D1.5

Final SELP report

DOCUMENT	D1.5	**WORKPACKAGE**	WP1
DELIVERABLE STATE	FINAL	**PROGRAMME IDENTIFIER**	H2020-SU-DS-2020
REVISION	V1.0	**GRANT AGREEMENT ID**	101020560
DELIVERY DATE	30/09/2024	**PROJECT START DATE**	01/10/2021
DISSEMINATION LEVEL	PU	**DURATION**	3 YEARS

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 101020560

DISCLAIMER

ACKNOWLEDGEMENT

This document is a deliverable of CyberSEAS project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 101020560.

The opinions expressed in this document reflect only the author's view and in no way reflect the European Commission's opinions. The European Commission is not responsible for any use that may be made of the information it contains.

PROJECT ACRONYM	CyberSEAS
PROJECT TITLE	Cyber Securing Energy dAta Services
CALL ID	H2020-SU-DS-2020
CALL NAME	Digital Security (H2020-SU-DS-2018-2019-2020)
TOPIC	SU-DS04-2018-2020 Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks and data breaches
TYPE OF ACTION	Innovation Action
COORDINATOR	ENGINEERING – INGEGNERIA INFORMATICA SPA (ENG)
PRINCIPAL CONTRACTORS	CONSORZIO INTERUNIVERSITARIO NAZIONALE PER L'INFORMATICA (CINI), AIRBUS CYBERSECURITY GMBH (ACS), FRAUNHOFER GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V. (FRAUNHOFER), GUARDTIME OU (GT), IKERLAN S. COOP (IKE), INFORMATIKA INFORMACIJSKE STORITVE IN INZENIRING DD (INF), INSTITUT ZA KORPORATIVNE VARNOSTNE STUDIJE LJUBLJANA (ICS), RHEINISCH-WESTFAELISCHE TECHNISCHE HOCHSCHULE AACHEN (RWTH), SOFTWARE IMAGINATION & VISION SRL (SIMAVI), SOFTWARE QUALITY SYSTEMS SA (SQS), STAM SRL (STAM), SYNELIXIS LYSEIS PLIROFORIKIS AUTOMATISMOU & TILEPIKOINONION ANONIMI ETAIRIA (SYN), WINGS ICT SOLUTIONS INFORMATION & COMMUNICATION TECHNOLOGIES IKE (WIN), ZIV APLICACIONES Y TECNOLOGIA SL (ZIV), COMUNE DI BERCHIDDA (BER), COMUNE DI BENETUTTI (BEN), ELES DOO SISTEMSKI OPERATER PRENOSNEGA ELEKTROENERGETSKEGA OMREZJA (ELES), PETROL SLOVENSKA ENERGETSKA DRUZBA DD LJUBLJANA (PET), AKADEMSKA RAZISKOVALNA MREZA SLOVENIJE (ARN), HRVATSKI OPERATOR PRIJENOSNOG SUSTAVA DOO (HOPS), ENERIM OY (ENERIM), ELEKTRILEVI OU (ELV), COMPANIA NATIONALA DE TRANSPORT ALENERGIEI ELECTRICE TRANSELECTRICA SA (TEL), CENTRUL ROMAN AL ENERGIEI (CRE), TIMELEX (TLX).
WORKPACKAGE	WP1
DELIVERABLE TYPE	REPORT
DISSEMINATION LEVEL	Public
DELIVERABLE STATE	Final
CONTRACTUAL DATE OF DELIVERY	30/09/2024
ACTUAL DATE OF DELIVERY	30/09/2024
DOCUMENT TITLE	Final SELP report
AUTHOR(S)	Hans Graux, Pedro Demolder, Geert Somers (TLX)

,REVIEWER(S)	CRE, GT
ABSTRACT	SEE EXECUTIVE SUMMARY
HISTORY	SEE DOCUMENT HISTORY
KEYWORDS	Security, Ethical, Legal, Privacy

Document History

Version	Date	Contributor(s)	Description
V0.1	31/01/2024	TLX	First outline and structure – scoping and analysis;– legal framework; scoping the SELP work
V0.5	31/05/2024	TLX	Initial updates on lessons learned – outline of the Manual on SELP compliance in EPES projects
V0.6	31/08/2024	TLX	Updates on legal frameworks - updates of piloting information
V0.8	23/09/2024	TLX	Finalisation of the draft deliverable
V0.9	30/09/2024	TLX	Incorporated internal review comments
V1.0	30/09/2024	TLX	Finalisation after review

