the purpose of the present document, taking in consideration that within chapter 7 of D1.1 – Identification of existing threats and data privacy requirements it was already provided an analysis concerning the inter-relation between data protection regulation and smart grid specifications and peculiarities, here it is worth to recall that the compliance with GDPR in practical terms entails not only the respect of the principles set forth in of that piece of legislation, but also the capacity of an individual (a data subject) to exercise his/her rights.

In addition, when it comes to data protection in smart grid, a special attention should be paid also to the interrelation between GDPR and the so-called Electricity Directive[4], which is part of the "Clean Energy for All Europeans" package[5] and specifically regulates smart meters' deployment.

[4] Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L0944

[5] https://ec.europa.eu/energy/topics/energy-strategy/clean-energy-all-europeans_en

Figure 2: Clean Energy for All Europeans package

In particular, the Electricity Directive provides for a general obligation for the Member States to regulate smart metering (and consequently smart grid) without incurring in discrimination of consumers (which is as well as ensuring the protection of their personal data). For the sake of clarity, it should be noted that even if the Electricity Directive is a directive (i.e. one of the EU legislative acts listed in article 288 TFEU), and therefore it is not directly applicable in the Member States, but rather it has to be timely transposed into national legislation, it can in any case provides some guidance in identifying privacy and data protection requirements specifically targeted in smart metering and smart grid.

In this respect, it is interesting to see how article 20, paragraph 1, letter f) of the Electricity Directive essentially represents a transposition of the general duty of transparency provided in articles 5, 12, and 14 of GDPR as well as article 20, paragraph 1, letter e) recognized also the importance of implementing mechanism in data exchange enabling for the consumer/data subject to exercise his/her rights of access as provided in article 15 of GDPR. As last remark, in a very general term, and therefore with a very broad meaning, article 23, paragraph 3 of the Electricity Directive concerning "Data management" provides that "*The processing of personal data within the framework of this Directive shall be carried out in accordance with Regulation (EU) 2016/679*".

2.2. Privacy Methodology

As explained within the Executive Summary, to define privacy and data protection requirements, at the beginning of the Project it has been evaluated whether or not the Project and the results of the same would have had as object personal data and if they would have had the possibility to impact on individuals' privacy. In consideration of the positive answer to this question, some steps have been taken in order to protect the personal data of the individuals that might be affected.

In particular, a series of deliverables have been submitted to provide those guidelines and rules concerning the data protection during the Project. On the other hand, as per the data protection requirements that the PHOENIX architecture shall comply with, i.e. the results of the Project, in deliverable D1.1 after having explained the main privacy and data protection principles, in sections 7.7.1 (*PHOENIX Personal Data processing – practical recommendations*) a first set of high level requirements was provided.

At the time of the submission of the above-mentioned deliverable (i.e. month 6 of the Project), those recommendations have represented a general guidance for the definition of the PHOENIX architecture. However, the same were already customised considering the general principles of data protection provided in article 5 of GDPR and the specific sector and its related activities pertaining to smart grid and smart metering.

For the purpose of the present document, it is worth to recall the following Table 3 reporting the privacy and data protection requirements ("**PRx**").

Table 3: Privacy and Data Protection requirements

#ID	Requirements	Description
PR1	Transparency	The **purposes of the data processing** should appear clear and intelligible for the data subject. This can be ensured providing all the appropriate and necessary information to data subjects to exercise their rights, to data controllers to evaluate their processors, and to Data Protection Authorities to monitor according to responsibilities. The technology solutions, and their relative **data models**, thus should ensure that a data subject might get easily access, at any time also after the start of the data processing operations, to that information. For the sake of clarity, it should be noted that all that information should be made available to the data subjects in a clear and intelligible way.
PR2	Lawful data collection	The data processing shall originate from those personal data that have been collected with a lawful ground. Particular attention should be paid when implementing those components that will help to collect and get the **data subject's consent**. In this respect, the relevant Partner should ensure the possibility to map the data flow. Particular attention should be given in case of secondary processing (even if, at the time of submission, this kind of operations are not foreseen).
PR3	Personal data collected are (i) adequate, (ii) proportionate and (iii) relevant to the objectives of the system	The implementation of the principle of **purpose limitation and data minimisation** , representing two of the core principles set forth in GDPR, requires that the amount of data collected shall be proportionate to the purposes to be achieved, and at the same time, the purpose itself shall be legitimate. In this respect, data should be gathered if and only if it is strictly necessary for achieving the specified purpose and that data is "**need to know**".
PR4	The personal data collected are accurate	Besides the amount and the relevancy of the data collected, the technology solutions should ensure that the data to be processed are **accurate**, i.e. data are correct and up-to-date in all details.
PR5	Storage limitation	The development team of the technology solutions should define and implement an infrastructure pursuant to which it is possible to foresee for how long the personal data will be stored (ideally **the shorter the better**), and that in any case shall be compliant with the applicable legislation. Data subjects must be informed about it. Moreover, provided that those data are no longer necessary to fulfil the said scope, and any other restrictions can be found applicable, such data should be immediately erased and/or anonymised pursuant to the best standards and practices.
PR6	Procedures for granting individual rights	The components of the technology solutions should be designed taking also into consideration how, in concrete, the relevant data subject might exercise his/her rights in connection with the data processing. In this respect, the relevant Partner should be aware of all the rights that GDPR grants to data subjects, and for each of them tailor **a specific solution** (e.g. data subjects have the right to rectify their data and to request their erasure).
PR7	Accountability principle and	The implementation of the accountability principle entails that the technology solutions should allow a clear **identification of the responsibilities** related to the data processing. In particular, examples of accountability measures are related to

