Integrated Cybersecurity Solution
for the Vulnerability Assessment, Monitoring and Protection of
Critical Energy Infrastructures

INNOVATION ACTION
H2020 Grant Agreement Number: 832907

WP1 SYSTEM SPECIFICATIONS & ARCHITECTURE

D1.3 REGULATORY REQUIREMENTS SPECIFICATION

Document info	
Contractual delivery	30/12/2019
Actual delivery	30/12/2019
Responsible Beneficiary	TEC
Contributing beneficiaries	All
Version	1.0

This project has received funding from the European Union's H2020 research and innovation program under the Grant Agreement No. 832907

DOCUMENT INFO

Document ID:	D1.3
Version date:	30/12/2019
Total number of pages:	62
Abstract:	Task 1.3. identifies regulatory requirements related to the development, deployment and operation of the EnergyShield toolkit. In particular this deliverable examines the EC Directive on network and information security (NIS Directive) and the General Data Protection Regulation (GDPR). The NIS Directive requires critical infrastructure operators in sectors such as energy to adopt risk management practices and report major security incidents on their core services. Therefore, the task shall ensure that the EnergyShield solution will be consistently compliant with the relative legislative frameworks as provided on a European and International level, both vis-a-vis those legislative frameworks that concern network and information security but also taking into consideration legislative requirements that may affect the Electrical Power and Energy System (EPES) sector (e.g., GDPR). In Europe, both the NIS Directive and the GDPR have a profound impact on the EPES sector, especially as smart meters collect an increasing amount of customer personal data.
Keywords	Regulatory Requirements, GDPR, Encryption, Anonymization, Pseudonymization, Homomorphic Encryption, Data Security, Data Transfers, Risk Assessment, NIS, GDPR, EPES, critical infrastructure

AUTHORS

Name	Organization	Role
Marcelo Corrales C.	TEC	Overall Editor
Arasaratnam Arasilango	TEC	Contributor
Janos Meszaros	TEC	Contributor
Lavinia Dinca	SIVECO	Contributor
Otilia Bularca	SIVECO	Section editor

REVIEWERS

Name	Organization	Role
Yasen Todorov	CEZ	Overall Reviewer
Lambros Ekonomou	SC	QA Reviewer

VERSION HISTORY

0.1	31/07/2019	First structure of the document
0.2	15/09/2019	Analytical framework
0.3	30/09/2019	Collecting the information from partners
0.4	10/11/2019	Editing the main chapters
0.5	6/12/2019	First draft ready for internal review
0.6	18/12/2019	Draft including suggestion from reviewers
1.0	24/12/2019	Final version, released to the EC

EXECUTIVE SUMMARY

This report aims to ensure that the EnergyShield project is compliant with the new provisions enshrined in the EU General Data Protection Regulation [GDP16] and the Directive on Security of Network and Information Systems [NIS16]. In particular, the focus is to establish the main legal requirements with regard to data protection and data security, and to show how some of these requirements have been technically implemented.

Both the GDPR and the NIS Directive introduced new and stricter regulatory rules that impact upon any business or organization that handles personal and sensitive data. In this report we examine how the EnergyShield project can provide a more transparent tool that embeds effectively these legal requirements in the architecture design of the toolkit. The new compliance challenge is how to operationalize these legal requirements in all software components in a way that affords meaningful protection of the relevant interests.

This report also provides general guidance and recommendations regarding the exploitation of the toolkit by potential companies, which will use and benefit from the outcome of this project. An important aspect of the GDPR refers to the encryption of data. Therefore, anonymization and pseudonymization techniques are considered and we showcase how the Homomorphic Encryption (HE) tool will be developed and implemented in the toolkit.

The ubiquitous and dynamic nature of the cloud allows data transfers through a supple distributed network of infrastructure and service providers. Therefore – even though the partners of the EnergyShield project are currently not making any data transfers outside the EU/EEA countries – service and infrastructure providers deploying the toolkit at a later stage must ensure that data transfers are compliant with the GDPR and the consent of data subjects. We review the avenues for making such international personal data transfers legally compliant with the GDPR and provide recommendations for the further exploitation of the toolkit. This is aimed at assisting the end-users of the toolkit in complying with the GDPR's requirements on overseas data transfer.

This report also provides an overview of the data security standards that could serve to achieve an appropriate level of information security pursuant to the GDPR and NIS Directive provisions. The requirement to take 'appropriate technical and organizational measures has been standardized and unified among the EU Member States. However, the GDPR provides only the basic requirements, without going into technical details. Therefore, in this report we highlight the key measures that the developers and potential users of the toolkit should take into consideration. These measures are based on different standards, guidelines, frameworks and good practices currently available.

Last but not least, risk management is addressed and a list of both generic and specific security risks are listed alongside with calculation of their minimum and maximum cost exposure based on impact and probability of occurrence.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS

ACRONYM	DESCRIPTION
API	Application programming interface
B2B	Business to Business
BCR	Binding Corporate Rules
BYOD	Bring-your-own-Device
CCTV	Closed-Circuit Television
CD	Compact Disc
CIP	Criticial Infrastructure Protection
CJEU	Court of Justice of the European Union
CNIL	Commission nationale de l'informatique et des libertés
CSIRT	Computer Security Incident Response Team
DDoS	Distributed Denial of Service
DPIA	Data Protection Impact Assessment
DSP	Digital Service Providers
DVD	Digital Versatile Disc
EC	European Commission
EEA	European Economic Area
ENISA	European Network and Information Security Agency
EPES	Electrical Power and Energy System
EU	European Union
GDPR	General Data Protection Regulation
HE	Homomorphic Encryption
HDR	Hubbard Decision Reasearch
IEC	International Electrotechnical Commision
ICT	Information Communication Technology

IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
ISMS	Information Security Management System
ISO	International Standardization Organization
ITA	International Trade Administration
NEC	Noth Amercian Electric Reliability Corporation
NIS	Network and Information System
NIST	National Insitute of Standards and Technlogy
OES	Operators of Essential Services
PLC	Programmable Logic Controller
RSA	Rivest-Shamir-Adleman
SCADA	Supervisory control and data acquisition
SCC	Standard Contractual Clauses
US	Unites States
USB	Universal Serial Bus
VA	Vulnerability Assessment
VoIP	Voice over Internet Protocol
WI-FI	Wireless Fidelity

1. INTRODUCTION

1.1. SCOPE AND OBJECTIVES

EnergyShield project addresses socio-cyber-physical vulnerabilities of energy sector systems, mainly Electrical Power and Energy System (EPES).

In this report, the most salient points with regard to encryption, data transfers, data security and risk assessment are considered to ensure that the EnergyShield project is compliant with the new provisions enshrined in the General Data Protection Regulation (GDPR) [GDP16] and Network and Information Security (NIS) Directive [NIS16].

1.2. STRUCTURE OF THE REPORT

The cybersecurity regulatory framework with regard to data protection and data security are approached to show how some of these requirements have been technically implemented within and outside the European countries. The report is composed of four major sections dealing with data protection, data transfer, data security and risk management.

Data protection section investigates if EnergyShield tools are using personal data and identifies a set of security requirements.

Data transfer section checks for potential situations when data could be transferred within EU or EEA countries and drafts safe paths for partners that may fall in this situation while examining the main legal requirements.

Data security section provides recommendations on how data can be secured and addresses technical and organizational applicable measures. This section also delves into detail with regard to the Homomorphic Encryption tool that is currently being developed as one of the components of the EnergyShield project.

Risk management refers to standards, methods used to mitigate cybersecurity risks and draft a list of applicable risks that are assessed based on risk cost modelling developed by Hubbard Decision Research (HDR).

The last section concludes the report by highlighting the outcomes achieved.

Overall, this report investigates the applicable legal requirements and provides general guidance and recommendations regarding the exploitation of the toolkit by potential companies, which will use and benefit from the outcome of the EnergyShield project.

1.3. TASK DEPENDENCIES

The outcomes of this task will be used in WP2, 3 and 4 which are dealing with development and adapting of EnergyShield tools.

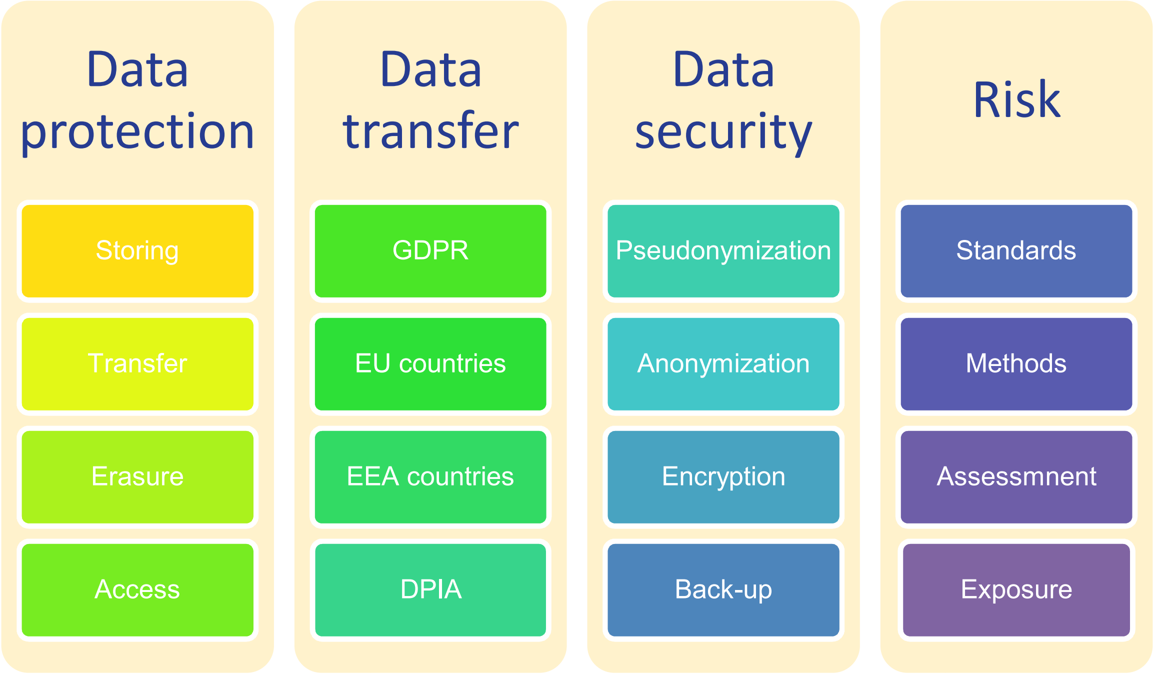
In parallel with this task T1.1 Technical requirements has assessed the security maturity level of EnergyShield practitioners and collected meaningful details about the security measures in place while feeding T1.3 with insights about the energy sector critical security aspects.

2. APPROACH ON REGULATORY REQUIREMENTS

This report relies on the legal assessment of the GDPR [GDP16] and examines the provisions enshrined in the NIS Directive [NIS16]. The GDPR was designed to strengthen data protection and privacy for all EU citizens and to empower them by granting more control and transparency over their data when using Internet services [MNF15] while the NIS Directive was designed to provide legal measures to raise the overall level of cybersecurity and protect network and information systems across the EU [NIS16].

To address EnergyShield project applicable legal requirements, a survey was designed and shared with the technological partners. Figure 1, below summarizes the focus of the survey:

- **Data protection** investigates if EnergyShield tools are using personal data;
- **Data transfer** checks for potential situations when data could be transferred within EU or EEA countries;
- **Data security** provides recommendations on how data can be secured;
- **Risks** refers to standards, methods used to mitigate cybersecurity risks.



Data protection	Data transfer	Data security	Risk
Storing	GDPR	Pseudonymization	Standards
Transfer	EU countries	Anonymization	Methods
Erasure	EEA countries	Encryption	Assessmnent
Access	DPIA	Back-up	Exposure

Figure 1. Regulatory requirements approach

The data collected revealed that only a few components of the toolkit will process personal data and at the moment there are no data transfers outside of the EU/EEA countries.

However, potential users of the toolkit should take into account the recommendations provided in this report in order to be compliant with the provisions of the NIS Directive and the GDPR.

3. DATA PROTECTION & DATA SECURITY REQUIREMENTS

The GDPR [GDP16] came into force on May 25th, 2018 and replaced the previous EU Data Protection Directive [DIV95]. It was designed to strengthen data protection and privacy for all EU citizens and to empower them by granting more control and transparency over their data when using Internet services [MNF15]. The GDPR has been generally well-received for updating some of the provisions of the previous data protection regime and has triggered regulatory action around the world. However, it has clearly created a higher standard of data protection and a new level of legal risks for businesses and organizations [KER19].

Falling foul of compliance with the GDPR, for instance, can result in hefty fines and data breaches must be reported within 72 hours. Data breach notifications are mandatory. While data controllers must report the breach immediately to their supervisory authority, data processors must notify the breach to the controllers [SAN19].

The GDPR expanded its territorial scope of protection in comparison to the previous data protection regime (extraterritorial applicability). This means that the GDPR applies not only to data controllers and data processors established within the EU, but also outside of the EU territory with regard to the processing of personal data of European citizens [GDP16]. The GDPR also strengthened the definition of consent which must be concise, unambiguous, clear and freely given. This means that companies have to be clearer about their terms and conditions. It will no longer be acceptable for companies to hide crucial privacy information somewhere in the middle of long user agreements full of legalese [GDP16].

An important new element of the GDPR is the concept of Privacy by Design and by Default. In the context of the EnergyShield project, this means that privacy and data protection requirements must be embedded directly into the software components and overall architectural design of the toolkit. Data controllers and processors using the toolkit must adopt this approach by default, making an explicit reference to ‘data minimization’ [GDP16], [SVA16] and also implementing different ‘anonymization’ and ‘pseudonymization’ techniques.

By and large, the GDPR also included a number of new legal provisions that the EnergyShield project must take into account such as access rights, the right to be forgotten and data portability. Access rights give data subjects control over their data. This right allows them to request the data controller more information regarding the way and purpose of their data processing [GDP16] (See Recital 43, Article 7 (4) of the GDPR and Wisman, 2017, 357.). The data subject can explicitly solicit information regarding the type of data stored and the source of the data (if not collected from the data subject directly). The data subject can inquire about what the data is being used for including information of automatic decision making and profiling. The latter might be important in the case of smart meters if the automatic decision making might directly affect the data subject

The right to be forgotten endows data subjects to have the controller erase their personal data and stop further processing of data from third parties [GDP16]. (See Article 5 (1) (c) of the GDPR).