Table of Contents

List of Figures

List of Acronyms and Abbreviations

CER	Critical Entities Resilience
CIP	Critical Infrastructure Protection
DGA	Data Governance Act
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSO	Distribution System Operators
ECDS	Energy Common Data Space
ECI	European Critical Infrastructures
EPCIP	European Programme for Critical Infrastructure Protection
EPES	Electrical Power and Energy System
IEC	Internal Ethical Committee
IED	Intelligent Electronic Device
IM	Information Management
GDPR	General Data Protection Regulation
NIS	Network and Information Security
OSP	Operator Security Plan
PES	Power and Energy System
PRMP	Privacy Risk Mitigation Plan
SELP	Security, Ethical, Legal and Privacy
SoA	State of the Art
TSO	Transmission System Operators
WP	Work Package

Executive Summary

One of the topics being addressed in Work Package 1 (Project Management) is the management of legal and ethical compliance issues. More specifically, Task 1.3 aims to support the coordination of SELP management (Security, Ethical, Legal and Privacy) in CyberSEAS.

To support SELP management in CyberSEAS, an initial deliverable (D1.4 - Interim SELP report) was delivered in the first year of the project, providing a consolidated view of the SELP activities and issues to be addressed in the project, along with the methodology to implement and monitor these issues.

As outlined in D1.4, these issues focused on:

- Data protection and privacy requirements, as addressed also in more operational detail in other tasks and deliverables;
- Security requirements, which are not only driven by data protection, but can also be linked to existing and emerging cybersecurity legislation, network and information security legislation and critical infrastructure protection (CIP) laws;
- The emerging data governance legislation at the EU level, notable the emerging notion of a single European Energy Data Space, as well as the impacts of the European Energy Package and its provisions related to the sharing of energy data;
- And finally, the ethical requirements, which are detailed in other deliverables.

Task 1.3 ran throughout the CyberSEAS project, and the deliverable was continuously refined and updated to reflect both the progress of piloting activities, and evolutions of the legal framework.

These evolutions have been significant, as had been largely expected. Most notably, since the submission of D1.4, over a period of barely 24 months, the EU has adopted the NIS 2 Directive, the CER Directive, the AI Act, the first network code on cybersecurity for the electricity sector, and the EUCC cybersecurity certification scheme, to name but the most significant ones. The legal framework has thus been a continuously and fast moving target. While these new frameworks only rarely and indirectly affected piloting activities directly, it was nonetheless important to analyse them, and identify current impacts on CyberSEAS products and services, either now or in the future.

The present final SELP report has a 'best practice' goal, and aims to share the difficulties and solutions linked to SELP that have been encountered during the lifetime of CyberSEAS. As such, it provides a summary of the requirements that includes these new frameworks, reports on their implementation in the project, and describes the principal lessons learned.

The report includes in its Annex a high-level SELP manual for EPES projects, that can be used to deploy CyberSEAS solutions in a secure and legally compliant manner even after the project's duration, and that can also be used as a tool to guide EPES deployments even outside the context of CyberSEAS projects and services. In this manner, CyberSEAS aims to provide a significant contribution to increased cyber resilience in European EPES, also from a SELP perspective.

1 Introduction

1.1 Goals of this document

The present document summarises the final of play of the CyberSEAS project's Security, Ethics, Legal and Privacy (SELP) activities, as specified in the Grant Agreement - Ref. 2. The creation and implementation of a SELP framework in EU funded projects is generally done to support the implementation and application of Responsible Innovation (RI).

The goal is not merely to list relevant requirements on the basis of existing laws and policies, but also to identify how these requirements have been formalized and monitored in practice. In that way, compliance has been continuously evaluated, and CyberSEAS has ensured that there is transparency on the checks that have been applied.

The starting point of the CyberSEAS SELP Framework is the **protection of freedoms and fundamental rights of the participants, and compliance with the principle of responsible innovation**, as required for all EU funded research projects. The objective of the SELP Framework in CyberSEAS is to ensure that the innovation brought about by the project is in line with European legal, ethics and moral values.