	technical implementation	**tracking** of personal data access and of communications with external systems. In addition, the abovementioned principle implies the set-up of internal audits and handle complaints procedures. Additionally, it should be noticed that at a national level, accountability is supported by independent DPA for monitoring and checking as supervisory bodies. However, the PHOENIX Project has established an Ethics Advisory Board and a Security Board in order to check that personal/sensitive data management is appropriately performed, according to the procedures outlined in D1.1 and D9.1.
PR8	Implementation of security measures	Information security addresses integrity, confidentiality and availability concerns. As mentioned in paragraph 7.6 (*Privacy Enhancing Technologies - PETs*) of D1.1. IT measures such as PETs represent an important tool (among others) to protect privacy and data protection, in terms of implementing technology solutions able to restrict access to personal data only to authorized people (e.g. **permissions**), and to ensure that the data is trustworthy and accurate (e.g. based on **provenance information**). The relevant Partner should also: (i) regularly conduct privacy risk assessment and audit processes; (ii) regularly run reviews of the security measures implemented; and (iii) design an ad hoc procedure to be followed in case of data breach. Moreover, when it comes to security, besides the principles of confidentiality, integrity and availability, the relevant PHOENIX Partners should also take into consideration the concepts provided within the ENISA's *Report on Privacy and Data Protection by Design – from policy to engineering*[6] issued in December 2014.

2.3. Privacy and Data Protection potential concerns

In general terms, it is possible to say that the main privacy concern regards a general dis-respect of the principles expressed above. That also considering that smart grid are complex technology solutions that have been developed to increase the efficiency and the effectiveness of the electric supply chain. Moreover, considering the scope pursued by the implementation of smart grid it is possible to say that:

"Smart grids improve electricity generation and distribution through optimization and projection of electricity consumption by leveraging communication networks to exchange information between those different parties"[7].

In particular, smart grid can be seen as a complex of five domains (according to the Smart Grid Architecture Model - SGAM): generation, transmission, distribution, distributed energy resources and customer premises (consumption). Each domain, poses questions in terms of privacy and data protection (as well as ethics, security and other social concerns). Indeed, to properly functioning, each domain requires a considerable amount of data, entailing the exchange of such data among Transmission System

[6] https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

[7] Ismail Butun, Alexios Lekidis and Daniel Ricardo dos Santos "Security and Privacy in Smart Grids: Challenges, Current Solutions and Future Opportunities" February 2020, Conference: 6th International Conference on Information Systems Security and Privacy.

Operators (hereinafter "**TSO**") and Distributor System Operators (hereinafter "**DSO**"), as well as with prosumers and consumers.

In terms of "privacy concerns", among the other, the following might be identified as the main (general) ones:

- the possibility of inferring relevant information (e.g. particular habits) from personal data, due to the collection and processing of great amount of data and personal data;
- metering data will be accessible by several independent actors (e.g. DSO, service provider, the consumer)[8] performing roles as data controllers, data processors, third parties, recipients etc.;
- effective exercise of consumer/data subject's rights.

In light of these, and having in mind the potential data flow within the PHOENIX architecture and its components, and having considered paragraphs 2.2 (*Privacy methodology*), the Project is defining a detailed list of potential concerns or threats (uniquely identified with xTHRy). Each xTHRy represents a risk, and this document specifies in Section 5 the compliance rules and governance policies identified to avoid or in the worst case just to mitigate these risks. As per the privacy and data protection concerns or threats the following table shows the ones so far identified:

Table 4: Potential Concerns or Threats impacting Privacy and Data Protection Requirements

# ID	Requirement	Potential Concerns or Threats
PR1	Transparency	• PTHR1 - Data Subject is not informed of (i) which data are collected; (ii) which is the source of the collection; (iii) who are the actors involved in the collection and subsequent processing; and (iv) the purposes of the data processing; • PTHR2 - Data processing is done for different purposes from the ones agreed with the data subject;
PR2	Lawful data collection	• PTHR3 - Data Subject is not aware of data collected and shared • PTHR4 – The collection of data is made on a wrong legal basis or in absence of a legal basis;
PR3	Personal data collected are (i) adequate, (ii) proportionate and (iii) relevant to the objectives of the system	• PTHR5 - It is quite frequent the collection of unneeded (personal) data, i.e. data not relevant to the objectives of the system and for the agreed purposes of data processing.
PR4	The personal data collected are accurate	• PTHR6 – Lack of information among involved parties is the primary potential cause for inaccurate data in a system.

[8] Enisa, "Smart Grid Security – Recommendations for Europe and Member States" Deliverable 2012- 07-01

PR5	Storage limitation	• PTHR7 - Data persistency has to be guaranteed for the minimum required timeframe, according to contracts among parties and the applicable regulatory framework.
PR6	Procedures for granting individual rights	• PTHR8 – Lack of information of the data subject rights at design phase impacts on enabling/disabling the exercise of individual rights themselves.
PR7	Accountability principle and technical implementation	• PTHR9 – Accountability of the system is impacted by the lack of provenance information regarding activities of the components (i.e. logs), access to the system, integrity of data collected, integrity of data exchanged.
PR8	Implementation of security measures	• PTHR10 – There are not proportionate and security measures, because the system design has not considered the different data protection/privacy violation scenarios (i.e. threats identified in D1.1, including - inter alia - data breach), but rather just a general one and has not considered the presence of different categories of data which require different level of security.

3. Ethics and Social Requirements

3.1. Ethics and Social Framework

In general terms, it is possible to say that the PHOENIX Project pays a particular attention to either the ethics and the social aspects that the research activities might arise and impact during the whole Project lifecycle, as well as its results might have on the civil society.

It is therefore in this light that should be read the introduction of a specific WP providing for the definition of the procedures that each Partner committed to respect in terms of ethics, namely WP10 – Ethics Requirements, already submitted at month 5 of the Project (i.e. 31st January 2020).

In particular, for the purposes of the present chapter and adopting a definition of "ethics requirements" as those that are providing the essential rules and policies to involve external individual (i.e. external to the Consortium) in the research, a special attention shall be paid to the 3 deliverables listed in Table 5.