Last but not least, data portability allows data subjects to receive their personal data (which they have previously submitted to the data controllers) in a structured, commonly used and machine-readable format, and to send the data to another controller [GDP16] (See Articles 12–14 of the GDPR).

3.1. ENCRYPTION: DE-IDENTIFICATION, ANONYMIZATION AND PSEUDONIMIZATION

The GDPR identified the privacy-enhancing effect of anonymization and pseudonymization methods by providing exceptions to many of the cumbersome provisions of the GDPR [GDP16]. Article 40 (2) (d) of the GDPR recommends controllers and processors of personal data to implement pseudonymization of personal data as a code of conduct or good practice [ORI18]. Both approaches are good ways for the EnergyShield project to reduce the probability of data breaches and therefore reduce the risk of paying hefty fines.

Anonymization and pseudonymization are highly recommended data processing methods by the GDPR because they mitigate risk and aid data processors in complying with their data protection obligations for secure data storage of personal information [PER18]. These two techniques, however, vary significantly in light of the GDPR. The main difference rests on whether the data can be re-identified or not [CLA05].

Pseudonymization is a data management and de-identification procedure that increases privacy by replacing the true identities of individuals or organizations. Identifying fields are substituted or replaced with a data record by using one or more artificial identifiers, or pseudonyms, that cannot be linked directly to their corresponding nominative identities. Pseudonymization is defined under the GDPR as the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person [GDP16].

Most pseudonymization procedures use a trusted third party as an intermediary to perform the pseudonymization process. This means that there are at least three entities being involved in the process. There is the primary data source that has access to nominative personal data, the trusted third party, and the data register that uses the artificial identifiers (pseudonymized data) to protect the privacy of individuals [NOU07].

While pseudonymization is an effective security measure, is still regarded to be personal data and remains under the scope of the GDPR [ICO19]. The reason is that anybody within the organization or a malicious party can always obtain exposure by using secondary identification tools based on the open data fields [JAN11].

Contrary to pseudonymization, anonymization refers to the complete and irreversible removal of information from data sets, which could lead to any future re-identification of the data subject. For this reason, anonymization is regarded as the most desirable method for personal data protection. It allows data processing without risking the individuals' privacy [RAG13].

Recital 26 of the GDPR states that the principles of data protection should not apply to anonymous information. Namely, information that is not related to an identified or identifiable natural person [GDP16]. This means that when anonymization is engineered appropriately, it places the processing and storage of personal data outside the scope of the GDPR. For this reason, anonymization can be an effective method for mitigating privacy risk and protect data subjects [ICO19].

The Opinion 05/2014 [OP14] on anonymization techniques (namely, randomization and generalization such as noise addition, permutation, differential privacy, aggregation, k-anonymity, l-diversity and t-closeness) by the Article 29 Working Party adopted on 10 April 2014, concludes that in order to meet the current anonymization standards, data must be processed in such a way that a natural person cannot be identified anymore by using "all means likely reasonably to be used" either by the controller or a third party. This means that the prerequisites and the objectives of the anonymization process must be clearly established from the outset in order to achieve the targeted anonymization while producing some useful data. An important aspect is that the processing of data must use irreversible de-identification mechanism. That is, data must be stripped of sufficient elements such as the data subject can no longer be identified.

However, the Working Party advises that there is no one-size-fits-all solution; instead, anonymization should be taken on a case-by-case basis, using a variety of techniques and factoring in the opinion's recommendations. Data controllers are advised to tailor-make the anonymization method to the specific circumstances. In addition, risk assessment should be carried out on a regular, continuous basis in light of the residual risk of identification [OP14].

3.2. HOMOMORPHIC ENCRYPTION WITHIN ENERGYSHIELD

Personal data needs to be encrypted both at rest and in transit. Data at rest refers to data when data is stored and data in transit is when data is transferred from one place to another. While modern encryption techniques are very secure since they require a lot of time, effort and resources to break it, they also make it difficult to process and analyze the data without first decrypting it – and decrypting the data exposes the data again to potential threats [CAS19].

For this reason, the EnergyShield project is developing a Homomorphic Encryption (HE) tool. HE has a great deal of potential in the field of cryptography and cloud security. HE can be defined as the conversion of data into ciphertext that can be analyzed and worked with as if it were still in its original form [KAN17]. In other words, HE is a special kind of encryption which allows complex computation and mathematical operations on the ciphertext without decrypting and exposing the encrypted data [BHA18].

HE is expected to play an important role in cloud computing transformations since it allows companies to store encrypted data in public or hybrid clouds while still benefiting from the cloud provider's data analytic tools. In conventional approaches, different pseudonymization and anonymization techniques are applied to provide data security and data protection, however, at the expense of usability. HE techniques allow one to keep data encrypted while using all the computational power to analyze data in the cloud [JUN16].

Encryption schemes that allow operations on encrypted data have a wide scope of applications in cryptography. The purpose of HE is to permit robust and secure computation on encrypted data. This means that data analytics tools can be performed on the ciphertext without revealing the plaintext [SRI17]. The HE properties will have a valuable application in the context of the EnergyShield project since it will allow searching data privately in an encrypted domain.

While HE operations can add an extra layer of security, they are still in an early phase of development. The main problem with HE is that they often increase the 'noise.' Noise in computer science is a small term added to the ciphertext while encrypting data. This slows down processing speed and can make the decryption operation worthless. Put differently, if the noise is larger than a certain maximum value, the ciphertext will no longer be correctly decrypted [JLI19].

For this reason, one of the components of the EnergyShield toolkit will develop an automated framework which reduces the noise of HE operations. This will allow users to search and analyze data without ever revealing any private and confidential information because data would remain encrypted – both at rest and in transit.

While noise can add an extra layer of protection, if too much noise is added to the ciphertext, the decryption function does not work. The challenge from a data protection and data security point of view is to generate the right amount of noise, so as to protect the data subject's privacy while preserving the usefulness of the released responses. The proposed HE scheme in the EnergyShield project attempts to provide a high level of security while reducing and keeping the right amount of noise.

In order to manage and reduce the noise, the EnergyShield project is developing a searchable encryption tool based on Rivest-Shamir-Adleman (RSA). RSA is a widely used public-key cryptosystem for secure data transmission. An encryption scheme using noise in its encryption will be presented, and also the problems that may arise if the framework is to be fully homomorphic.

Managing the noise in practice can be done in two ways as follows [ACK19]:

a) Using the bootstrapping procedure: bootstrapping in the context of HE means taking an input ciphertext with a large amount of noise, and outputting a new ciphertext which has less noise and can be used for further computation. Therefore, the entire HE operation can be performed by bootstrapping at appropriate points [ACK19].
b) Pre-establishing the function to be evaluated and setting the specific parameters in order to allow for the noise growth to occur in a controlled environment. By using this technique, we ensure that the output ciphertext will have a noise level below the threshold at the end of the evaluation [ACK19].

In any case, in order to achieve correctness and optimal performance, it is fundamental to manage the level of noise growth. The partners of the EnergyShield project are currently working on a Java programming language based on a Paillier implementation scheme.

A Paillier scheme is a probabilistic asymmetric algorithm for public key cryptography. Probabilistic encryption in a HE context means the use of randomness in an encryption algorithm by introducing an element of chance [GFB10]. Although the Paillier scheme is not fully homomorphic, it is a good source to use since it enables flexibility to modify and implement for other requirements.

In the EnergyShield project, we are using the following algorithms for the elaboration of the HE searchable tool:

3.2.1. KEY-GEN ALGORITHM:

a) Choose two prime numbers p & q and calculate n=p*q and λ = lcm(p-1,q-1) such that gcd(p*q,(p-1)*(q-1)) = 1;
b) Select g Є Z*n^2 and calculate μ = (L(g^λ mod n^2))^(-1) mod n where L(x) = x-1/n;
c) n, g acts as a public key;
d) λ, μ acts as a private key.

3.2.2. ENCRYPTION ALGORITHM:

a) Let m Є Zn be the message;
b) Choose r Є Z*n;
c) Required Cipher text is c = g^m *r^n mod n^2.

3.2.3. Decryption Algorithm:

a) Compute m = L(c^λ mod n^2)*μ mod n.

The schema diagram below illustrates how the Programmable Logic Controller (PLCs) of the company send measurements or Anomaly alerts messages to an API. The API will filter the messages and encrypt the data and write to two separate database tables. One for actual measurement and the other for anomaly message. Then the Analyst will use the encrypted data to analyze them.

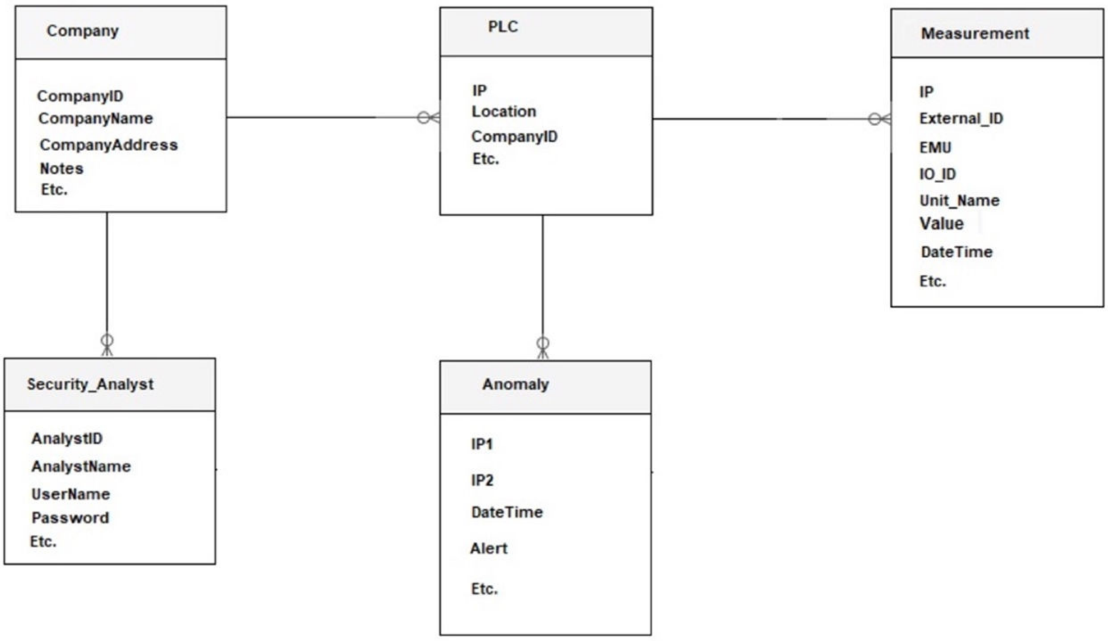


Figure 2. Schema diagram

The project partners will work on an extended and modified version in order to support more computations. The HE searchable component of the EnergyShield toolkit has been tested using the Java user interface which connects to a database. Further implementations of the HE component will be developed on the MySQL database on a later stage. This will make the scheme more suitable for data protection and data security.

4. INTERNATIONAL DATA TRANSFERS

The GDPR provides uniform protection of personal data and personal privacy in all the countries of the European Economic Area (EEA) The EEA includes EU countries and also Iceland, Liechtenstein and Norway. It allows them to be part of the EU's single market. Thus, personal data can be transmitted freely within this area without restrictions. However, in other countries outside the EEA, there are no general rules that provide equivalent protection. For example, Russian and Brazilian data protection rules are different than the European. The GDPR contains several rules and restrictions about the transfer of personal data to countries outside the EEA.

Not just sending data directly (e.g. email, flash drive) outside the EEA triggers this prohibition. If you process personal data that someone has access outside EEA or you use service providers outside the EEA, such as storing personal data on a cloud service, it is restricted by the strict rules of the GDPR [DIS19]. Transfer of personal data to a third country is when personal data is made available to someone outside the EEA.

For example:

- giving personal data on a hard drive to a person in a country outside the EEA,
- sending documents that contain personal data by e-mail to a person in a country outside the EU/EEA,
- using a data processor in a country outside the EEA,
- giving someone outside the EEA access to personal data (e. g., reading rights),
- the storage of personal data in a cloud service or on a server that is based outside the EEA.

However, publishing something on the Internet does not constitute a transfer of data to a third country if the website is stored with an Internet provider that is established inside the EEA [DIS19].