With respect to ethics and societal values, this is done by applying the theory of Value Sensitive Design, an approach which aims to integrate a wide range of human and moral values into the design of (information) technology. The present deliverable examines the legal framework, including specifically its impacts on security and data governance; and provides an updated of the ethics and societal values that had been previously integrated into D3.2 - CyberSEAS technical requirements.

1.2 Scope and methodological approach of the SELP compliance work in CyberSEAS

This deliverable provides a high level but thorough coverage of the main legal frameworks in relation to the CyberSEAS project, in a way that addresses data protection, privacy and security comprehensively.

Taking into account the objectives, scope and priorities of CyberSEAS and its application in its use cases, six legal areas are examined in detail in this deliverable:

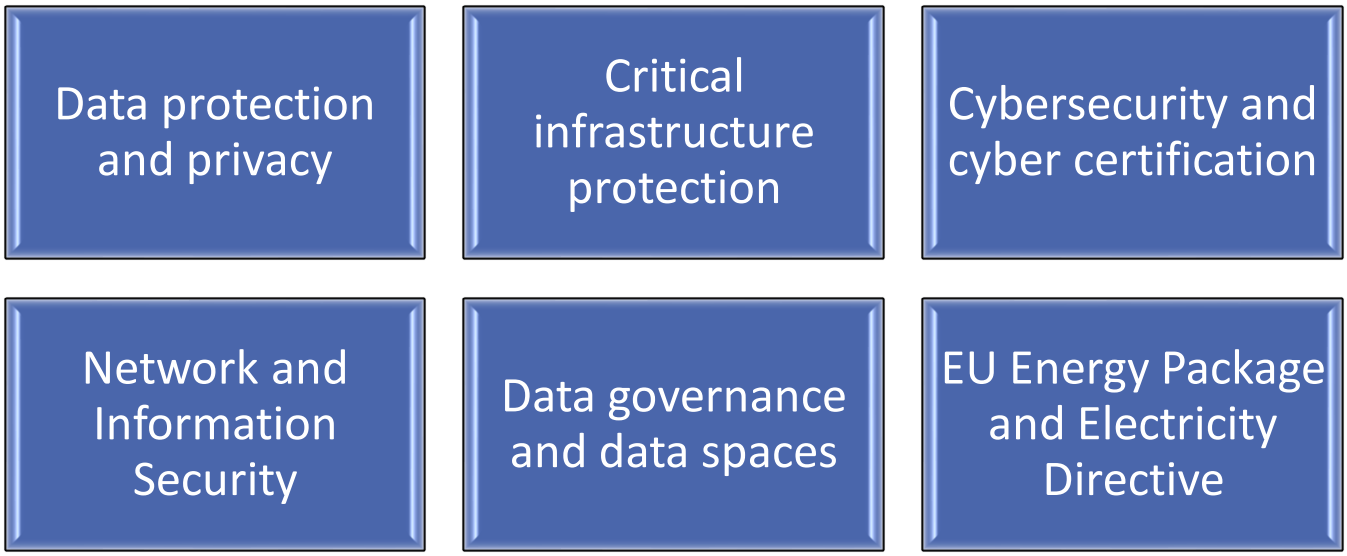

Figure 1: Priority legal topics for examination

More specifically:

- **Privacy and data protection** is arguably the key requirement for the CyberSEAS infrastructure, given that both privacy and data protection are recognized as fundamental rights under EU law. The application and impact of data protection law is linked to the notion of personal data, i.e. data that can be linked directly or indirectly to an identifiable natural person. The protection of EPES infrastructure doesn't have an impact on privacy and data protection by definition; this depends on the scoping of piloting activities. None the less, given the critical importance of these topics, data protection law – and specifically compliance with the General Data Protection

Regulation (GDPR - Ref. 1) is crucial to ensure legal compliance and long term value of the project results. The platform and its use cases thus needed to be designed with privacy and data protection in mind, in accordance with the **privacy by design and privacy by default** principles of European data protection law.