Table 5: Ethics Requirements

Requirement	Description
D10.1: H – Requirement No.1	Definition of the **procedures and criteria to recruit** research participants. Within the present deliverable has been provided the essential principles that the Project committed to respect when it will recruit participants for pilots, training and/or dissemination activities. Principles of non-discrimination, respect of individuals, voluntary participations and responsibility are the main guiding policies that will be applied and whose respect will also entail the respect of good research practices.
D10.2: H – Requirement No.2	Definition of the **informed consent procedure** for the participation of individuals in the research. The deliverable provides for the template to be used and to be provided to individuals external to the Consortium for their involvement of the research. Without prejudice to the content of the template provided, the essential part of the document is represented by the necessity to provide clear and intelligible information to the individual, in order to allow the same to make a conscious as well free decision.
D10.3: H – Requirement No.3	**Copies of opinions/approvals** by the Ethics Advisory Board for the research with humans. Considering the potential involvement of individuals during the research activities, and considering that their involvement might represent a potential prejudice for their rights and freedoms, if individuals will be concretely involved, it will be required an opinion/approval from the Ethics Advisory Board. In particular cases, provided that specific ethics issues arise, the Ethics Advisory Board instead of issuing the opinion/approval will request the relevant Partner to address the same issue to national/local ethics boards.

On the other hand, in terms of social requirements, or in terms of social acceptability, it should be considered the following.

While PHOENIX project aims to increase the security of EPES and critical energy Infrastructure, at the same time it (i) aims at guaranteeing the continuity of operations, in case of cyber incidents or attacks, and (ii) minimising cascading effects in the infrastructure itself, the environment, the citizens in vicinity and the energy end-users. This is beneficial for the society as a whole as it will continuously have access to energy (reduced down time of energy network) and disasters/terrorism incidents and crimes relevant to energy network operations are eliminated.

Security and continuity of operations in the energy sectors are widely perceived as primary needs from the citizens because their life and habits may be drastically affected in case of attacks. Energy infrastructure is usually perceived and trusted as a reliable system able to ensure 24hx7days operation, and for its relevance, it is designed and maintained to be a sheltered system.

Citizens daily life is based on a by-now obvious principle: we can always take advantage of electricity, water, means of transport, telecommunication, ATMs, commodities.

Figure 3: 28 September 2003 - Blackout in Rome

Yet on the night of September 28, 2003, a fallen tree in Switzerland triggered an incredible domino effect, leaving Italy (57 million people) and part of Switzerland “blocked and isolated”. On that night, citizens became aware of the limits in which they find themselves in the absence of electricity (see Figure 3[9]).

Other relevant and long electric outages have been occurred in the recent years in European countries impacting millions of citizens.

This remark how the underlying infrastructure is usually hidden and the citizens are not aware of its vulnerability, until it fails and doesn’t work.

In Europe, cities account for 75% of the population, consuming 80% of the EU’s resources, including energy. The United Nations[10] anticipates that the world’s population will reach 8.5 billion by 2030, with the number of people living within cities rising to 5 billion.

[9] http://www.lefotochehannosegnatounepoca.it/2017/05/05/28-settembre-del-2003-si-verificava-italia-piu-grande-black-out-del-sistema-elettrico-della-sua-storia

[10] United Nations, “World Population Prospect 2019: Highlights” (2019) - https://population.un.org/wpp/Publications/Files/WPP2019_Highlights.pdf

In such a scenario, continuous energy availability needs to be ensured by enhanced procedures and technologies, including disruptive technologies (such as - inter alia - AI, blockchain and 5G that are adopted by PHOENIX) that promise to (i) overcome the intrinsic limits of current “critical and vital” infrastructures, designed decades ago for different life scenarios, expectations in terms of Quality of Service and a smaller number of urban dwellers; (ii) enable capacities for efficiently enacting activities never considered in the past; and (iii) fostering innovation and sustainability for the next decades.

The abovementioned promises are part of the United Nations Sustainable Development Goals as well, and specifically SDG7, SDG9, SDG11 and SDG12 (see Figure 4).

ENVISION
disability
2030
SUSTAINABLE DEVELOPMENT GOALS
17 GOALS TO TRANSFORM OUR WORLD
7 AFFORDABLE AND CLEAN ENERGY
9 INNOVATION AND INFRASTRUCTURE
11 SUSTAINABLE CITIES AND COMMUNITIES
12 RESPONSIBLE CONSUMPTION

Figure 4: UN Sustainable Development Goals considered in PHOENIX

3.2. Ethics and Social Methodology

Although the abovementioned ethics requirements deliverables described in Table 5 are providing the basic rules concerning the involvement of individuals during the life of the Project, it should be noted that certain ground rules can be derived from them and applied to the results of the Project itself in terms of ethics requirements.

Moreover, the PHOENIX Project is adopting a methodology based on assessing social concerns (and specifically social acceptance) with respect to the delivered technology solutions. The methodology is based on the “Close-the-Loop” model[11] that brings together the different dimensions of the classical theories of social acceptance (i.e. socio-political acceptance, community acceptance, and market acceptance) and for this reason it is able to:

- “close-the-loop” between the main critical concerns for citizens, justice and policy-makers, and consequently

[11] https://ercim-news.ercim.eu/en121/special/close-the-loop-model-social-acceptance-of-technology-for-sustainability

- better track societal feedback. This allows to define and evaluate ethics-driven approaches (based on a better understanding of the technology and willingness to use it) aiming at reducing the barriers of diffidence and mystification against the technology solutions, and fostering its wider and faster deployment.