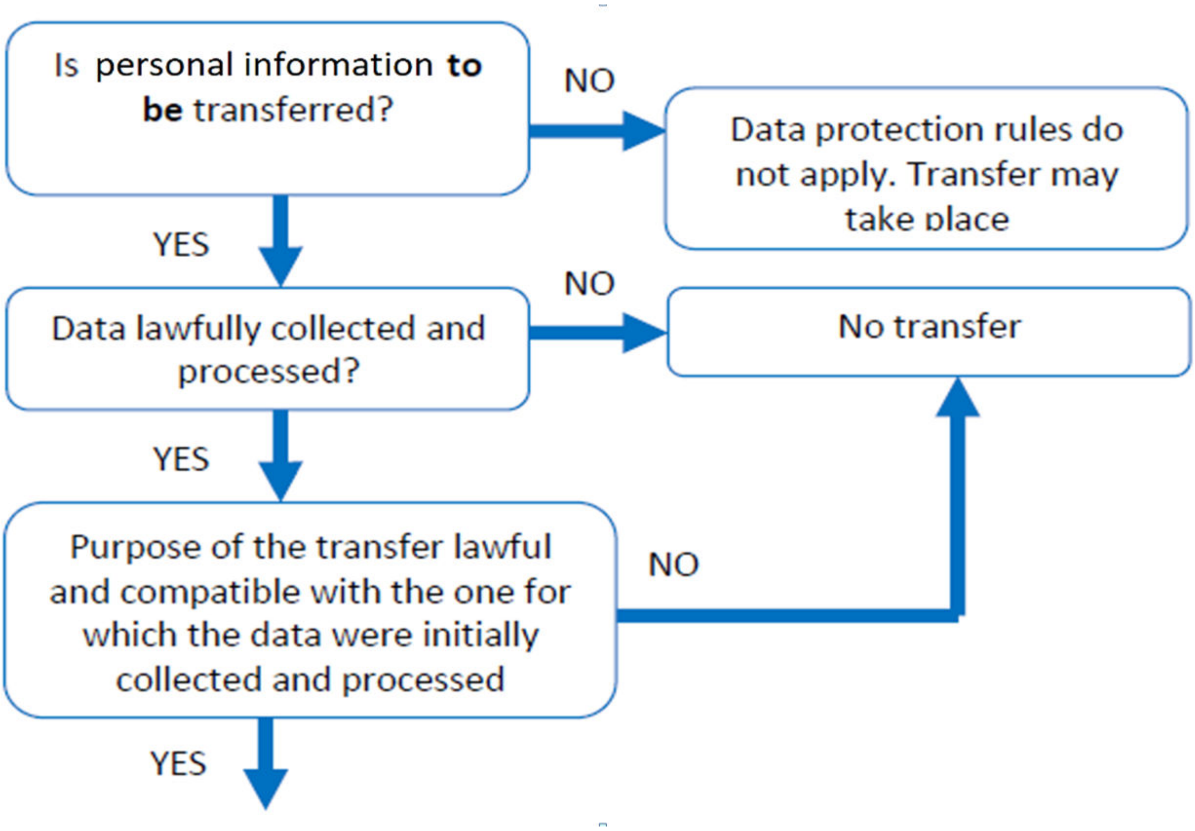

Is personal information to be transferred?
NO
Data protection rules do not apply. Transfer may take place
YES
NO
Data lawfully collected and processed?
No transfer
YES
Purpose of the transfer lawful and compatible with the one for which the data were initially collected and processed
NO
YES

Figure 3. Crucial questions before the examination of transfer methods [EDP19]

Figure 3 illustrates the first steps before sending data to third countries. First, if the data is not personal data (e.g., it is anonymous data), then it can be sent without restriction. However, if the data is personal, or just pseudonymized, then several restrictions apply. If the data is collected lawfully, and the purpose of the transfer is compatible with the one for which the data was collected, the data controller might go to the second step.

The transfer of personal data is permitted to countries outside the EU/EEA, if:

a) There is an **adequacy decision**: there is a decision from the European Commission that, for example, a certain country outside the EU/EEA ensures an adequate level of protection [GDP16] (e.g., Israel, Japan), or
b) **Adequate safeguards**: the data controller has taken appropriate protection measures (e.g., using Standard Contractual Clauses or Binding Corporate Rules to send data), or
c) **Specific derogations** and single cases (e.g., consent).

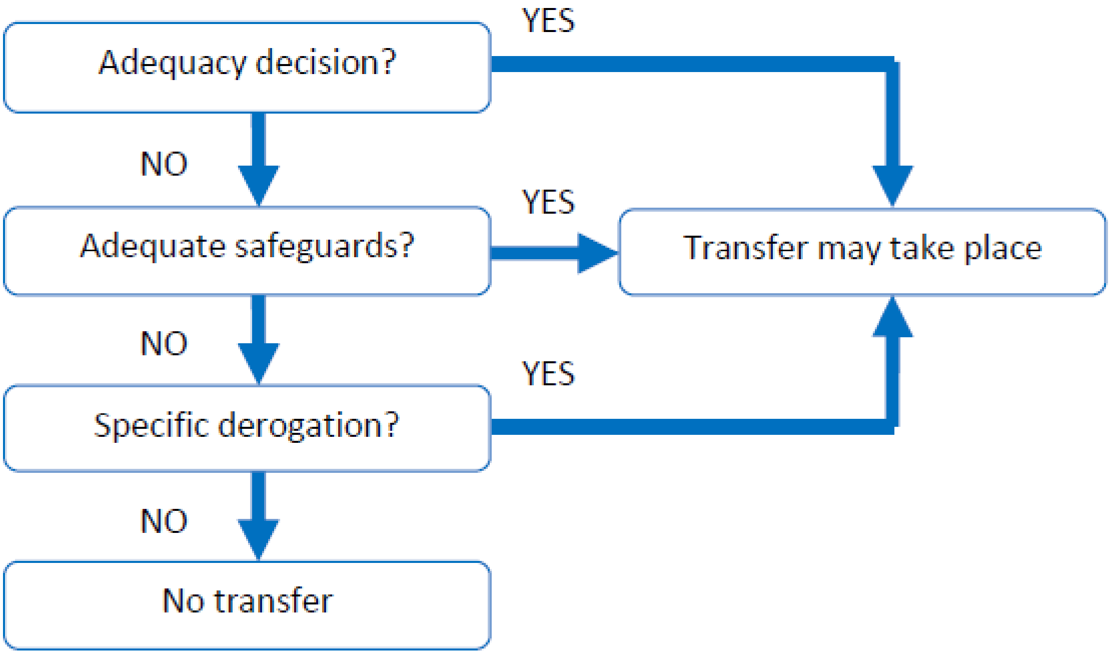


Figure 4. Permitted transfer of personal data from EEA to a third country [EDP19]

4.1. COUNTRIES WITH ADEQUATE PROTECTION

4.1.1. DECISION OF THE EUROPEAN COMMISSION

The European Commission decides which countries provide a sufficiently high level of protection for personal data. When the European Commission takes decisions concerning an adequate level of protection, they look, among other things: respect for human rights and fundamental freedoms, relevant legislation, the existence and effective functioning of one or more independent supervisory authorities.

The GDPR calls this 'adequate level of protection'. In those countries, national laws provide a level of protection for personal data which is comparable to those of EU law [WAG18]. It can also apply to international organizations, certain territories or sectors in a third country (e.g., United States and Canada). The personal data can be transferred in these countries and organizations without any specific authorization.

The European Commission has so far recognized Andorra, Argentina, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, as providing adequate protection [EUR19].

The European Commission has also assessed that the level of protection is adequate in certain areas or under special conditions in the following countries:

- Canada, if their legislation for the protection of personal data in the private sector is applicable to the recipient's personal data processing [EUC19].
- The USA, if the recipient has joined the Privacy Shield Framework [EUS19].

4.1.2. PRIVACY SHIELD

In general, the EU does not list the US as one of the countries that meet the requirements of the GDPR, thus the US does not provide adequate protection of personal data by the terms of the GDPR [GDP16]. However, the transatlantic relations are important, thus the EU and US created the Privacy Shield framework to facilitate data transfers. This framework protects the fundamental rights of the data subjects in the EU whose personal data is transferred to the US for commercial purposes [SHA17]. It allows the free transfer of data to companies that are certified in the US under the Privacy Shield Framework [ESS19]. However, the framework is currently under the revision of the European Court of Justice; thus it is possible it might be declared invalid (as happened with the Safe Harbor before [SCH14], [KUN17]) or changed in the future [HCI19].

The program is administered under the International Trade Administration (ITA) within the US Department of Commerce, enabling US-based organizations to join to the Privacy Shield Framework in order to benefit from the adequacy determinations. To join the program, a US-based organization will be required to self-certify to the Department of Commerce and publicly commit to comply with the Framework's requirements. While joining the Privacy Shield is voluntary, once an organization has made the public commitment to comply with the Framework's requirements, the commitment will become enforceable under US law [PSP19].

Before sending personal data to a US organization under the Privacy Shield Framework, it is important to:

- check on the Privacy Shield list [PSP19] to see whether the organization has a current certification; and
- make sure the certification covers the type of data you want to transfer.

4.2. TRANSFERS WITH APPROPRIATE SAFEGUARDS

If there is no adequacy decision for a third country (e.g., Brazil, Russia), this does not necessarily foreclose the data transfer there. Rather, the sender needs to ensure in another way that the personal data will be sufficiently protected by the recipient in that country. This can be assured with several solutions, such as Standard Contractual Clauses (SCC) or Binding Corporate Rules (BCR) [GDP16].

4.2.1. STANDARD CONTRACTUAL CLAUSES

It is possible to transfer personal data to a third country without adequate protection if the sender and the receiver have entered into a contract incorporating standard data protection clauses [GDP16]. These are also known as the 'Standard Contractual Clauses' (SCC) or model clauses. These clauses are adopted by the European Commission, and they can be downloaded from their website [ECC19]. These clauses contain contractual obligations for the sender (data exporter from the EEA), the receiver (data importer), and rights for the individuals whose personal data is transferred. Individuals can directly enforce those rights against the data importer and the data exporter. The European Commission plans to update the existing contracts; thus, it is advised to keep checking the official EU national data protection authority [ECC19], [EUC04], [EUP10] websites before entering into a contract.

It is also very important that **the parties must use the standard contractual clauses in their entirety and without amendment.** They can include additional clauses on business-related issues if they do not contradict the standard contractual clauses. They can also add parties (i.e., additional data importers or exporters) provided they are also bound by the standard contractual clauses. In conclusion, it is possible to add new information into the contract, but the **original text about standard contractual clauses for the protection of personal data cannot be changed and contradicted**. As mentioned above, at the moment of writing these reports, there is a pending case before Court of Justice of the EU (CJEU) which might amend or strike down the Standard Contractual Clauses (SCC). Therefore, organizations wishing to use the EnergyShield toolkit should monitor the outcome of this trial [HCI19].

4.2.2. BINDING CORPORATE RULES

The aim of using BCR is to provide adequate safeguards for transferring data to a third country. This instrument was developed by the Article 29 Working Party in a series of working documents, including application forms and guidance.[IAP19], [DPW18], [DWP18], [DPW17], [DPP18]. Data controllers and processors can transfer data to a third country if both the sender and the receiver have signed up to a group document called BCR [GDP16]. BCR is an internal code of conduct operating within a multinational group, which applies to restricted transfers of personal data from the group's EEA entities to non-EEA group entities [MAK18]. This entity might be a corporate group or a group of undertakings or enterprises engaged in a joint economic activity (e.g., franchises or joint ventures) [ICO19]. The sender must submit BCR for approval to an EEA supervisory authority in an EEA country where one of the companies is based. Usually, this is where the EEA head office is located, but it does not need to be [DPP18].

4.2.3. OTHER SAFEGUARDS IN SPECIAL CASES

a) A legally binding and enforceable instrument between public authorities or bodies.

In a very limited scenario, data transfer to a third country can be made if both parties are a public authorities or public bodies, and both have signed a legally binding instrument that provides for ‘appropriate safeguards’ for the rights of the individuals whose personal data is being transferred and it is legally binding and enforceable [GDP16].

b) An approved code of conduct together with binding and enforceable commitments of the receiver outside the EEA.

The restricted transfer can be made if the receiver has signed up to a code of conduct, which has been approved by a supervisory authority in the EEA. The code of conduct must include appropriate safeguards to protect the rights of individuals whose personal data transferred, and which can be directly enforced. However, this option is newly introduced by the GDPR, and there is no supervisory authority in the EEA that has adopted an approved code of conduct yet.

c) Approved certification mechanism.

An approved certification mechanism, together with binding and enforceable commitments of the receiver, might allow the transfer of personal data. The certification scheme must include appropriate safeguards to protect data subjects` rights, and these safeguards can be directly enforced. This option is newly introduced by the GDPR and no approved certification schemes are yet in use [GDP16].

4.3. SPECIFIC DEROGATIONS (EXCEPTIONS)

If the data transfer that is not covered by an adequacy decision (safe countries, such as Japan), nor an appropriate safeguard (e.g., standard contractual clauses, binding corporate rules), then the data controller can only make that transfer if it is covered by one of the 'exceptions' set out in Article 49 of the GDPR. It is important that these derogations can be only applied as a last solution, in the absence of an adequacy decision or appropriate safeguards [GDP16].

4.3.1. EXPLICIT AND SPECIFIC CONSENT FROM THE DATA SUBJECT

Given that valid consent must be both specific and informed, the data controller must provide the data subject detailed information about the data transfer [GDP16]. It is crucial that the data controller cannot obtain valid consent for transfers in general. Because of the high threshold for valid consent, and it can be withdrawn anytime, it is not a feasible solution for the data transfer.

In this case, the data subject needs to be informed:

a) the identity of the data receiver, or the categories of receivers;
b) the country or countries to which the data is to be transferred;
c) why the data controller needs to make a restricted transfer;
d) the type of data;
e) the individual's right to withdraw consent; and
f) the possible risks involved in making a transfer to a country which does not provide adequate protection for personal data and without any other appropriate safeguards in place. For example, the data controller might explain that there will be no local supervisory authority, and no (or only limited) individual data protection or privacy rights in the third country. [ICO19]

4.3.2. CONTRACTS

The transfer is possible in special cases if it is necessary for the

a) performance of a contract between the data subject and the controller, or
b) the implementation of pre-contractual measures taken at the data subject's request, or [GDP16]
c) for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person [GDP16].

These exceptions can be only used for occasional transfers (more than once, but not regularly). Thus, it cannot cover for example a cloud computing service [ICO19]. Furthermore, the transfer must be also necessary, thus the contract cannot be concluded or performed without the data transfer. For instance, in the case of booking a hotel in a third country, it is necessary to send basic information about the passenger to reserve the room. The necessary basic information can be the name of the person. However, sending other data (e.g., profession, political opinion) is unnecessary for the contract/reservation.

4.3.3. IMPORTANT REASONS FOR PUBLIC INTEREST

In this case, there must be a Member State or EU law, which states or implies that transferring data for a purpose is allowed for public interest. For instance, an international treaty on fighting against terrorism. The data transfers should not be general on this legal base neither, this is also an exemption [GDP16].

4.3.4. LEGAL CLAIMS

In this case, the transfer is necessary for the establishment, exercise or defense of legal claims [GDP16]. The GDPR also clarifies that the transfer can be made where it is occasional and necessary in relation to a contract or a legal claim, regardless of whether in a judicial proceeding or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies [GDP16].

4.3.5. VITAL INTEREST

The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent [GDP16]. In this case, there is a medical emergency and the transfer is directly necessary in order to give the medical care required.