- **Critical infrastructure protection** refers to the legal framework that aims to protect societally crucial assets, i.e. assets which are "*essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions*", as defined in the applicable legal framework – principally the Critical Infrastructure Protection (CIP) Directive (Ref. 11), and the Critical Entities Resilience (CER) Directive that was adopted in the course of the project (Ref. 12). For such assets, specific governance and security obligations are defined to ensure that they remain operational, and that any disruptions can be detected and addressed as a matter of priority. As will be examined in this deliverable, the legal framework is currently still undergoing revision to expand its scope and strengthen resilience.
- **Cybersecurity and cyber certification** refer to a vibrant and quickly evolving policy area in the EU, specifically created via the so-called Cybersecurity Act (Ref. 9). The Act aims to create a general framework for the verification and certification of certain products and services that aim to support cybersecurity resilience. Other topics addressed in the Act, which are less relevant to CyberSEAS, include the extension of the European Network and Information Security Agency (ENISA), and the expansion of national level cyber security governance and cooperation mechanisms.
- **Network and Information Security** relates to the EU level definition of a minimum level of security of network and information systems, particularly for certain designated "essential services". In the EU, this topic was regulated by the Network and Information Security (NIS) Directive (Ref. 8), which defines 'security of network and information systems' as "*the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems*". The Directive defines an '**operator of essential services'** as "*a public or private entity of a type referred to in Annex II, which meets the criteria laid down in Article 5(2)*". Crucially for CyberSEAS, the energy sector, namely electricity, gas, and oil, are covered under

Annex II, implying both governance and notification duties for this sector. During the course of the CyberSEAS project, the NIS 2 Directive was adopted, which expanded the scope and the operational obligations of regulated operators compared to its predecessor. Member States are required to transpose the NIS 2 Directive into national law by 18 October 2024; and as such, assessment of its impacts was a critical priority of CyberSEAS.

- **Data governance and data spaces** relates to a relatively recent policy domain, that aims to establish sector specific, specialized 'data spaces' – i.e. data infrastructures that are tailored to the needs of a specific industry, and that would allow members of that industry to more easily select appropriate infrastructure from provides established anywhere in the EU (Ref. 7). Data spaces are regulated either generally (via the recently adopted Data Governance Act - Ref. 6), or via complementary industry specific legislation (such as via the recently adopted Health Data Spaces Regulation). The energy sector is still expected to be the subject of its own specialized data space, now referenced as the Common European Energy Data Space; and the CyberSEAS project thus also monitored whether and to what extent legal requirements would be created as well to further ensure legal interoperability.
- Finally, the **EU Energy Package (and particularly the Electricity Directive - Ref. 13)** harmonize the functioning of specific segments of the energy market across the EU, creating an equal playing field across all Member States, and establishing duly mandated national regulators/supervisors. The legal framework defines high level security and governance requirements for the industry as a whole, and (in the case of the Electricity Directive) also sets out rules, requirements and an infrastructural model for sharing access to household level electricity data. This legal framework may therefor also prove to be relevant for CyberSEAS.

While not necessarily all-encompassing, a thorough insight in the scope, requirements and implications of these frameworks is required for the creation of a SELP framework in CyberSEAS. Therefore, the principal EU level legal frameworks for all six of these topics will be briefly described and assessed below, in chapter 2. Each section of this chapter will:

- Briefly **describe the relevant legislation** and its main features (including any particularly relevant emerging or proposed legislation).

- Describe the **impacts and lessons learned** of the legal frameworks on the CyberSEAS project, at the infrastructural level or for specific use cases.

Next, an overview will be provided of (non-legal) **ethical considerations** in the project, in chapter 3, focusing on fundamental rights protections and impacts in the project.

Finally, in chapter 4 we will summarise the **main lessons learned**, and provide guidance for future use of CyberSEAS products and services, as well as general recommendations for the legal compliance assessment of EPES projects via the **SELP Manual for EPES Projects**, which is included in Annex I of this deliverable.

1.3 Final status of this deliverable – summarising best practices and lessons learned and a Table of Changes

1.3.1 Final status

As required by the Grant Agreement, the first version of this deliverable contained a first iteration of the analysis of the legal framework. A more thorough analysis, including evolutions of the legal framework, a report on compliance measures and analysis of any lessons learned, is included in this second and final iteration.

1.3.2 Table of Changes

This document was developed iteratively, starting from the first version (D1.4 – Interim SELP Report) and was continuously adapted throughout the project's duration. This was particularly necessary due to the anticipated high likelihood of evolutions in the legal framework during the project, which has indeed materialised, and had to be duly monitored, evaluated, and where necessary implemented, in order to ensure that the CyberSEAS products and services remain fit for use for the EU energy market.