The "Close-the-Loop" model (see Figure 5) includes six fundamental dimensions over which social acceptability (i.e. perception, motivation, trust, awareness, capacity enabling and accountability) is measured and assessed. The method of evaluating technological acceptability is innovative due to its stepwise nature, which is as follows:

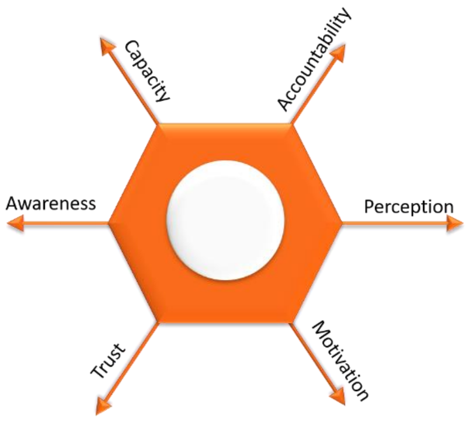

Figure 5: "Close-the-Loop" Model

1. **perception** works on a subject's conscious and subconscious mental patterns;
2. **motivation** illustrates the moral basis according to which subjects align their preferences;
3. **trust** represents the level of reciprocity of individual and social expectations;
4. **awareness** shows the ability for individuals to choose and judge using universal values;
5. **capacity** for action pinpoints to what extent a technology enables people to all of the above;
6. **accountability** refers to the degree to which a society and its institutions are able to introduce policies that favour such complex models of acceptance.

The analysis of this model is out of the scope of this document, and Social Acceptance model will be further investigated in the Task 7.7 "Validation of results, certification & replication guidelines" of the Project. However, this short premise is useful to clarify the rationale behind the following social requirements, and for their relative compliance rules and governance policies defined in Chapter 5 (*Compliance Rules and Governing Pol*ices).

For their interlinked nature, ethics and social requirements are mixed together (i.e. ESRx requirements), and are illustrated in the following Table 6.

Table 6: Ethics and Social requirements

ID#	Requirement	Description
ESR1	Respect for the individual life	The results of the PHOENIX Project shall not lead in any case to discriminatory or unjustified arbitrary behaviours addressed to the individuals/consumers. In addition, the same PHOENIX results cannot lead in any case to the creation of unnecessary or un-proportionate risks for the physical life of the consumers/individuals.
ESR2	Informational Transparency	Individuals/consumers should be informed (i.e. aware) about the existence of PHOENIX infrastructure and provided with a level of details (e.g. rationales and purposes) adequate to ensure the transparency of the solution but at the same time without violating any confidential or security obligation.

		Transparency impacts on trust, that is a key dimension for the social acceptance.

3.3. Ethics and Social potential concerns

Based on the abovementioned requirements, the following Table 7 identifies the list of potential concerns or threats impacting ethics and social requirements. As per the privacy and data protection concerns/threats identified in the previous 2.3 (*Data Protection and Privacy concerns*), in Chapter 5 specific compliance rules and governing policies will be illustrated in order to avoid the occurrence of the identified concerns (or at least to mitigate them in the worst case scenario).

Table 7: Potential concerns or threats impacting Ethics and Social requirements

# ID	Requirement	Potential Concerns or Threats
ESR1	Respect for the individual life	• ESTHR1 – Abuse of data collection, i.e. data collected is not strictly necessary for the specific purpose of the project objectives, might allow to derive information that could potentially threat individual life based on personal behaviours and habits.
ESR2	Informational Transparency	• ESTHR2 – lack of information, or lack of transparency, or use of technical jargons - in communicating the relevant information might lead to a general non-acceptance of the technology solutions developed by PHOENIX.

4. Security Requirements

The analysis of the legislative requirements imposed at EU level in terms of (cyber) security aspects is particularly relevant in consideration to fact that the Project deals with critical infrastructure, that can be defined as "*an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions*"[12].

As already recognised in 2012 by ENISA, the impacts of cyber-attacks and threats on smart grid and smart metering infrastructures might affect society's way of life.

In terms of security the objectives of the PHOENIX Project are really ambitious. It is for this reason that in the next paragraphs it will be analysed the cyber-security legal framework from which it is possible to infer those security requirements that the Project intends to implement through its components within the PHOENIX architecture.

4.1. Security legal framework

4.1.1. The Directive on Security of Network and Information System

At EU level in 2013 was launched the "Cybersecurity Strategy of the European Union – an Open, Safe and Secure Cyberspace"[13] (hereinafter, the "**Strategy**"). Among the five objectives identified by the Strategy there was also the so called "cyber-resilience", to support the internal market[14] and also to boost the security of the EU.

Already within the Strategy the EU was promoting the adoption of a more uniform legislative approach to tackle cybersecurity threats, in particular with reference to those having cross borders dimension.

It is in this light that should be read and welcomed the adoption of the Directive on Security of Network Information System EU 2016/1148 (hereinafter the "**NIS Directive**"), which is the first horizontal piece of legislation aimed at protecting the security of network and information system.

In particular, the NIS Directive has 3 main objectives:

1. improving national cybersecurity capabilities;
2. building and fostering cooperation (on cybersecurity) at EU level; and
3. promoting a culture of risk management and incidents reporting among key economic actors, operators providing essential services for the maintaining of economic and societal activities, and digital service providers.

[12] Article 2, letter a) of the COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN.

[13] http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

[14] Article 1 of the NIS Directive

With reference to the PHOENIX Project, even if the NIS Directive sets forth obligations directly on Member States, the same had in any case a duty to transpose into national legislation the said directive, providing for specific obligations on operators of essential services[15]. Having in mind the ultimate goals of the Project, and the actors involved in the production and transmission of the electric energy, it appears clear that the same can be considered as operator of essential services and, therefore, that shall be considered as the addressee of the obligations set forth with the NIS Directive. In fact, reading in conjunction article 4(4) and article 5(2) of the NIS Directive an organization can be defined an "operator of essential services" (hereinafter "**OEP**") provided that:

- it is a public or private entity of the type referred in Annex II of the NIS Directive, which includes energy (including electricity), transport, banking, financial market infrastructures, health sector, drinking water supply and distribution, digital infrastructure. In this respect, it is worth noticing that being the NIS Directive a directive pursuant to article 288 of the TFEU, during it transposition into national legislation, it might be subject to certain changes. With reference to the identification of the operators of essential services, even if the said legislation provided the main criteria, however by 2018 Member States had to identify the operators of essential services with an establishment on their territory.
- the said entity provides a service which is essential for the maintenance of critical societal and/or economic activities;
- the provision of that service depends on network and information systems; and
- an incident would have significant disruptive effects on the provision of that service.