4.3.6. PUBLIC REGISTRIES

The GDPR allows the transfer of personal data from registers under certain conditions. A register, in general, is defined as a “(written) record containing regular entries of items or details” or as “an official list or record of names or items” [MER19]. In the context of Article 49, a register could be in written or electronic form [GDP16]. For example, registers of companies, criminal convictions, public vehicles. The register in question must, according to Union or Member State law, be intended to provide information to the public. Therefore, private registers (those in the responsibility of private bodies) are outside of the scope of this derogation [DWW18].

4.3.7. COMPELLING LEGITIMATE INTEREST

This is the final exception for transferring personal data, in case no other exceptions can be applied. The transfer must be necessary for compelling legitimate interests, which is the highest level of legitimate interest. Only interests that can be recognized as “compelling” are relevant and this limits the scope of the application of this derogation. Not all conceivable “legitimate interests” [GDP16] will apply here. The transfer might concern only a limited number of data subjects, cannot be repetitive and the controller needs to inform the supervisory authority and the data subjects about the transfer.

For instance, this might be the case if a data exporter is compelled to transfer the personal data in order to protect its organization or systems from serious immediate harm or from a severe penalty which would seriously affect its business [DWW18].

Table 1. Assessment of transfer methods

Transfer method	Pros	Cons
Explicit consent of the data subject	It can be shaped for the purposes/goals of the processing	Difficult to change it and reach the data subjects
Privacy Shield	Easy to register	Rigid rules on sensitive data, just for United States
Adequacy decision by the EU	Smooth data transfer	Difficult to get it
binding corporate rules	Just for companies dealing with the employee data inside the organization	
Standard data protection clauses	High chance that it will have the Safe Harbor's fate (similar problems, not enough appropriate safeguards)	

5. DATA SECURITY

The EnergyShield toolkit is itself a great asset for providing data security, by conducting a vulnerability assessment, monitoring & protection (anomaly detection and DDoS mitigation) and learning & sharing (security information and event management). However, since the developers, the operators, and the toolkit itself might process personal data, it is crucial for all the actors to handle personal data properly by providing the data security measures which are proportional to the risk posed. In the following sections, this report provides the essential technical and organizational data security requirements.

Weak information security might lead to individual harms, which can result in minor or serious damages. Weak security within critical infrastructures might cause disruption in essential services, such as water and electricity. For these reasons, the GDPR requires data controllers to process personal data securely. The requirement to take 'appropriate technical and organizational measures' to protect the data against inappropriate use is not new. It replaces and mirrors the previous requirements of the Data Protection Directive from 1995. The improvement and the biggest achievement of the GDPR are that these requirements are more standardized and unified among the EU Member States, providing stronger data security in the whole EU. However, the GDPR just states the basic requirements, without going into technical details. On the one hand, this technical neutrality ensures the long applicability of the Regulation. On the other hand, there might be a lot of confusion about the level of the technical security required to comply with the GDPR. There are several detailed guides available from national authorities and international organizations, but it may not be immediately clear what kind of security measures the developers and clients need to put in place, what is simply a suggested approach and what is essential [ICO01].

Our report intends to highlight essential measures, what both developers and clients need to follow to comply with the relevant data protection and other regulations concerning safety and security. It is important to mention that the technical and organizational measures described in this section are representing the minimum requirements. In some cases, the data controllers and processors would need to implement stronger measures to comply with the legal requirements. There are several guidelines [ICO09] and certifications [CES01] that can help to comply with these duties and the consultation with the data protection authorities might be also necessary. Furthermore, the security level maturity survey among the partners also highlights the differences and the fields which require improvement in data security.

5.1. APPROPRIATE MEASURES

The GDPR security principle lays down the most important requirements for data security, requiring data controllers and processors to ensure appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organizational measures. These principles are called 'integrity and confidentiality' [GDPR Article 5 (1) (f)].

The question is what level of security is necessary to provide an adequate level of protection. There is no ‘one size fits all’ solution to information security; thus, the GDPR also provides a risk-based approach. This means that the following circumstances need to be taken into account when the security measures are chosen:

a) state of the art of technology;
b) the costs of implementation;
c) the nature, scope, context and the purposes of processing [GDPR Recital 83];
d) level of risk of the data processing [GDPR Article 32];
e) the sensitivity of the data (e.g., data about health or religion);
f) the number of staff at the data controller or processor and the extent of their access to personal data (just a few people can access it, or hundreds; they can read or also edit, delete the data).

5.2. TECHNICAL MEASURES

During the development, testing, and application of the EnergyShield toolkit, the following technical measures need to be applied, when personal data is processed.

5.2.1. PSEUDONYMIZATION AND ANONYMIZATION

As explained above in section 3, anonymization means that the data subject is (theoretically) no longer identifiable, thus anonymized data cannot be linked to an individual and falls outside of the data protection law [GDPR Recital 26]. Pseudonymization is a data management and de-identification procedure that increases privacy by replacing the true identities of individuals or organizations. Identifying fields are substituted or replaced with a data record by using one or more artificial identifiers, or pseudonyms, that cannot be linked directly to their corresponding nominative identities [CBD05]. It is important to highlight that pseudonymized data is still personal data, thus the requirements of the GDPR need to be applied. In the survey that we carried out during this report, several partners noted that they only process anonymized data. However, we recommend the project partners to ensure the data is correctly anonymized, since in many cases, it is still possible to identify individuals. Pure statistics, such as network usage, are anonymized data. (See more about de-identification techniques in section 3, in particular with regard to the Homomorphic Encryption tool).

Example from the Vulnerability Assessment (VA) tool

The Vulnerability Assessment (VA) tool is a component of the EnergyShield toolkit that will operate in an integrated context and it will build a threat model based on input from the Cyber-socio-culture tool and infrastructure descriptions. This model will continuously be updated as the source information changes. Although the system does not need to handle personal data, the developers of the component have drawn up a use case scenario, when the toolkit might process personal data due to the operator’s settings. In this scenario, personal data could be included in the infrastructure description feed or as part of security events. Personal data as part of the infrastructure description feed is to be considered a misconfiguration in system deployment. However, even in situations like this, the Security Culture tool should protect the VA tool from such data. Furthermore, the developers of the VA tool will investigate opportunities to avoid this by technical means (e.g., pseudonymization/anonymization of PII in the data feed of the Security Culture tool).

5.2.2. ENCRYPTION

The GDPR highlights the importance of the encryption of personal data [GDPR Recital 83 and Articles 4 (c); 32 (1) (a)]. In this Report [ICO02], the adequate security measures by encryption is highlighted above in section 3.

3) Data can be only accessed and processed by authorized people

The developers and operators need to ensure that each user uses her/his own username and password and they use an account that has permissions appropriate to the job they are carrying out at the time.

Authentication factors can be grouped into three families according to:

a) something the user knows (e.g., a password);

b) something the user has (e.g., a smart card);

c) something that the user does, for example providing a digital fingerprint or a handwritten signature [CNI18].

The authentication of a user is qualified as strong when it needs at least the combination of two of these factors.

BOTH TOOLKIT DEVELOPERS AND OPERATORS SHOULD AVOID:

d) Creating shared accounts for multiple users;

e) Granting administrator rights to users who do not need them;

f) Granting a user more privileges than necessary;

g) Forgetting to remove temporary authorizations granted to a user (e.g., for a replacement);

h) Forgetting to delete user accounts of individuals who have left the organization or changed their role/position.

5.2.3. PASSWORDS

The toolkit developers need to maintain a high level of security during the development period, to make sure intruders do not acquire critical information about the toolkit components since it can also lead to vulnerability issues during the application of the toolkit. Furthermore, the operators need to have strong security and access in the toolkit to protect their staff and critical data.

There are some general expectations [CNI18], when passwords are used for authentication, notably by storing the passwords in a secure way and applying the following complexity requirements to them. For instance, the Commission National de L'Informatique et des Libertes (CNIL) Guideline requires the following measures:

a) be at least 8 characters long including 3 out of 4 types of characters (uppercase, lowercase, numbers, special characters), if the authentication includes a measure restricting access to the account (e.g., temporary lockdown of the account after several failed attempts; a ‘Captcha’; the locking of the account after 10 failed attempts);

b) have 12 characters minimum and 4 types of character if the authentication only relies on a password;
c) have over 5 characters if the authentication requires some additional confidential information. For the additional information, use a confidential identifier that is at least 7 characters long and block the account on the 5th unsuccessful attempt;
d) the password can be just 4 characters if the authentication relies on equipment held by the individual and if the password is only used to unlock the physical device held by the individual himself/herself (for example a smart card or mobile phone) and that the device is blocked on the third unsuccessful attempt.

The staff should not communicate any information about security measures and their passwords (e.g., they should not send their password via email or tell it to other colleagues; the password should be different than the one used for other accounts, and should not include their birthday or name).

5.2.4. LOGGING ACCESS AND MANAGING INCIDENTS

There might be fraudulent access or misuse of personal data both on the side of the developers and the operators of the toolkit in the future. Therefore, it is necessary to log the most important actions carried out on the IT systems to determine the origin of an incident. The logging and incident management system must record relevant events and guarantee that these logs cannot be altered [CNI18].

5.2.5. PREVENTING FRAUDULENT ACCESS, VIRUSES OR REMOTE-CONTROL TAKEOVER

To avoid these fraudulent incidents on the developer’s side, it is crucial to:

a) install firewall and antivirus software;
b) regular updates of the software;
c) security updates are carried out automatically when possible;
d) limit the connection of mobile media (USB sticks, external hard drives, etc.) to what is essential;
e) remove unused software and services from the devices to reduce the number of potential vulnerabilities.

5.2.6. SECURING MOBILE DATA PROCESSING

The increased use of laptops, tablets, flash drives and smartphones makes it necessary to prepare for data breach following the theft or loss of such equipment. Therefore, toolkit developers need to:

a) implement controlled backup and synchronization measures to avoid losing data in the case of theft, destruction or loss of mobile devices;
b) encryption measures protecting mobile workstations and storage media (e.g., encryption of the hard drive in its entirety, or certain files);

c) in the case of smartphones, in addition to the PIN code for the SIM card, safe login is also necessary, such as password, fingerprint or FaceID;
d) limit the storage of data on mobile workstations;
e) Implement protection measures against theft (e.g., security cable, visible marking of equipment).

5.2.7. PROTECTING INTERNAL NETWORK

It is crucial to provide adequate protection for the internal network on both the developers' and operators' side, by limiting the network functions. For instance:

a) limiting Internet access by blocking non-essential services (VoIP, peer to peer, etc.);
b) providing safe Wi-Fi networks, by applying the state-of-the-art encryptions (WPA2 or WPA2-PSK with a complex password);
c) networks open to guests must be separate from the internal network;
d) limit network traffic to essentials [CNI18].

5.2.8. SECURING SERVERS

Since servers store a large amount of important data, it must be well protected against incidents by both toolkit developers and operators, with several measures, such as:

a) allowing only qualified individuals to access the tools and administration interfaces;
b) specific, more secure password policy for server administrators;
c) installing updates and carrying out backups regularly;
d) implementing protocols ensuring encryption and authentication, as a minimum for any online data exchange and verify its proper implementation via the appropriate tools [TSL01];
e) server administration operations should be carried out via a dedicated and isolated network, accessible only with strong authentication and enhanced traceability.

5.2.9. REGULAR BACKUPS

It is crucial to have an appropriate backup process for the case that the systems suffer a physical or technical incident. This is crucial for both toolkit developers and operators since an accidental data loss can slow down and hinder the achievement of the EnergyShield project milestones. During the application of the toolkit, servers are also used. For instance, the anomaly detection tool directly gathers electrical signals from the endpoint device (not relying on data fed by the PLC, which could be faked by malware) and the software is installed on a server at the customer's location (in complete isolation from externally-connected communications networks), which makes the EnergyShield solution uniquely insulated from the cyber-threat itself so it cannot be breached, infiltrated or circumvented.

The organizations should be able to restore the lost data as soon as reasonably possible. For instance, applying the well-known '3-2-1' backup strategy: three copies, with two stored on different devices and one stored off-site. Furthermore, the backups should be stored on media which is safe (e.g., CDs and DVDs are unsafe, hard drives or flash drives have better longevity).

5.2.10. ARCHIVING DATA

The data which is no longer necessary for the purpose it was collected for should be archived, but still, it has not yet reached the end of its data retention period (e.g., it should be still kept in the case of litigation). Specific care is necessary when sensitive data are archived.

Furthermore, when the archived data is destroyed at the end of the retention period, it should be done properly and entirely. For instance, on hard drives, using dedicated data deletion software which has been audited or certified, destroying the DVDs.

5.2.11. MAINTENANCE OF SYSTEMS

All computer hardware has a limited lifecycle, thus servicing and maintaining them is crucial. However, third parties responsible for repairing them might pose risk, thus deleting data from the devices is crucial before sending them out to third parties. Furthermore, maintenance actions need to be logged and described with the dates, nature of operations and names of the intervening parties. Both toolkit developers and operators need to follow this advice since vulnerabilities might result from maintenance issues.

5.2.12. CLOUD PROVIDERS

Storing and processing personal data in the cloud poses risk, since the data for which the data controller is responsible will leave its own network. Furthermore, using cloud computing services in the absence of any guarantee regarding the effective geographical location of the data or without ensuring the lawfulness of the data transfers outside of the European Union might be unsafe, unlawful and result in penalty. It is crucial to have safe use and backups on cloud services, such as two-factor authentication, and default backup and sync options, with data restore tools [ICO03].

The toolkit will use homomorphic encryption-based algorithms to allow smart meter data to be encrypted and passed onto a third-party cloud service where it can be securely shared for operational and business intelligence without compromising the privacy and identity of the consumers.

5.2.13. SECURING TRANSMISSION OF DATA WITH OTHER ORGANIZATIONS

It is important to note that electronic messaging services are not a secure means of communication to transmit personal data, without additional measures [CNI18]. Data transmissions need to be secure, by applying encryption and protocols (e.g., using encrypted mail services). During the development of the project and the application of the toolkit, critical information (e.g., key information on the operators' safety infrastructure) need to be transmitted in a secure way.

5.2.14. SOFTWARE DEVELOPMENT

Privacy and data security should be reflected from the design stages [ICO05] of the software development. CNIL and other guidelines provide examples of data minimization, encryption, virtual machines and fictional data to test applications [GDPR Recital 78]. The EnergyShield toolkit already aims to reach this goal, for instance by applying homomorphic encryption. However, in every stage of data processing, using anonymized or at least pseudonymized data would be preferable. In a case of a breach, this would minimize the potential damages.