The table below summarises the principal changes between D1.4 (Interim SELP Report) and the current D1.5 (Final SELP Report):

Section of the Deliverable	Updates in D1.5 compared to D1.4
1. Introduction	Principally updates to the actions undertaken in section 1.3
2. Description of the legal framework	Significant expansions of the sections on data protection (2.1, describing pilot details and decisions); Security (2.3, describing the impacts of NIS2); Cybersecurity (2.4, describing the EUCC scheme in the context of the Cyber Security Act); Critical Infrastructure (2.5, describing the new CER Directive); and the Energy Package (2.6, describing the new Network Code)
3. Ethical requirements	No substantive changes.
4. Best practices and lessons learned	New section, summarising the framework, describing implementation actions, and the SELP Manual for EPES projects
Annexes	Annex I contains the SELP Manual for EPES Projects and is entirely new. Annex II contains a DPIA template, which is a generalised version of the template that was initially created in D2.6 (Privacy Risk Mitigation Plan v2)

Figure 2: Table of changes

1.4 Relation to other activities

As the summary above already signalled, this deliverable (and Task 1.3 in general) is a part of a broader workstream in CyberSEAS, focusing on ethics, compliance, risk identification and risk management. It is intended to steer future CyberSEAS development and testing, including in the context of piloting.

For that reason, this deliverable is complementary to multiple other tasks and deliverables, notably integrating **inputs** from:

- **Task 2.5 – Data Protection Impact Assessment**, which aims to identify privacy and data protection risks to individual persons that are created by CyberSEAS activities. Having assessed the impacts of these risks, measures must then be implemented to mitigate them, and compliance should be monitored continuously via a Privacy Risk Mitigation

Plan. The analysis of Task 1.3 and Task 2.5 was done in parallel, with the current deliverable focusing more on the conceptual requirements of European data protection law, and the D2.5 and D2.6 focusing more on the implementation and application of those requirements in practice (via data protection impact assessments as required by the GDPR, and via the creation and application of a privacy risk management plan).

- **Work Package 8 (Fostering the culture of cyber-resilient Energy supply chain)** provides guidance on security and certification best practices and requirements in Europe, among other topics. These best practices and obligations are driven in part by the regulatory framework (NIS2, CER, and the Network Code, among other points). Alignment between the SELP work and Work Package 8 was needed to ensure that the outputs were based on, and in line with, EU regulatory requirements.
- **Work Package 10 (ethics)** provides guidance on how to implement certain data protection safeguards in CyberSEAS. Outputs include the appoint of a DPO, the creation of an incidental findings policy, guidance on anonymization /pseudonymization approaches, and procedures and criteria that will be used to identify/recruit research participants during piloting activities (including templates of informed consent forms and information sheet). Most of these elements can be linked to specific regulatory requirements emanating from European data protection law, notably the GDPR.

Figure 3: Links to other deliverables

2 Description and impacts of the legal framework

2.1 Data protection and privacy risks

2.1.1 Scope of the legal framework and general impacts

Both the right to privacy and to protection of personal data are fundamental rights, enshrined in the **EU Charter of Fundamental Rights (Ref. 17)**, respectively in Articles 7 and 8 of the Charter. The right to privacy generally relates to the right to respect for an individual's private and family life, home and communications. The right to protection of personal data relates to the right of any individual to have data relating to them processed (i.e. collected or used) in a fair and lawful manner. More specifically, the Charter requires that such data is only "*processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified*". The Charter furthermore requires that compliance with these rules is subject to control by an independent authority.

These generic descriptions are developed in greater detail in the **General Data Protection Regulation (GDPR - Ref. 1)**, which outlines the requirements for fair and lawful processing of personal data. The GDPR applies in principle to any processing (i.e. collection and any other use, including simple exchanges) of personal data, defined as any information relating to an identified or identifiable natural person (a 'data subject') (Article 4 (1) of the GDPR, and Ref. 4). An identified or identifiable natural person for the purposes of the GDPR is "*one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*".[1]

For the avoidance of doubt, the GDPR explicitly notes that it applies to the processing of personal data in the context of the activities in the Union, regardless of whether the processing takes place in the Union or not; and to the processing of personal data of data

[1] Article 29 Working Party (2007) "Opinion 4/2007 on the concept of personal data", *WP136*, 15-17.

subjects who are in the Union, even if the processing is done by an organization that is *not* established in the Union, if the processing activities are related to the offering of goods or services to such data subjects in the Union.