Similarly as the EU legislator did in other piece of regulation, in terms of identification of the obligations that the NIS Directive created, these can be distinguished in two macro - categories: security requirements and information/notification obligations.

Before analysing the abovementioned two set of obligations, it is important to remark that the NIS Directive and GDPR cannot be seen as alternative, as they do not have the same subject matter. This means that, in terms of compliance, the Project shall have to bear in mind these two pieces of legislations, as well as proposing and implementing IT requirements and components able to satisfy both.

Security obligations under NIS

In terms of ensuring the security of the network and of the information system as defined in article 4 (2), the NIS Directive provides that Member States shall ensure that OEPs shall adopt:

- appropriate and proportionate technical and organisational measures with regard to the security of the network and information systems they use in the provision of their services;
- these measures shall aim to: (i) manage the risks posed to those systems and (ii) prevent and minimise the impact of incidents affecting those systems, with a view to ensuring the continuity of their services; and

[15] For the sake of completeness, the NIS Directive provides also for obligations to be complied with by service operators (cloud computing services, online marketplaces and search engines), for which a dedicate implementing regulation providing for more details have been issued in 2018

- shall have regard to the state of the art and ensure a level of security appropriate to the risk posed.[16]

In this respect, it should be noted that since there is not further explanation on the concepts of proportionality and appropriateness in relation to such measures, a large discretion has been left to Member States.

Nevertheless, the principle of the risk approach shall be always bore in mind when identifying and implementing such measures, and should be considered a sort of guiding light when implementing security measures. In this respect, in order to give more content to the "risk approach" suggested, a useful reading is represented by the ENISA document "Appropriate security measures for Smart Grid"[17], whereby, inter alia, it is provided that the risk assessment shall be performed during the entire life cycle of the smart grid itself (and so also during the creation of the same), and in particular, the risk assessment *"is a key preliminary step that should be conducted in order to understand what risk level is appropriate/acceptable for each organisation before deciding upon the required sophistication levels needed by the smart grid organization"*[18]

Moreover, in order to foster the homogeneity of these security measures, the NIS Cooperation Group in 2018, published some guidelines[19] whereby the following principles where identified and explained in order to give some guidance: *"these measures should be effective, tailored, compatible, proportionate, concrete, verifiable and inclusive*".

In addition, in the same document, the NIS Cooperation Group identifies the following 3 macro – areas (each of them sub-categorized) in which specific security policies should be implemented (see Table 8).

Table 8: NIS Cooperation Group macro-area

Macro - area	Sub - category
Governance and Ecosystem	Information System Security Governance & Risk Management
	Ecosystem management
Protection	IT Security Architecture
	IT Security Administration
	Identity and Access management
	IT Security maintenance
	Physical and environmental security
Defense	Detection

[16] Articles 14 (1) and (2) and 16 (1) and (2) of the NIS Directive.

[17] ENISA "*Appropriate security measures for smart grids Guidelines to assess the sophistication of security measures implementation [2012-12-06]"* available at https://www.enisa.europa.eu/publications/appropriate-security-measures-for-smart-grids.

[18] Ibidem pages 15-16.

[19] NIS Cooperation Group, February 2018, "Reference document on security measures for Operators of Essential Services", publication 01/2018**"**.

	Computer security incident management

Information obligations

In terms of compliance with this set of obligations, the same can be distinguished in obligations to (i) notify the national legislator/regulators concerning incidents that met a certain threshold, and (ii) voluntary[20] disclose information/incidents.[21]

For the purpose of the present deliverable, what it is relevant is "the incident notification obligation". In particular the NIS Directive defines an incident as "*any event having an actual adverse effect on the security of network and information systems*". In order to determine the significance of the impact of an incident, operators of essential services and digital service providers must take into account the following parameters:

[1] the number of users affected by the disruption of the essential service;
[2] the duration of the incident; and
[3] the geographical spread with regard to the area affected by the incident.

The timing of the notification will have to take place without unjustified delay.

As per the security measures, also in this case the NIS Cooperation Group published some useful guidelines in 2018, aimed at providing non-binding technical guidance "*to national competent authorities and CSIRTs with regard to formats and procedures for the notification of incidents by OES, to facilitate alignment in the implementation of the NIS Directive across the EU*".[22] Indeed also in this case the adoption of uniform guidelines could represent a vital asset to tackle cross-border incidents, improve collaboration and the aggregation of the data and their analysis, as well as improve the entire efficiency of the system.

In particular, in the said document, the NIS Cooperation Group, in terms of notification procedures, provides the following:

- alert notifications to be addressed to the competent national authority or to the competent Computer Security Incident Response Team (hereinafter "**CSIRT**") in order to:
  - *"Offer support to the affected organization, for example, the CSIRT could give technical support3.*
  - *Assess the potential impact for essential services, citizens, the society, the economy, etc.*

[20] Which, according to the NIS Cooperation Group Guidelines on notification of Operators of Essential Services incidents – Formats and procedures" publication 05/2018, can allow authorities to get a better situational awareness as well as to identify potential new threats and consequently informs also other OES.

[21] Michels, Johan David and Walden, Ian, How Safe is Safe Enough? Improving Cybersecurity in Europe's Critical Infrastructure Under the NIS Directive (December 7, 2018). Queen Mary School of Law Legal Studies Research Paper No. 291/2018. Available at SSRN: https://ssrn.com/abstract=3297470

[22] NIS Cooperation Group "Guidelines on notification of Operators of Essential Services incidents – Formats and procedures" publication 05/2018.

 - ○ *Inform, in exceptional circumstances, and when this is in the public interest, other organizations, so they can take action.*
 - ○ *Prevent spreading or reduce the impact by warning and sharing information with relevant organizations, for example with other OESs, CSIRTs, etc.*
 - ○ *Inform authorities abroad when there is significant impact across the EU*"[23].
- Follow up notifications to update on the status of the alert notification.