5.2.15. CONSTANT AWARENESS

Cybercrimes and security breaches can go unnoticed for long periods of time. Many organizations only find out they have been attacked when it is too late. It is crucial to constantly check the security software messages, access control logs and other reporting systems you have in place on a regular basis [ICO06]. As the toolkit aims to avoid these situations on the operator's side, this requirement mainly concerns the toolkit developers. They should:

a) constantly check security software logs and messages;
b) immediately act on alerts;
c) be aware of the software and services are running on the network to spot any issues.

5.2.16. POLICIES AND RULES IN THE CASE OF 'BRING-YOUR-OWN-DEVICE' IF IT IS OFFERED TO THE STAFF

Bring-your-own-Device (BYOD) refers to the policy when workplaces allow the employees to take their own IT devices to work (e.g., laptop, tablet) and use them to work and access information at the organization. When the developers allow their employees to use their own devices, it might pose risk. Permitting employees to process the company's personal data on their own devices raises a number of questions about compliance with data protection obligations. It is important that the data controller (the developer) must remain in control and responsible for the personal data, regardless of the ownership of the device used to carry out the processing [ICO07]. Storing critical information on a BYOD is extremely risky. It should be avoided when it is possible.

5.3. ORGANIZATIONAL MEASURES

It is crucial for both toolkit developers and operators to apply security measures outside technical measures. The organizational measures are as crucial for reaching and maintaining a high level of security as technological solutions. Even the strongest technical safeguards can be bypassed if unauthorized people can have access to critical assets, such as servers. Therefore, we suggest all the developers and operators to follow the essential organizational measures described below.

5.3.1. PHYSICAL AND ORGANIZATIONAL PROTECTION OF DATA

The most important task is to build awareness of security and privacy in the whole organization. This can be reached by pointing to a person responsible for this area and providing this person with resources and real power to enforce these tasks.

There are several crucial tasks to improve the security in organizations, the most essential are:

a) co-ordination between key people in the organization (e. g., the IT and security manager(s) need to know about disposing or selling any IT equipment); [ICO08]
b) monitoring and protecting the access to premises or equipment;
c) setting up smoke detectors, as well as firefighting resources, and inspect them annually;
d) systematic checks to ensure that the security measures remain appropriate and up to date; [ICO09]
e) carrying out an information risk assessment;
f) the staff need to sign a confidentiality agreement, or include in the employment contracts a specific confidentiality clause concerning personal data;
g) have a responsible person from the organization to supervise the work done by third parties (record maintenance in a register);
h) withdraw the users' access rights as soon as they are no longer authorized to access a room or an IT resource, as well as at the end of their contract. Carry out an annual review of the access rights.

5.3.2. DATA PROCESSORS AND SUBCONTRACTORS

Almost every business needs to rely on third parties to process personal data. Whether it is an email client, a cloud storage provider, or analytics software, the organisation must have a data processing agreement with each of these services to achieve GDPR compliance [DPA01]. Thus, we suggest all the toolkit developers to have a proper agreement with third parties who process personal data. Subcontractors always need to provide guarantees that they are reliable and that they possess the required knowledge and resources [GDPR Article 32 (4)]. These guarantees should include, for instance:

a) encryption of transmission and data according to its sensitivity;
b) network protection, traceability (logs, audits), access rights management, authentication [GDPR Recital 81].

The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller unless he or she is required to do so by Union or Member State law [GDPR Article 32 (4)]. The data processing agreements need to be signed with the subcontractors, before the start of the processing [GDPR Article 28 (3)]. Sending data before signing the contract violates data protection law. The contract should detail the parties, rights and duties, and adequate safeguards of the processing. There are several data processing agreement templates on the Internet from various sources [DLA17]. However, we recommend looking for legal advice to draft the most updated and suitable agreement for the services. The rights and duties need to be carefully allocated among the data controllers and processors [GDPR Recital 79].

GDPR Article 28 (3) states:

'Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.'

The minimum requirements data processing agreements need to include:

a) The processor agrees to process personal data only by the written instructions of the controller;
b) New parties who come into contact with the data are sworn to confidentiality;
c) Appropriate technical and organizational measures are in place to protect the security of the data;
d) The subcontractor/data processor cannot engage another processor without prior specific or general written authorization of the controller. In the case of general written authorization, the processor has to inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes;
e) The processor will help the controller uphold their obligations under the GDPR, particularly concerning data subjects' rights;
f) The processor will help the controller maintain GDPR compliance with regard to Article 32 (security of processing) and Article 36 (consulting with the data protection authority before undertaking high-risk processing).
g) The processor agrees to delete all personal data upon the termination of services or return the data to the controller.
h) The processor must allow the controller to conduct an audit and will provide any information necessary to prove compliance [DPA02].

5.3.3. RAISING USER AWARENESS

Human error is a leading cause of breaches in security. This can be caused by simply sending an email to the incorrect recipient or opening an email attachment containing malware and clicking on a corrupted link. The staff at the toolkit developers' and operators' sides need to be trained to recognize these threats, such as phishing emails and other malware. Furthermore, the employees need to be aware of the risks involved in posting information relating to the business activities on social networks (this is also part of the requirement of confidentiality). Therefore, it is crucial to raise the awareness of privacy in the organization, by informing and educating staff about the measures implemented by their organization in order to deal with the risks and their potential consequences. This can be conducted by organizing awareness-raising sessions, regularly sending updates on the relevant procedures for the individuals' roles, sending them reminders via e-mail.

The following information should be clearly communicated to the staff, all the toolkit developers and future operators; [CNI18]

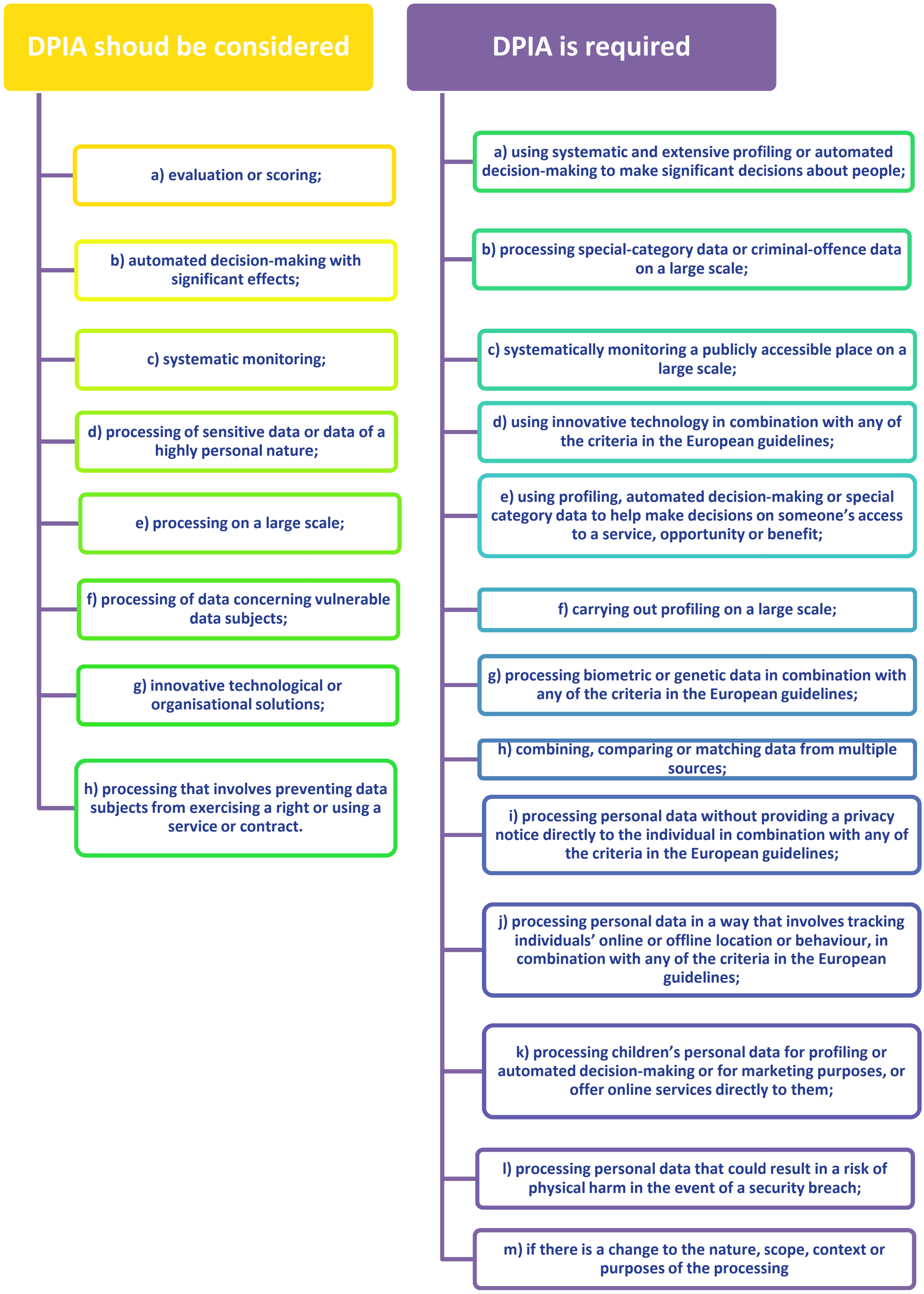
a) authentication means used by the organization;
b) the duty to inform the internal IT department about any suspected data breach or attempt to violate IT user account and generally any dysfunction;
c) never entrusting an identifier/password to a third party;
d) never installing, copying, editing or destroying software without authorization;
e) locking computers as soon as users leave their workstations;
f) never accessing, trying to access, or remove information if it does not relate to the tasks performed by the user;
g) respecting the procedures defined beforehand by the company in order to supervise data transfer on mobile media, notably by obtaining prior authorization from the supervisor and by complying with the security rules;
h) methods of intervention of the teams in charge of managing IT resources for the organisation.

5.4. DATA PROTECTION IMPACT ASSESSMENT

The Data Protection Impact Assessment (DPIA) is required under the GDPR when the data controller begins to process personal data in a way that is likely to involve ‘a high risk’ [DPI01]. The GDPR Article 35 (1) describes the requirement of DPIA:

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

While this passage makes it clear that a DPIA is required by law under certain conditions, it does not specify these conditions. To help clarify this requirement, we present below some concrete examples that would require a DPIA.



DPIA shoud be considered

- a) evaluation or scoring;
- b) automated decision-making with significant effects;
- c) systematic monitoring;
- d) processing of sensitive data or data of a highly personal nature;
- e) processing on a large scale;
- f) processing of data concerning vulnerable data subjects;
- g) innovative technological or organisational solutions;
- h) processing that involves preventing data subjects from exercising a right or using a service or contract.

DPIA is required

- a) using systematic and extensive profiling or automated decision-making to make significant decisions about people;
- b) processing special-category data or criminal-offence data on a large scale;
- c) systematically monitoring a publicly accessible place on a large scale;
- d) using innovative technology in combination with any of the criteria in the European guidelines;
- e) using profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit;
- f) carrying out profiling on a large scale;
- g) processing biometric or genetic data in combination with any of the criteria in the European guidelines;
- h) combining, comparing or matching data from multiple sources;
- i) processing personal data without providing a privacy notice directly to the individual in combination with any of the criteria in the European guidelines;
- j) processing personal data in a way that involves tracking individuals' online or offline location or behaviour, in combination with any of the criteria in the European guidelines;
- k) processing children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them;
- l) processing personal data that could result in a risk of physical harm in the event of a security breach;
- m) if there is a change to the nature, scope, context or purposes of the processing

Figure 5. Things to be considered before running a DPIA

Since the development and deployment of the toolkit still takes time, we recommend revisiting the requirements on DPIA and consulting the relevant data protection authorities on the necessity of DPIA before the processing of large scale and\or sensitive personal data and the deployment of the toolkit. In these cases, if the developer or operator decides not to carry out a DPIA, the reasons should be documented. For instance: the data protection authority did not require the DPIA after the consultation, or no personal data (only statistics) was processed.

5.5. RECOMMENDATIONS, CERTIFICATIONS AND DATA SECURITY STANDARDS

There are several international standards and good practices on data security applicable across all the energy subsectors. In this section, we highlight and introduce the most relevant standards. An Information Security Management System (ISMS) is a framework of policies and procedures that include all legal, physical and technical controls involved in an organization's information risk management processes. From the GDPR's point of view, there is no legal obligation for the data controllers to implement a specific ISMS and obtain certification. However, the GDPR encourages the application of certifications by stating the following:

The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account (GDPR Article 42 (1) [GDP16]

'Certification' means the assessment and impartial, third-party attestation that the fulfilment of certification criteria has been demonstrated. 'Certification body' is a third-party conformity assessment body [ISO17] operating certification mechanisms. Third-party conformity assessment activity is performed by an organization that is independent of the person or organization that provides the object, and of user interests in that object.

The GDPR clarifies that the certification shall be voluntary and available via a process that is transparent [GDPR Article 42 (3)]. The controller or processor which submits its processing to the certification mechanism shall provide the certification body, or where applicable, the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the certification procedure [GDPR Article 42 (4)]. The Certification can be issued for a maximum of three years and may be renewed, under the same conditions, provided that the relevant requirements continue to be met. The certification might be also withdrawn by the certification body or by the competent supervisory authority, if the requirements for the certification are not or are no longer met [GDPR Article 42 (7)]. The advantage of the meaningful certification mechanisms is that they can enhance compliance with the GDPR, NIS Directive and transparency for data subjects and in business to business (B2B) relations. Data controllers and processors can benefit from an independent third-party certification for the purpose of demonstrating compliance of their processing operations. [EDP19].