The personal data processing operation must be conducted under the responsibility of a data controller. A controller is "*the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data*" (Ref. 4). It is up to the data controller to ensure that the general principles for data processing, as outlined in Article 5 of the GDPR, are respected. These principles are as follows:

1. **Lawfulness, fairness and transparency**: a main requirement related to this principle is the that for the processing to be lawful, the data controller must be able to rely on one of the exhaustively listed processing grounds under Article 6 GDPR.[2]
2. **Purpose limitation**: personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. The GDPR clarifies, however, that further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should not be considered as incompatible with the initial purposes.
3. **Data minimization**: personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This principle means that no more data can be collected than necessary and that the data may not be stored longer than necessary.
4. **Accuracy**: personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
5. **Storage limitation**: personal data shall be kept in a form that permits identification of data subject for longer than is necessary for the purposes for which the data are processed. This principle requires the data controller to clearly state, in advance to the processing, for how long the personal data must be stored to achieve the purposes of the processing.
6. **Confidentiality and integrity**: personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against

[2] The 6 legal bases are: consent, performance of a contract, compliance with a legal obligation, protection of vital interests, carrying out a task in the public interest, legitimate interest (see Article 6 GDPR).

unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

7. **Accountability**: the data controller bears the responsibility for the processing, which includes the responsibility to demonstrate compliance with the abovementioned principles.

Another important principle, introduced in Article 25 of the GDPR, includes the obligation for the data controller to implement **data protection by design** and **data protection by default** in any new initiatives (sometimes also referred to as privacy by design and privacy by default), implying respectively that data protection compliance must be built into architectural designs at the earliest possible stage, and that any features that protect personal data must be activated by default. Furthermore, the controller must implement appropriate technical and organizational measures to ensure that only the necessary personal data are processed by default.

Beyond these principles, the GDPR contains numerous operational and procedural safeguards, including the supervision of data processing activities by an independent authority (a data protection authority, Article 51 and following), safeguards against the processing of special categories of personal data (such as data concerning health; Article 9) and against automated individual decision-making, including profiling (Article 22 of the GDPR), and rules and procedures on how to deal with incidents involving personal data (so-called personal data breaches, Article 33 and following). In addition, Article 35 GDPR requires the data controller to make a prior assessment of the impact of the envisaged processing operations on the protection of personal data (Data Protection Impact Assessment, DPIA - Ref. 3), particularly when using new technologies and when the processing – considering its nature, scope, context and purposes – is likely to result in a high risk to the rights and freedoms of natural persons.

Data subjects should also be able to exercise specific predefined rights, such as the right to information about the processing and the data controller, the right of access to copies of their personal data, the right to halt or limit data processing, and to have their data deleted by the current holder and by any parties to whom they have provided copies of the data (the so-called "right to be forgotten" or "right to erasure"). Data subjects also have the right to obtain a rectification of inaccurate data concerning them, to request the data controller to restrict the processing in certain cases, to receive their personal data in a machine-readable format ("right to data portability"), and in certain cases to object to the processing of their data. According to Article 23 of the GDPR, these rights can be restricted by law, when such a restriction respects the essence of fundamental rights and freedoms and is necessary

and proportionate to safeguard matters such as national and public security, defence, crime prevention, the public interest, etc.

The GDPR principally requires the processed personal data of EU citizens to remain within a place where sufficient guarantees are offered to safeguard the rights and freedoms of those citizens. Transfers outside of the EU, so-called transfers to third countries, are therefore only possible if the level of protection of natural persons guaranteed by the GDPR is not undermined.[3] One way to ensure such level of data protection is offered by adequacy decisions, according to article 45 GDPR. This allows the European Commission to decide that a third country ensures an adequate level of protection. Where no adequacy decision has been taken, transfers to a third country can still be allowed if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.[4] Such appropriate safeguards may be offered by means of a legally binding and enforceable instrument between public authorities or bodies, binding corporate rules, standard data protection clauses, an approved code of conduct, or an approved certification mechanism. In the case of CyberSEAS, all partner members are established in the EU and there are no planned transfers of data within the project, meaning that the requirements for data transfer will not be central to the project implementation.