In addition, the documents then highlight how much is important the timing of the notification itself, proposing also different methods to transmit the same, as well as indicating that the same notifications shall be also protected.

4.1.2. Cybersecurity Act

The Cybersecurity Act[24] has been adopted in April 2019 and, among its objectives, it introduced the first EU certification scheme for ICT digital products, services and processes. In this respect, it should be noted that the certification scheme is based on a risk-based approach.

Moreover, it is worth noticing that for the implementation of the certification framework, it has been established an European Cybersecurity Certification Group.

In this respect it should be recalled that among the objectives of PHOENIX Project there is also "*the establishment of certification methodologies and procedures through a Netherlands-based Cybersecurity Certification Centre*".

PHOENIX Cybersecurity Certification Centre will be found by DNV and a comprehensive focus on cybersecurity and interoperability certification (incl. types of elements, specifications of test cases, and parametrization guidelines) will be developed. Cybersecurity conformance certification will be earned by cybersecurity systems, platforms and smart metering products and systems suppliers that demonstrate adherence to industry consensus cyber security specifications for security characteristics and supplier development best practices, by leveraging on knowhow and effort of DNV, ISKRA and PPC partners. This will contribute, to the to EPES standardization.

This objective in particular represents the subject matter of deliverable D8.8 due at month 36.

4.2. Security Methodology

After having analysed the abovementioned legal framework and considering also the structure of the a smart grid (which as indicated in section 2.3 (*Privacy and Data Protection potential concerns*) is composed by 3 different components), it might be possible to identify the following security requirements[25] to be considered and illustrated in the following Table 9. In particular the same have

[23] Ibidem, page 11.

[24] REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

[25] "Cyber Security in Smart Grid: Survey and Challenges" Z. Elmrabet , H. Elghazi , N. Kaabouch , available on line https://arxiv.org/pdf/1809.02609.pdf

been also identified by the National Institute of Standards and Technology[26] (an US based governmental organization, which in any case can provide guidance in this matter).

Table 9: Security requirements

#ID	Requirement	Description
SR1	Implementation of security measures (in general)	The IT infrastructure shall implement adequate and appropriate security measures able to protect the data to be ingested in the infrastructure as well as its functionalities. In this respect, such measures shall include either physical measures as well as technological ones, and in any case shall be designed applying a risk based approach, which shall consider all the components and their interactions.
SR2	Notification system	This requirement entails that the infrastructure is able to (i) detect and to send a prompt warning notification/message in case of actual attacks or even potential to the most appropriate authority; (ii) send a notification message complete with all the necessary information to detect the threats and determine the countermeasures; and (iii) the same notification system shall also be designed and construed applying adequate and proportionate security measures.
SR3	Confidentiality	The requirement of confidentiality aims at protecting both personal and non-personal information from un-authorized access and/or use.
SR4	Availability	Means that the information circulating within the smart grid are timely and reliably accessible in case of need.
SR5	Integrity	Means that the information stored or in any case circulating within the IT infrastructure cannot be modified (nor be tampered or loss), and therefore are reliable and trustable. A good practice might be the implementation of a blockchain solution.
SR6	Accountability	Entails that the information (i.e. data) and the operations made on certain data can be tracked and traced back to specific and pre-authorise individuals. Ensuring the respect of the accountability therefore entails the respect of the principle of authenticity.

[26] https://www.nist.gov/

4.3. Security potential concerns

Having in mind the abovementioned table, it is also possible to identify a series of potential threats or potential concerns in Table 10.

Table 10: Potential concerns or threats impacting security requirements

#ID	Requirement	Threats or potential concern
SR1	Implementation of security measures (in general)	• STHR1 - appropriate security measures either at organizational and at technical level have not been developed/have been wrongly implemented. In particular, there might be the risk to cover all the identified potential threats (i.e. defined in D1.1) but the implementations are not sufficiently flexible to cover also unforeseen events; • STHR2 - an alignment among the security measures *strictu sensu* and the security measures implemented to ensure the privacy and data protection rights has not been performed and such dis-homogeneity might create conflicts.
SR2	Notification system	• STHR3 - the system has not been designed to provide timely alerts and/or the addressee of the alerts have not been correctly identified, or the alert chain is per se not secured and possible intrusions or interferences might happens jeopardising the alert system itself and the messages contained.
SR3	Confidentiality	• STHR4 – an improper definition and management of authorisations to access and/or use data might entails: (i) several vulnerabilities and impact on the confidentiality of its managed information; (ii) the violation of several GDPR provisions.
SR4	Availability	• STHR5 – overload of security operations might potentially impact on timely access to important information, necessary for the proper operating conditions of the smart grid.
SR5	Integrity	• STHR6 – data, flowing from EdgeNetwork devices to PHOENIX architecture, undergo several transformations (e.g. format and protocol) that might impact on its authenticity and integrity.
SR6	Accountability	• STHR7 – if any specific data transformation is performed without ensuring the traceability of authorised permissions, or permissions are not assigned to trustable entities, accountability of the system is definitely compromised, as well as the authenticity of its managed information.

5. Compliance rules and Governance policies

The following table intends to provide a clear and practical guide to PHOENIX IT Partners when it comes to apply all the above mentioned considerations in developing the PHOENIX IT architecture and its relevant components, in particular considering that to develop and implement an appropriate IT solutions it is necessary to implement all the above mentioned requirements, in order to avoid - or at least mitigate - the impacts from potential concerns or threats.

However, it should be made on final remark: the following practical guidelines can be refined as soon as a technological improvement take place. As a consequence, the following should be considered as a "living document" that can be updated if needed.

The rules and policies defined in the following Table 11 are applicable to all PHOENIX components, due to the fact that each of them (depending on the concrete data flow) might play the role of data controller/processor for data made available from EdgeNetwork devices (e.g. PLC or RTU of substations and eV-chargers).