Table 2. International standards and good practices applicable across the energy sector [ENI01]

STANDARDS	GOOD PRACTICES
ISO 27001 – Information technology — Security techniques — Information security management systems — Requirements. **ANSI/ISA, Series "ISA-62443: Security for industrial automation and control system."** **NIST Framework for Improving Critical Infrastructure Cybersecurity.**	• Detailed Measures – Cybersecurity for Industrial Control Systems – ANSSI (France). • Good Practice Guide Process Control and SCADA Security – CPNI. • AMI System Security Requirements updated – UCAIUG: AMI-SEC-ASAP. • BDEW whitepaper – Requirements for secure controls and telecommunications systems – Bundesverband der energie un Wasserwirtschaft. • Information security baseline requirements for process control, safety and support ICT systems – OLF. • Twenty Critical Controls for Effective Cyber Defence: Consensus Audit Guidelines. • Catalogue of Control Systems Security: Recommendations for Standards Developers – USA DHS. • 21 Steps to Improve Cyber Security of SCADA Networks – US DOE.

Table 3. International standards and good practices applicable across the electricity subsector [ENI01]

STANDARDS	GOOD PRACTICES
• **NIST SP800-82 Guide to Industrial Control Systems (ICS) Security.** • **ISO 27019 – Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy**	• Cybersecurity model electricity subsector cybersecurity capability maturity model (es-c2m2) – U.S. Department of Energy. • NISTR 7628 – Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-

utility industry. ● **NERC CIP Series "Critical Infrastructure Protection Cyber Security": CIP–002 to CIP-011.** ● **IEEE STANDARD 1402-2000 – IEEE Guide for Electric Power Substation Physical and Electronic Security.** ● **IEC 61850 – Power Utility Automation.**	Level Requirements. ● ENISA Appropriate security measures for Smart Grids – ENISA. ● Best practices for handling smart grid cyber security – California Energy Commission.

The European Union Agency for Cybersecurity (ENISA)

The ENISA is actively contributing to European cybersecurity policy, supporting Member States and EU stakeholders to support a response to large-scale cyber incidents that take place across borders in cases where two or more EU Member States have been affected. The ENISA provides recommendations on cybersecurity and independent advice [ENI02]. ENISA is a reference point for advice and expertise on cybersecurity for Union institutions, bodies, offices and agencies as well as for other relevant Union stakeholders. Furthermore, the new EU Cybersecurity Act [REG19] revamps and strengthens the ENISA and establishes an EU-wide cybersecurity certification framework for digital products, services and processes.

International Organization for Standardization (ISO)

The ISO is a non-governmental organization that aims to form a bridge between the public and private sectors and it is the largest standards organization in the world. ISO is a network of standards institutes from 164 countries with a central office in Geneva, Switzerland, that coordinates the system [ISO02].

ISO 27000 standard series specify requirements for the establishment, implementation, monitoring and review, maintenance and improvement of a management system for managing an organization's data security. The series can be categorized as follows:

a) ISO/IEC 27000 contains the fundamentals and vocabulary, providing an overview of the ISO 27000 series.
b) ISO/IEC 27001 contains normative requirements for the development and operation of an ISMS, providing a set of (customizable) security controls and mitigation of the risks associated with the information, which the organization seeks to protect.
c) The remaining standards (ISO/IEC 27002 to ISO/IEC 27007) contain guidance standards or guidelines, good practice and methodologies. For instance, the ISO/IEC 27002 incorporates a list of commonly accepted control objectives and best practice controls for achieving information security. Furthermore, it provides specific implementation advice and guidance on best practices in support of the security controls specified in ISO/IEC 27001.

The EU Commission Recommendation of 3.4.2019 on Cybersecurity in the Energy Sector

The EU Commission Recommendation of 3.4.2019 on Cybersecurity in the Energy Sector elucidates the main issues related to cybersecurity in the energy sector, namely real-time requirements, cascading effects and combination of legacy and technology, and discusses how to implement crucial cybersecurity measures in the energy sector. The Recommendation highlights the issue of cascading effects since electricity grids and gas pipelines are strongly interconnected across Europe and cyber-attacks creating an outage or disruption in the energy system might trigger far-reaching cascading effect into other parts of the system. Another important issue is that two different types of technologies co-exist in today's energy system: an older technology with a lifespan of 30 to 60 years, designed before cybersecurity considerations, and modern equipment, reflecting state-of-the-art digitalization and smart devices.

The Recommendation requires the Member States to ensure that the relevant stakeholders, notably energy network operators and technology suppliers to implement the relevant cybersecurity measures related to real-time protection and security in the energy sector. Some elements of the energy system need to work under "real-time", which means it needs to react to commands within a few milliseconds, which makes it difficult or even impossible to introduce cybersecurity measures due to a lack of time.

The Recommendation provides examples for the most important measures, what energy network operators need to do [EUR20]:

a) applying the most recent security standards.
b) implementing international standards on cybersecurity and adequate specific technical standards for secure real-time communication,
c) considering real-time constraints in the overall security concept for assets,
d) considering privately-owned networks for tele-protection schemes to ensure the quality of service level required for real-time constraints; when using public communication networks, operators should consider ensuring specific bandwidth allocation, latency requirements and communication security measures,
e) splitting the overall system into logical zones and within each zone, choose a secure communication protocol and introduce an appropriate authentication mechanism for machine-to-machine communication.

The document provides further recommendations concerning the most important security requirements, such as analyzing risks, monitoring and updating software. These essential security requirements have been discussed in the report and many of them addressed by the Toolkit, providing monitoring, analysis and real time protection.

5.6. NIS DIRECTIVE

5.6.1. GENERAL INFORMATION ABOUT THE NIS DIRECTIVE

The European Commission proposed the Directive on Security of Network and Information Systems [NIS16] as a part of the EU cybersecurity strategy. The Directive was adopted by the European Parliament on 6 July 2016 and entered into force in August 2016. Since it is an EU directive, EU Member States have started to adopt national legislation, that follows or 'transposes' the directive. EU directives give the Member States some level of flexibility to consider their own national circumstances, for example, to re-use existing organizational structures or to align with existing national legislation.

The NIS Directive contains the requirements for the security of crucial systems to enhance the protection against incidents that might disrupt these systems or data contributing to service.

The Directive has been developed at the same time as GDPR, but it goes beyond the security and protection of personal data. The Directive focuses on availability, authenticity and integrity as well as confidentiality [CET01]. The objective of the NIS Directive is to strengthen the protection of the services which EU citizens use during their daily lives from cyber-attacks. The providers of these services are the Operators of Essential Services (OES, including several Critical National Infrastructure operators) and Digital Service Providers (DSP). To reach these goals, the NIS Directive requires Member States to be appropriately equipped against cyber-attacks, e.g., via a Computer Security Incident Response Team (CSIRT) and have a competent national NIS authority.

Furthermore, the Directive requires setting up a cooperation group to facilitate cooperation among all the EU Member States [NIS Directive Article 11 (1)]. The NIS Cooperation Group's goal is to achieve a high common level of security of network and information systems in the EU. It supports and facilitates strategic cooperation and the exchange of information among EU Member States [NIS16]. The Member States also need computer security incident response teams (CSIRTs), in order to promote swift and effective operational cooperation on specific cybersecurity incidents and sharing information about risks [ENI03].

5.6.2. 2. SCOPE OF THE NIS DIRECTIVE

5.6.2.1. ORGANIZATIONS

The NIS Directive focuses on two types of organizations: Operators of Essential Services (OES) and Digital Service Providers (DSP).

Operators of Essential Services (OES) that operate services that are essential for the maintenance of critical societal and economic activities. This includes operators in the sectors of energy, transport, health, drinking water supply and distribution, banking, financial market infrastructure and digital infrastructure [NIS04].

<u>NIS Directive Article 5. (2)</u>

The criteria for the identification of the operators of essential services, as referred to in point (4) of Article 4, shall be as follows:

a) an entity provides a service which is essential for the maintenance of critical societal and/or economic activities;
b) the provision of that service depends on network and information systems; and
c) an incident would have significant disruptive effects on the provision of that service.

Digital Service Providers (DSP) that are an important resource for their users, among which we can find OESs. This includes cloud service providers, search engines, and marketplaces.

NIS Directive Article 5 (2)

(5) 'digital service' means a service within the meaning of point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council (1) which is of a type listed in Annex III;

(6) 'digital service provider' means any legal person that provides a digital service;

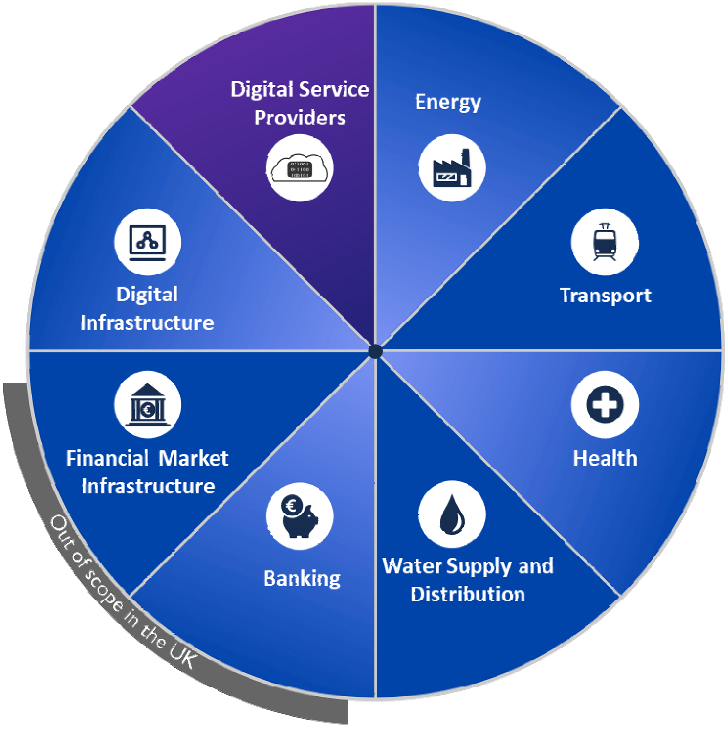

Digital Service Providers
Energy
Transport
Health
Water Supply and Distribution
Banking
Financial Market Infrastructure
Digital Infrastructure
Out of scope in the UK

Figure 6. Sectors in Scope of the NIS Directive [CET05]

Assets in Scope (Critical Infrastructure)

The scope of the NIS Directive covers 'network and information systems' that are used to provide a service. These systems can be networks, hardware, software that are essential to delivering a service, thus the scope of the directive goes far beyond data, protecting physical devices and their software.

NIS Directive Article 4 (1)

'network and information system' means:

a) *an electronic communications network within the meaning of point (a) of Article 2 of Directive 2002/21/EC;*
b) *any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or*
c) *digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance;*

It is crucial to identify critical infrastructure. However, in practice, not every organization knows exactly what it is important (critical) to deliver its service (and run the business) and it is not always easy to maintain an up-to-date asset inventory (if it exists), list all critical parts, their dependencies, and the necessary information to secure them. However, ENISA developed guidelines to help identifying critical infrastructure [ENI14].

5.6.2.2. INCIDENTS IN SCOPE

Incident means any event having an actual adverse effect on the security of network and information systems, while 'incident handling' refers to all the procedures supporting the detection, analysis and containment of an incident and the response to it [NIS Directive Article 4 (7) and (8)]. Any incident that causes a disruption fits into the definition, irrespective of the severity and size of the disruption.

5.6.2.3. OUT OF SCOPE

The NIS Directive only regulates network and information systems that are essential to provide a service, thus non-essential systems are out of scope. For instance, an email server that does not directly contribute to the service would be out of scope. Similarly, manual processes would fall out of scope. However, experts highlighted that it is important to consider a holistic approach during scoping since some systems might present a risk even though they are not essential. For instance, an Internet of Things (IoT) CCTV system might not be essential to provide a service. Yet, it may contain vulnerabilities that can give an entry-point to an attacker against essential systems.

5.6.3. SECURITY REQUIREMENTS AND INCIDENT NOTIFICATION

The NIS Directive requires the organizations to enact the following safety measures and protocols in the case of a data breach:

NIS Directive [NIS16] Article 14 (1) states that Member States shall ensure that operators of essential services take appropriate and proportionate technical and organizational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed.

'Appropriate and proportionate' are the two keywords in the NIS Directive, which is similar to the language of the GDPR. This requirement means that operators of essential services must demonstrate that their security measures are appropriate to the risks they might face. These security measures must also be proportionate to the potential risk. Therefore, while providing the appropriate level of protection, these measures should not result in serious damage to the business, finance, organization, or ability to operate. The meaning of ‘technical and organizational measures’ have been elucidated in this report, under the ‘data security’ section.

Furthermore, the NIS Directive requires operators to minimize the effects of incidents.

NIS Directive Article 14 (2)

Member States shall ensure that operators of essential services take appropriate measures to prevent and minimize the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services.

Incident notification

Both OESs and DSPs must notify their competent authority and/or the national CSIRT in the case of incidents that could disrupt their service.

NIS Directive Article 14 (3)

Member States shall ensure that operators of essential services notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide. Notifications shall include information enabling the competent authority or the CSIRT to determine any cross-border impact of the incident. Notification shall not make the notifying party subject to increased liability.

These incidents must be reported without undue delay, which gives OESs and DSPs the possibility to reemploy the same mechanisms as in [GDPR Article 13 (1)]. However, the NIS Directive does not specify any time-bound requirement for this notification, the time limit specified by the GDPR is 72 hours and some Member States have also defined the same limit for the NIS Directive. Thus, it is crucial that operators need to inform the data protection authority within 72 hours if a personal data breach has happened.

GDPR Article 33 *Notification of a personal data breach to the supervisory authority*

1.In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

For OESs, the competent authorities in the Member States establish these notification thresholds when an incident has a significant impact on the continuity of service. These thresholds can depend on any of the following parameters:

- - the number of users affected by the disruption of the essential service;
- - the duration of the incident;
- - the geographical spread with regard to the area affected by the incident.

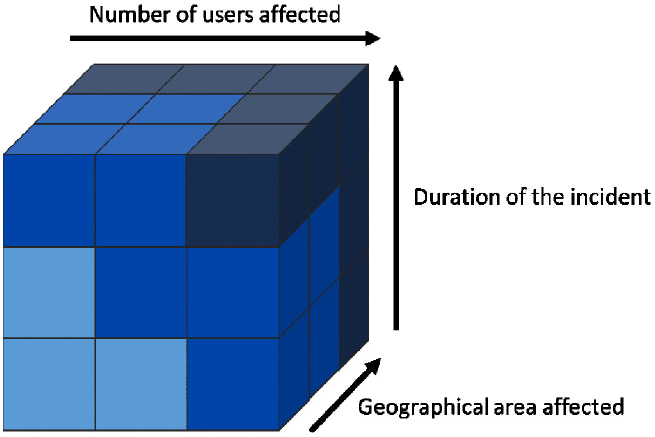


Figure 7. Incident notification parameter [CET02]

Most of the competent authorities in Member States define NIS incident thresholds using one or two parameters to keep them measurable.

5.6.4. DUTIES OF THE MEMBER STATES

The NIS Directive requires each Member State to adopt a national strategy on the security of network and information systems to achieve and maintain a high level of security of network and information systems. The Member States need to reach these goals by defining:

a) the objectives and priorities of the national strategy on the security of network and information systems;
b) a governance framework to achieve the objectives and priorities of the national strategy on the security of network and information systems, including roles and responsibilities of the government bodies and the other relevant actors;
c) the identification of measures relating to preparedness, response and recovery, including cooperation between the public and private sectors;
d) an indication of the education, awareness-raising and training programs relating to the national strategy on the security of network and information systems;
e) an indication of the research and development plans relating to the national strategy on the security of network and information systems;
f) a risk assessment plan to identify risks;
g) a list of the various actors involved in the implementation of the national strategy on the security of network and information systems [NIS Directive Article 7].

6. RISK MANAGEMENT

Cybersecurity risk assessment represents the process of identifying, analyzing, and evaluating risks. Based on this analysis cybersecurity controls are selected and sized.

As defined in NIS Directive [NIS16] risk means any reasonably identifiable circumstance or event having a potentially adverse effect on the security of network and information systems, while a risk assessment plan identified the risks.

Considering the implementation status of the EnergyShield project, i.e., requirements analysis and architecture design a list of cybersecurity events relevant for EPES has been identified. Furthermore, cost-based risk assessment is run to foresee the financial impact of the risks by assigning a monetary value to the impact.

6.1. RISK IDENTIFICATION

Three types of risks have been identified and assessed: operational, cybersecurity and 3rd party risks.

A culture of risk management, involving risk assessment and the implementation of security measures appropriate to the risks faced is promoted via the NIS Directive [NIS16] and aims at establishing effective cooperation between all EU member states via CRIST networks.

6.1.1. OPERATIONAL RISKS

Operational risks refer to prudential regulation and supervision and cover security, integrity and resilience of network and information systems. The security of network and information systems comprises the security of stored, transmitted and processed data [NIS16].

Exposure to operational risks may have an impact on business continuity and infrastructure:

- **Demand response/flexibility failure.** Fake alerts could be triggered or real alerts disable if ransomware manages to encrypt backups or backups are compromised.
- **Infrastructure breach through social engineering.** If it leads to a specialized malware being installed and/or other infrastructure mishandled (measurements, equipments).

Within organizations insider threats represent a major form of cybersecurity breaches. The users together with ex-staff represent a vulnerability point. Awareness and training on cybersecurity for employees is of major importance when trying to limit data breaches like:

- **GDPR violations resulting in fine or censure.**
- **Internal leak of documents.** For infrastructure and network data, supplier data, pricing etc.
- **Internal mistake leaking customer data.**

- **Internal malicious leaking customer data.**
- **Account deprovisioning.** E.g., ex-employee account is still active.

6.1.2. CYBERSECURITY RISKS

With cybersecurity risks the organizations are facing potential loss or harm of technical infrastructure alongside with reputation damage. Reliance on computers and global connectivity via cloud services call for sophisticated cybersecurity professional and software.

Grid infrastructure undergoes a continuous process of transformation towards a smarter interconnected topology. An important part of this process is represented by updating the legacy systems by using new generation equipment (sensors, meters, actuators, protections, etc.). These devices use a large amount of data and exchange information via specific communication protocols becoming vulnerable during exploitation. Examples of risks include energy disruptions, injecting and hacking of smart grid devices (IoT connected devices) [DEN17].

Moreover, utilities are exposing over the Internet services not only to industrial customers but also to residential untrained individuals. Encryption and authentication process must be stringent to avoid or at least limit customer account being hacked as a result of a weak password or other vulnerabilities. Multifactor authentication can be considered in strengthening the security procedures.

DDoS attacks have increased in magnitude as more and more devices come online through the Internet of Things (IoT). IoT devices often use default passwords and do not have sound security postures, making them vulnerable to compromise and exploitation [CIS19]. DDoS allows for exponentially more requests to be sent to the target, therefore increasing the attack power. It also increases the difficulty of attribution, as the true source of the attack is harder to identify.

Software infrastructure needs constant and careful monitoring and updating. If any vulnerabilities identified these should be expediently addressed to avoid system compromise.

6.1.3. PARTNERS RISK

When assessing the risks associated with energy sector IT applications the entire EPES value chain (generator, TSO, DSO, consumer) needs to be considered. A breach in this chain may have cascading effects on all involved actors.

6.2. RISK ASSESSMENT

Based on a risk cost modelling developed by Hubbard Decision Research (HDR) [HDR19] EnergyShield partners have investigated a number of potentially applicable security risks.

The table below illustrates the list of identified risks alongside with calculation of their minimum and maximum cost exposure based on impact and probability of occurrence.

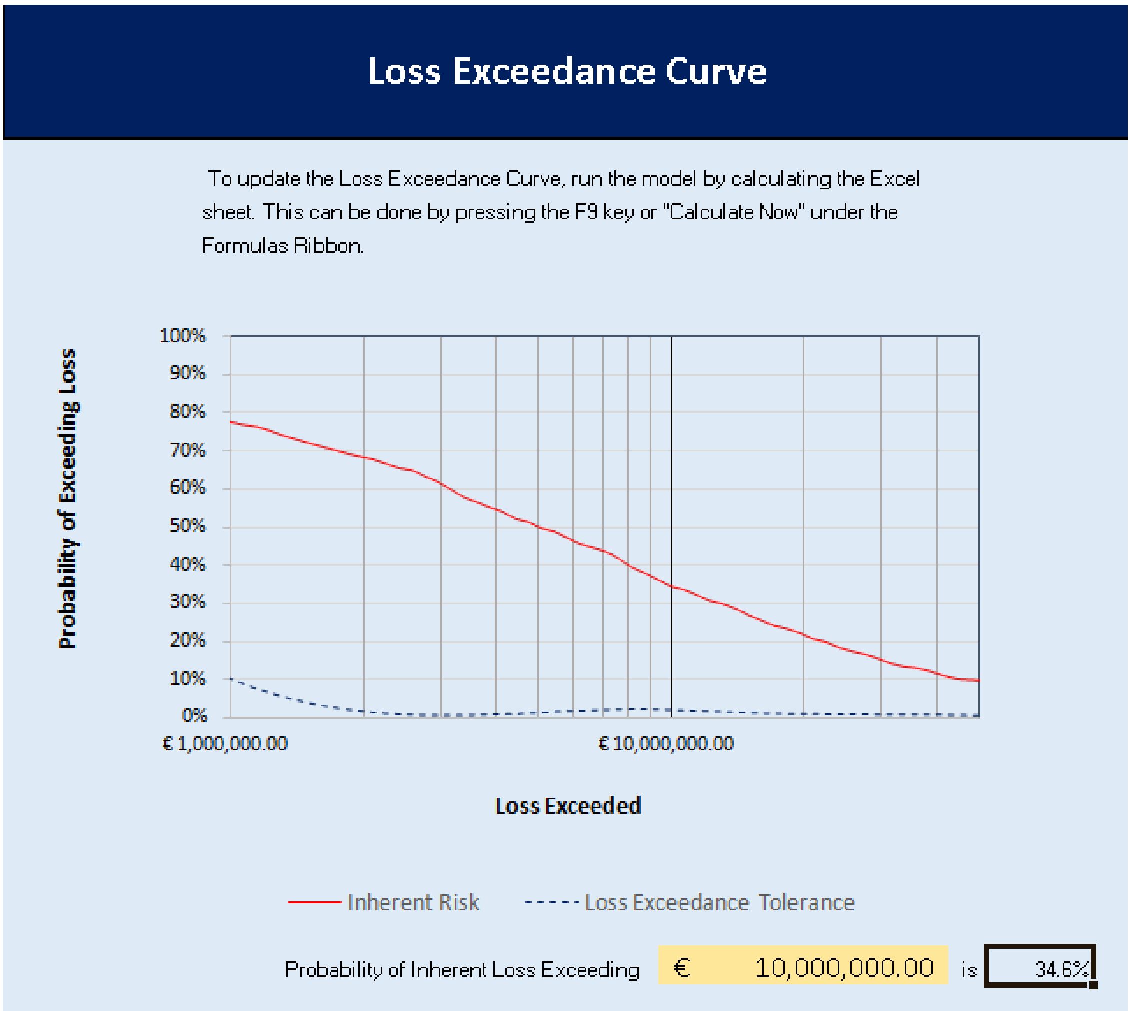
Table 4. Risk identification and cost exposure estimates

ID	Name	Classification	One year loss probability	90% Confidence Interval of Impact		Expected Inherent Loss
				Lower bound	Upper bound	
1	Demand response/flexibility failure	Operational	10%	€100K	€10.000K	€266.398
2	Energy not being provided due to infrastructure breach	Cyber security	25%	€100K	€50.000K	€3.329.372
3	Customer account hacked via vulnerabilities (WebUI)	Cyber security	5%	€10K	€100K	€2.020
4	Customer account hacked via weak customer password (WebUI)	Cyber security	20%	€5K	€50K	€4.040
5	DDoS attack public facing customer site	Cyber security	5%	€20K	€100K	€2.520
6	GDPR violations resulting in fine or censure	Operational	5%	€50K	€10.000K	€129.337
7	Internal leak of documents	Operational	10%	€20K	€1.000K	€28.681
8	3rd party breach - Supply chain breach	Partner	20%	€200K	€10.000K	€573.612
9	Internal mistake leaking customer data	Operational	5%	€10K	€1.000K	€13.320
10	Internal	Operational	2%	€20K	€10.000K	€53.270

	malicious leaking customer data					
11	Infrastructure breach through social engineering	Operational	30%	€40K	€50.000K	€4.445.654
12	Account deprovisioning	Operational	10%	€10K	€500K	€14.340
13	Partner breach cloud platform	Partner	1%	€10K	€100.000K	€503.641
14	Using End of Life systems -	Cyber security	50%	€100K	€50.000K	€6.658.744
15	No 24/7 event monitoring - can't see if a breach occurs	Cyber security	10%	€10K	€50.000K	€2.018.606
16	Not patching a critical vulnerability	Cyber security	40%	€100K	€50.000K	€5.326.995
17	Smart meter IoT hardware vulnerability	Cyber security	10%	€10K	€500K	€14.340

Table 4 represents a preliminary analysis of the EnergyShield associated with cybersecurity risks. When developing data privacy and security mechanisms for EnergyShield toolkit this assessment will be considered.

The figures below present the loss provisions.

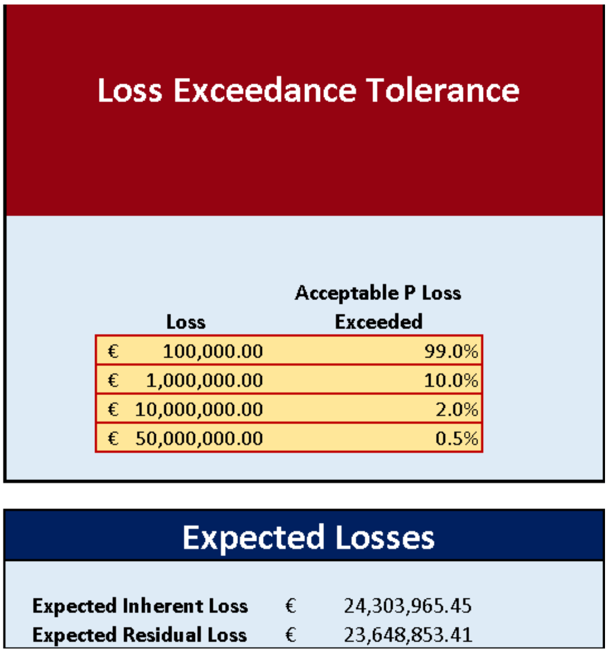


Loss Exceedance Curve

To update the Loss Exceedance Curve, run the model by calculating the Excel sheet. This can be done by pressing the F9 key or "Calculate Now" under the Formulas Ribbon.

Probability of Inherent Loss Exceeding € 10,000,000.00 is 34.6%

Figure 8. Loss exceeded curve



Loss Exceedance Tolerance

Loss	Acceptable P Loss Exceeded
€ 100,000.00	99.0%
€ 1,000,000.00	10.0%
€ 10,000,000.00	2.0%
€ 50,000,000.00	0.5%

Expected Losses

Expected Inherent Loss	€ 24,303,965.45
Expected Residual Loss	€ 23,648,853.41

Figure 9. Loss exceedance tolerance

7. CONCLUSION

This report examined the regulatory aspects applicable to the EnergyShield project specifically focusing on data protection, data transfers, data security and risk assessment.

Having identified key data protection and security legal issues, we recommended a series of technical implementations which should be embedded in the architecture design of the toolkit such as encryption (anonymization, pseudonymization and Homomorphic Encryption), data transfer restrictions outside of the EU/EAA and a number of data security measures.

Additionally, legal guidance for those potential users wishing to use EnergyShield toolkit with regard to GDPR and NIS Directive compliance was provided. These recommendations extend beyond the task lifecycle and aim at supporting the implementation of a level of privacy and security right from the design phase of the EnergyShield toolkit.

Expectations are that these recommendations alongside with the ones provided in the technical (T1.1) and commercial (T1.2) requirements that are being rolled out and edited in parallel will draft the EnergyShield requirements landscape and support development, integration and exploitation activities.

8. REFERENCES

[ACK19] Anamaria Costache, Kim Laine and Rachel Player, 'Homomorphic Noise Growth in Practice: Comparing BGV and FV, 2 <https://eprint.iacr.org/2019/493.pdf> accessed 5 November 2019.

[BHA18] Nirdosh Bhatnagar, Mathematical Principles of the Internet (CRC Press 2018), 203-204.