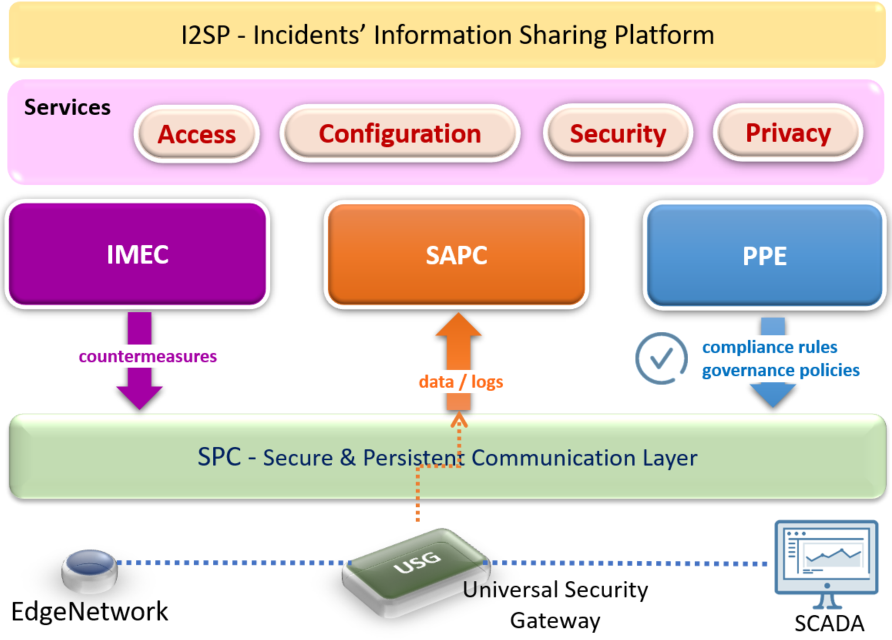

Figure 6: PHOENIX Overall Architecture

Indeed, the overall architecture of PHOENIX (shown in Figure 6 as a schematic representation without interactions details due to security restrictions) identifies the most relevant layers of the technology solutions. EdgeNetwork devices are the source entities of network traffic destined to SCADA servers for monitoring and control the smart grid. In the middle of this link, the USG (Universal Security Gateway) enables gateway functionality and on top of it is built the PHOENIX technology solution.

Table 11: PHOENIX Compliance rules and Governance policies

Impacted requirement	Potential concerns or threats	Rules and policies
Privacy and Data Protection		
PR1	- PTHR1, - PTHR2	- Data exchange may be carried out if and only if purposes of the data processing is clearly specified in the "contract" among data subject and data controller (i.e. source and destination) - The "contract" among data subject and data controller (and potentially also the contract between the data controller and data processor) must be defined according to the data model - Purposes of data processing may be revised at any time, considering changes in data models and purposes of data processing as well.
PR2	- PTHR3, - PTHR4	- Data Subject has to be always informed and has to provide consent to data collection and exchange. - Data Subject must always be able to access data to ensure lawfulness and evaluate potential update/rectification. - If data need to be "erasable", data have to be stored in non-DLT storage.
PR3	- PTHR5	- When defining the data model of the component, each single data property has to be strongly justified, by applying the "need-to-know" principle. - Data aggregation, anonymization and pseudonominisation techniques have to be adopted for the purpose of component testing and demonstration. - At the time of writing of this document, the most used ontologies are STIX2.0 and OCPP2.1. Other "proprietary" data models and ontologies are used in the PHOENIX Architecture. It is recommended to continuously monitor the adoption of additional ontologies, based on better data models defined by the components owners and LSP owners.
PR4	- PTHR6	- Data Subjects and Data Controllers have to be continuously informed about the status of the ongoing data sharing activities, as well as of their requests for changes (i.e. fundamental information for ensuring accuracy of exchanged information). - It is recommended that the appropriate interfaces (e.g. concerning Incidents' Information Sharing Platform) are defined and assessed with the continuous engagement of Data Subjects and Data Controllers.
PR5	- PTHR7	- According to the purposes of the project objectives, it is recommended that each single component of the PHOENIX architecture contributes to the definition of the minimum storage timeframe. This relevant parameter has to be based on data model of the component and of the relative pilot in which the component instance is running.
PR6	- PTHR8	- It is recommended to continuously monitor changes and updates in the data model of the components and the pilots, in order to identify

		potential personal/sensitive data and consequently plan how components enable/disable the exercise of individual rights (including rectification and/or erasure).
PR7	• PTHR9	• It is recommended to adequately trace the data exchange, and integrity of data exchange with appropriate tools and techniques (e.g. log, provenance information, hashing algorithms). • DLT technology, that is going to be considered for the SPC layer, represents a key solution for ensuring the traceability and data integrity.
PR8	• PTHR10	• It is recommended that security measures implemented to secure data protection/privacy violation scenarios are defined, implemented and tested both at architectural level (i.e. integration security measures) and for each component specification (i.e. unit security measures).
Ethics & Social		
ESR1	• ESTHR1	• It is always recommended the implementation of the principle of "data minimisation" and the continuous verification if data collected is strictly necessary (i.e. "need-to-know") for the specific purpose of the component and of the project objectives. • During the data model definition, it is a good practice to investigate the rationale behind the existence of specific data property. • During the test of the components, it is good practice to use "fake data", i.e. not using real data gathered from pilots and their participants.
ESR2	• ESTHR2	• It is recommended to provide any information to the target audience, in a comprehensible manner, and verifying that audience understands the expected objectives of the project and the use of collected data. • Use of technical jargons should be avoided when communicating with the target audience, especially if external to the Project consortium. It is recommended the implementation of rules defined in the D9.1 "Project Handbook" and dealing with the External Communication Board.
Security		
SR1	• STHR1, • STHR2	• It is recommended that the PHOENIX DevSecOps process considers for each component the definition of security test procedures, acceptance thresholds and reports in order to evaluate the addressing of all the defined threats, as well as to identify new potential and unforeseen threats. • It is recommended to release the PHOENIX components with relative test reports, in order to provide evidence of security level.
SR2	• STHR3	• It is recommended to promptly notify the parties (i.e. data subject and data controller) about the status of any event occurred in the system and that can directly or indirectly impact on them. • Notification system has to adopt appropriate measures in order to guarantee the authenticity and integrity of alerts themselves.