[CAS19] Casey Crane, 'What is Homomorphic Encryption?' (4 October 2019) <https://www.experfy.com/blog/what-is-homomorphic-encryption> accessed 5 November 2019

[CBD05] Claerhout B and DeMoor G.J.E (2005) Privacy Protection for Clinical and Genomic Data: The Use of Privacy Enhancing Techniques in Medicine. International Journal of Medical Informatics 74:257-265

[CES01] Cyber Essentials by the UK National Security Centre

https://www.cyberessentials.ncsc.gov.uk/

[CET01] Cetome, Introduction to the NIS Directive https://cetome.com/article/introduction-to-the-nis-directive

[CET02] Cetome – Scoping the NIS Directive https://cetome.com/article/scoping-the-nis-directive

[CET05] http://www.cetome.com/

[CIS19] CISA(2019) Security Tip (ST04-015) Understanding Denial-of-Service Attacks, https://www.us-cert.gov/ncas/tips/ST04-015

[CLA05] Claerhout B and DeMoor G.J.E (2005) Privacy Protection for Clinical and Genomic Data: The Use of Privacy Enhancing Techniques in Medicine. International Journal of Medical Informatics 74:257-265

[CNI18] The CNIL`s Guides (2018) Guidance on the Security of Personal Data p. 7, 10, 15

[DEN17] Deutsche Energie-Agentur GmbH (dena) and ESMT European School of Management and Technology GmbH (2017) Blockchain Vulnerabilities in smart meter infrastructure – can blockchain provide a solution? https://eventhorizonsummit.com/data/uploads/2019/04/Vulnerabilities_in_smart_meter_infrastructure_EventHorizon2017.pdf

[DIS19] https://www.datainspektionen.se/other-lang/in-english/the-general-data-protection-regulation-gdpr/transfer-of-data-to-a-third-country/

[DIV95] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. OJ 1995 No. L281, 23 November 1995, 31–50.

[DLA17] DLA Piper (2017) Example Data Protection Addendum Addressing Article 28 GDPR (Processor Terms) and Incorporating Standard Contractual Clauses for Controller to Processor Transfers of Personal

Data from the EEA to a Third Country

https://www.dlapiper.com/~/media/files/insights/publications/2017/08/example_data_protection_addendum.doc

[DPA01] Official Guideline on Data Processing Agreement https://gdpr.eu/what-is-data-processing-agreement/

[DPA02] Data Processing Agreement https://gdpr.eu/what-is-data-processing-agreement/

[DPI01] Data Protection Impact Assessment Template https://gdpr.eu/data-protection-impact-assessment-template/

[DLA17] DLA Piper (2017) Example Data Protection Addendum Addressing Article 28 GDPR (Processor Terms) and Incorporating Standard Contractual Clauses for Controller to Processor Transfers of Personal Data from the EEA to a Third Country

https://www.dlapiper.com/~/media/files/insights/publications/2017/08/example_data_protection_addendum.doc

[DPW17] A29 WP, Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, 17/EN WP 257, 29 November 2017

[DPW18] Article 29 Data Protection Working Party (2018) Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679

[DWP18] A29 WP, Working Document Setting Forth a Co-Operation Procedure for the approval of “Binding Corporate Rules” for controllers and processors under the GDPR, 17/EN WP263 rev.01, 11 April 2018

[DWW18] A29 WP, Guidelines on Article 49 of Regulation 2016/679, 18/EN WP261, 6 February 2018, p. 15.

[DPP18] A29 WP, Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, 17/EN WP264, 11 April 2018

[ECC19] European Commission, Standard contractual clauses for data transfers between EU and non-EU countries, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

[EDP19] European Data protection Supervision website https://edps.europa.eu/data-protection/data-protection/reference-library/international-transfers_en

[ENI01] ENISA (2017) Mapping of OES Security Requirements to Specific Sectors, p. 7 and 8.

[ENI02] ENISA Official Website and Information https://www.enisa.europa.eu/about-enisa

[ENI03] ENISA, CSIRTSs Network

https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network

[ENI14] ENISA (2014) `Methodologies for the identification of Critical Information Infrastructure assets and services  Guidelines for charting electronic data communication networks` December 2014

[EUC04] 2004/915/EC: Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries (notified under document number C(2004) 5271)Text with EEA relevance

[EUC19] Adequacy decision on Canada, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32002D0002 accessed on 02 October 2019

[EUP10] 2010/87/: Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593) (Text with EEA relevance)

[EUR19] European Commission: Adequacy decisions, How the EU determines if a non-EU country has an adequate level of data protection. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en accessed on 02 October 2019

[EUR20] The EU Commission Recommendation of 3.4.2019 on Cybersecurity in the Energy Sector, Brussels, 3.4.2019 C (2019) 2400 final p. 3.

[EUS19] Adequacy decision on the EU-US Privacy Shield, Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176) (Text with EEA relevance), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG accessed on 02 October 2019

[ESS19] European Commission (2019) EU-US data transfers, How personal data transferred between the EU and US is protected, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en

[GDP16] Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[GFB10] Gregory Neven, Frank Piessens and Bart De Decker, ‘On the Practical Feasibility of Secure Distributed Computing: A Case Study’ in Sihan Qing and Jan Eloff (eds) Information Security for Global Information

Infrastructures (Springer 2010), 366.

[HCI19] Preliminary ruling from the High Court (Ireland) made on 9 May 2018 – Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems (Case C-311/18) http://curia.europa.eu/juris/document/document.jsf?text=&docid=204046&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=6462885

[HDR19] Hubbard Decision Research (2019), https://hubbardresearch.com/

[IAP19] Article 29 Working Party guidelines, opinions, and documents, https://iapp.org/resources/article/all-of-the-article-29-working-party-guidelines-opinions-and-documents /

[ICO01] ICO, Security outcomes https://ico.org.uk/for-organisations/security-outcomes/

[ICO02] ICO Guidance on Encryption, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/encryption/

[ICO03] ICO (2018) Guidance on the use of cloud computing, https://ico.org.uk/media/for-organisations/documents/ 1540/cloud_computing_guidance_for_organisations.pdf

[ICO05] ICO Data protection by design and default, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/

[ICO06] ICO (2016) A practical guide to IT security – Ideal for the small business p. 13, https://ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf

[ICO07] ICO (2012) Bring your own device (BYOD) guidance, https://ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf

[ICO08] The ICO has released guidelines on the safe disposal of IT devices, https://ico.org.uk/media/for-organisations/documents/1570/it_asset_disposal_for_organisations.pdf

[ICO09] The ICO Guide on data security, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/

[ICO10] ICO – Guides to Data Protection Impact Assessments

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

[ICO19] Information Commissioner's Office, What is personal data? Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/

[ISO02] https://www.iso.org/about-us.html, https://the9000store.com/articles/who-is-iso/

[ISO17] ISO 17000, 2.5: “body that performs conformity assessment services“; ISO 17011: “body that performs conformity assessement services and that can be the object of accreditation”; ISO 17065, 3.12.

[JAN11] Jan Willemson (2011) Pseudonymization Service for X-Road eGovernment Data Exchange Layer, p. 143. In: Kim Andersen et al. (eds) Electronic Government and the Information Systems Perspective. Second International Conference, EGOVIS 2011. Toulusse, France, August/September 2011, Proceedings. Springer, Berlin

[JLI19] Jing Li and Licheng Wang, ‘Noiseless Fully Homomorphic Encryption’ <https://eprint.iacr.org/2017/839.pdf> accessed 29 November 2019.

[JUN16] Jun Sakuma, ‘Secure Outsourcing of Data Analysis’ in Fei Hu (ed) Big Data: Storage, Sharing and Security, (CRC Press 2016), 365.

[KAN17] Kannan Balasubramanian et al., ‘Homomorphic Encryption Schemes: A Survey’ in Kannan Balasubramanian and M Rajakani (eds) Algorithmic Strategies for Solving Complex Problems in Cryptography (IGI Global 2017), 98

[KER19] Kerina Jones, ‘Incongruities and Dilemmas in Data Donation: Juggling Our 1s and 0s’ in Jenny Krutzinna and Luciano Floridi (eds), The Ethics of Medical Data Donation, Philosophical Studies Series Vol. 137 (Springer 2019), 79.

[KUN17] Kuner, Christopher, Reality and Illusion in EU Data Transfer Regulation Post Schrems (July 7, 2017). 18 German Law Journal 881 (2017)

[MAK18] Maksó B. (2018) Binding Corporate Rules As a New Concept for Data Protection in Data Transfers. In: Bakhoum M., Conde Gallego B., Mackenrodt MO., Surblytė-Namavičienė G. (eds) Personal Data in Competition, Consumer Protection and Intellectual Property Law. MPI Studies on Intellectual Property and Competition Law, vol 28. Springer, Berlin, Heidelberg

[MER19] Merriam Webster Dictionary, https://www.merriam-webster.com/dictionary/register (22.01.2018); Oxford Dictionary https://en.oxforddictionaries.com/definition/register (22.01.2018).

[MNF15] McNealy & Flowers, 2015, p. 199, and Gjermundrød, Dionysiou & Costa, 2016, p. 4.

[NIS04] NIS Directive Annex II, https://eur-lex.europa.eu/legal-content/en/TXT/HTML/?uri=CELEX:32016L1148#d1e32-27-1

[NIS16] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[NOU07] Noumeir R, Lemay A, and Lina J-M (2007) Pseudonymization of Radiology Data for Research Purposes. Journal of Digital Imaging 20(3):284-295

[OP14] Opinion 05/2014 on anonymization by the Article 29 Working Party adopted on 10 April 2014,

[ORI18] Oriol T (2018) Internet Laws, p. 40. In: Ahmad K (ed) Social Computing and the Law: Uses and Abuses in Exceptional Circumstances. Cambridge University Press, Cambridge

[PER18] Brad Perry (2018) Pseudonymization, Anonymization and GDPR. Available at: https://medium.com/@brperry/pseudonymization-anonymization-gdpr-3dc8405dd465

[PSP19] Privacy Shield Program Overview, https://www.privacyshield.gov/welcome

[RAG13] Balaji Raghunathan, The Complete Book of Data Anonymization: From Planning to Implementation (CRC Press 2013).

[REG19] 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)

[SAN19] Sanjay Sharma, Data Privacy and GDPR Handbook (Wiley & Sons 2019), 103.

[SCH14] Maximillian Schrems v Data Protection Commissioner, CJEU, Judgment in Case C-362/14

[SHA17] Shakila Bu-Pasha (2017) Cross-border issues under EU data protection law with regards to personal data protection, Information & Communications Technology Law, 26:3, pp. 223-227

[SRI17] Srinivas Divya Papisetty, 'Homomorphic Encryption: Working and Analytical Assessment' MSc Thesis, 21 (2017) <http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1082551&dswid=-318> accessed 5 November 2019.

[TSL01] TSL protocol, https://www.ssllabs.com/ssltest/

[SVA16] Svantesson, 2013, 89 and Hijmans, 2016, 497.

[WAG18] Julian Wagner, The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?, International Data Privacy Law, Volume 8, Issue 4, November 2018, Pages 318–337, https://doi.org/10.1093/idpl/ipy008

9. ANNEX

9.1. SURVEY FOR TECHNOLOGY PARTNERS

I. Data Protection

If your component processes any kind of personal data (such as storing, transferring, deletion, access, etc.) please explain in simple terms how your component works (or will work) and how it relates to other relevant components within the architecture.

Please feel free to use graphics, charts, etc., if necessary. The more detailed information, the more it will help us to prepare the legal background. However, please try to make a concise explanation in about 3 to 5 pages (max).

II. Data Transfers outside of EU/EAA countries

The GDPR has special provisions on the transfer of personal data outside the EU/EAA .

1) Therefore, we are interested to know if your component (and toolkit in general) is transferring (or planning to transfer) data outside of the EU/EAA countries?

2) If yes, in which countries do you plan to send data?

3) What kind of data? For instance, is sensitive data (e.g., health data) also included?

Please explain in simple terms how your component works (or will work) and how it relates to other relevant components within the architecture.

Please feel free to use graphics, charts, etc., if necessary. The more detailed information, the more it will help us to prepare the legal background. However, please try to make a concise explanation in about 3 to 5 pages (max).

III) Data Security

What kind of technical and organizational measures do you apply to protect data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access?

For instance, do you:

1) use pseudonymization/anonymization and encryption?

2) have emergency backups?

3) protect the premises against unauthorized access (safe and secure locks, cameras)?

4) control the disposal of IT equipment?

5) have policies and rules in the case of `Bring-your-own-Device` (BYOD)?

6) have other security measures?

Please explain in simple terms how your component works (or will work) and how it relates to other relevant components within the architecture.

Please feel free to use graphics, charts, etc., if necessary. The more detailed information, the more it will help us to prepare the legal background. However, please try to make a concise explanation in about 3 to 5 pages (max).

IV) If your component is using any kind of risk assessment the about processing of data or personal data.

1) What kind of risk assessment standards and guidelines are you using? (e.g., ISO standards, OCTAVE, ENISA Guidelines, etc.)

2) What kind of risk assessment methodology are you using? Please explain in simple terms, using graphics, etc.

3) During what part of the service lifecycle does your risk assessment work? (e.g., service deployment, service operation phase, etc.).

4) Are you planning to include a Privacy Impact Risk Assessment? If so, how would it work?

5) Explain the process of identifying the threats in each scenario. What kind of risk model are you using?

6) What are the risk assessment techniques and who are the typical actors involved?

7) Is there any kind of risk inventory?

8) We also need to identify the following (if applicable): a) use cases b) level of interactions c) assets d) incidents/risk scenarios e) triggering factors.

9) Different stages of the risk assessment (risk can occur at any time, please explain if your methodological process includes different stages of risk assessment).

10) Do you use a qualitative or a quantitative risk assessment? (or both?) Please explain the process.

11) Do you have a particular risk “use case” scenario that we could use as an example?

Please explain in simple terms how your component works (or will work) and how it relates to other relevant components within the architecture.

Please feel free to use graphics, charts, etc., if necessary. The more detailed information, the more it will help us to prepare the legal background. However, please try to make a concise explanation in about 3 to 5 pages (max).

DEVELOPING THE CYBER-TOOLKIT THAT

PROTECTS YOUR ENERGY GRID

www.energy-shield.eu