SR3	• STHR4	• It is recommended to define, implement and test appropriate management of authorisations to access and/or use data. • It is recommended to continuously update the level of reputation of the entities involved to gather, collect, access and process data. Based on the updated information, authorisation to access and/or use data have to be accordingly revised.
SR4	• STHR5	• It is recommended to identify the reasonable level of security with respect to the time constraints. Lightweight hashing algorithms and performing encryption mechanisms should be considered at the design phase of the communication protocols and mechanisms of the architecture.
SR5	• STHR6	• It is recommended to trace any operation on data (including the authorised permissions) in a secure and trustable register, in order to provide the evidences of integrity and authenticity of data managed by the system.
SR6	• STHR7	• It is recommended to adopt distributed ledger technology for ensuring the traceability of permissions, authorisations, reputations, events, and any vital information needed for providing evidence of system accountability, and data authenticity and integrity.

6. Conclusions

This document describes the work performed in Task 4.1 “**PRESS Framework Analysis”** during the first 10 months of the Project, specifically defining the framework for assessing the PHOENIX technology from 3 main perspectives, i.e. (I) **PR**ivacy and data PRotection; (II) **E**thics and **S**ocial; and (III) **S**ecurity.

The analysis carried out in this document shows 3 “pillars”, and for each of them, the document describes the relevant conceptual framework, the methodology for assessing the technology according to pre-defined requirements derived from the framework analysed, and then it identifies potential concerns able to impact the requirements identified.

The analysis has been carried out by starting from the outcomes inferred from ethics requirements (i.e. D10.x), the rules and processes defined in the Project Handbook (i.e. D9.1), as well as the preliminary version of the Data Management Plan (i.e. D7.1) and data privacy requirements (i.e. D1.1).

As per its outcomes, the PRESS Framework Analysis identifies 16 “PRESS” requirements alongside with the potential impacting concerns and threats, which should be considered during the DevSecOps process.

Indeed, as shown in the Figure 1, the PRESS Framework plays a relevant role for the PHOENIX DevSecOps process. In fact, besides the potential concern/threats it also identifies for each potential concern/threat a set of recommendations or countermeasures to be adopted and implemented during the whole Project lifecycle. These recommendations or countermeasures are reported in the chapter 5 as compliance rules and governance policies, which provides the Consortium with a practical “handbook” for properly applying ethics and legal (as well as social) principles during the research activity.

Moreover, in terms of interdependencies among deliverables and WP, it also is worth noticing that during the preparation of this document, a new relevant activity is running: the definition of the secure and persistent layer specification (i.e. D2.2). As a consequence, WP2 is strongly considering this PRESS Framework Analysis, and conversely the secure and persistent layer will be the first component to absorb and instantiate the compliance rules and governance policies provided hereto. To this extent, a chapter in D2.2 will create a link with PRESS Framework and will provide details on its implementation (and becoming consequently an example for the other components in PHOENIX).

This cooperation among Partners and the consideration of ethics and legal concerns into the DevSecOps entails that the “mind-set” created by the Legal & Regulatory compliance activity (i.e. Task 9.4) - mind-set that aims to prevent potential risks by applying a set of common methods and procedures for the Project research process - is deriving its benefits and it is not only considered as a task of “policemen and thieves”, but more properly as a “good research conduct”.

From this, the entire society can definitely benefit in terms of a sustainable innovation.

7. References

[1] I. Butun, A. Lekidis and D. Ricardo dos Santos, “Security and Privacy in Smart Grids: Challenges, Current Solutions and Future Opportunities,” *Conference Proceedings: 6th International Conference on Information Systems Security and Privacy,* February 2020.

[2] J. D. Michels and I. Walden, “How Safe is Safe Enough? Improving Cybersecurity in Europe's Critical Infrastructure Under the NIS Directive,” 7 December 2018. [Online]. Available: https://ssrn.com/abstract=3297470.

[3] Z. Elmrabet, H. Elghazi and N. Kaabouch, “Cyber Security in Smart Grid: Survey and Challenges,” April 2018. [Online]. Available: https://arxiv.org/pdf/1809.02609.pdf.

[4] European Parliament and of the Council;, “Directive (EU) 2019/944 on common rules for the internal market for electricity and amending Directive 2012/27/EU,” 5 June 2019. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L0944.

[5] Council of the European Union, “COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection,,” December 2008. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN.

[6] Proton Technologies AG, “EU General Data Protection Regulation no. 2016/679,” 2016. [Online]. Available: https://gdpr.eu/.

[7] UN, “UN International Covenant on Civil and Political Rights,” 1976. [Online]. Available: https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.

[8] ENISA, “Privacy and Data Protection by Design – from policy to engineering,” January 2015. [Online]. Available: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design.

[9] ENISA, “Smart Grid Security – Recommendations for Europe and Member States,” 2012. [Online]. Available: https://www.enisa.europa.eu/publications/ENISA-smart-grid-security-recommendations/at_download/fullReport.

[10] European Parliament and Council of the European Union, “Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act),” 17 April 2019. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN.

[11] NIS Cooperation Group, “Guidelines on notification of Operators of Essential Services incidents – Formats and procedures,” 2018. [Online]. Available: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53677.

[12] N. C. Group, “Reference document on security measures for Operators of Essential Services,” February 2018. [Online]. Available: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53643.

[13] D. Markopoulou and V. Papakonstantinou, “The new EU cybersecurity framework: The NIS Directive, ENISA’s role and the General Data Protection Regulatio,” *Computer Law & Security Review,* 31 July 2019.

[14] Council of Europe European Court of Human Rights, “Handbook on European Data Protection Law,” 2018. [Online]. Available: https://op.europa.eu/en/publication-detail/-/publication/5b0cfa83-63f3-11e8-ab9c-01aa75ed71a1/language-en.