2.1.2 Specific impacts and lessons learned

As is explained in much greater detail in the context of other deliverables – notably D2.5 and D2.6, respectively the first and second iteration of the Privacy Risk Mitigation Plan - the applicability of data protection law and the relevance of privacy concerns, to a project such as CyberSEAS is not readily apparent.

Essentially, CyberSEAS aims to raise the security of the modern-day grid, by protecting energy grid assets and the interaction and dependencies between assets. Inevitably, certain information assets (i.e. data) will be targeted for specific evaluation and protection by CyberSEAS. When those assets – or the interactions between those assets – involve the processing of personal data, privacy risks can emerge. In this case, the requirements of the GDPR apply.

[3] Article 44 GDPR.

[4] Article 46 GDPR.

In the context of the CyberSEAS project, privacy and data protection challenges can principally occur if and when personal data of a specific natural person – such as an energy user, their household, or the personnel of a utility or service company – is collected or processed in the context of CyberSEAS activities. If no personal data is involved, neither privacy nor data protection are likely to be impacted, and the legal requirements described above are irrelevant.

Compliance with the GDPR is required for all personal data processing operations within the CyberSEAS project as a whole, and specifically in the pilot demonstrations taking place in 6 infrastructures provided by CyberSEAS operators in 6 EU countries: Finland, Italy, Slovenia, Croatia, Estonia and Romania.

The above-mentioned activities will involve individuals both internal and external to the project. The GDPR will apply to the processing of any information 'related to' such individuals. This will be the case when the information is "about" that person i.e., there is a relationship between the information and an individual. In some cases, this is fairly straightforward, for instance in the case of a HR-file of a CyberSEAS employee or individualized data on energy infrastructure in a household. It can, however, also be less obvious, for instance where the characteristics of a house do not directly say anything about a person but do provide insight in the financial status of its owner.

The GDPR regulates measures that need to be taken 1) with a view to minimizing the risk of a data breach and 2) whenever a personal data breach occurs. These include the requirements under Article 35 for a prior assessment of the impact of the envisaged processing operations on the protection of personal data (DPIA) when the processing is likely to result in a high risk to the rights and freedoms of natural persons. In case the DPIA indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk, the controller should consult the national data protection supervisory authority prior to processing (Article 36 GDPR).

In case of successful attacks or other types of data breaches, the GDPR envisions specific measures aimed at managing and limiting the negative consequences for the data subjects, including:

- the processor should notify the controller without undue delay after becoming aware of a personal data breach.
- as soon as the controller becomes aware of a personal data breach, the controller should notify the supervisory authority no later than 72 hours after having become aware of it (unless the controller is able to demonstrate that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural person).

- when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller should communicate the personal data breach to the data subject without undue delay.

Since this is a complicated assessment that will have different results depending on the pilot use cases, CyberSEAS defined in the aforementioned deliverables D2.5 and D2.6 a Privacy Risk Mitigation Plan, including a comprehensive methodology for mapping data protection risks and mitigation measures, including the completion of a formal DPIA prior to initiating the pilot, and a requirement that piloting should always be done under the supervision of a duly qualified data protection officer (DPO) – i.e. under the guidance of a person that can independently evaluate data protection requirements, and advise on suitable mitigating measures.

The application of this approach in the pilots was often complicated, due to the need to assess the collected data on a case by case basis, in order to determine whether the GDPR applied. **In the majority of piloting activities**, testing either took place in controlled environments (including laboratory testing environments) using plausible but fake data; or relied on purely infrastructural data that could not reasonably be linked to natural persons. In other words, in the majority of cases, **data protection law did not apply**.

The **exception** to this assessment was the **Italian pilot**; which focused on the protection of electricity infrastructure around the communes of Berchidda and Benetutti, where piloting was conducted on-site (including real citizens, via their smart meters). The pilot has an infrastructural focus, targeting smart meters, but also electricity cabins, data storage units, management software, decision support systems, SCADA systems and disconnector modules.

It thus targets PES Components and IM Components, which, while not targeted specifically towards personal data, incidentally includes the processing of personal data, given that 5G enabled smart metering equipment is within the scope of the protectable infrastructure. Moreover, the pilot involved prosumer profiles (via solar panels at the household level), thus requiring household level data collection that also had to be analysed to determine security threats. Such smaller scale (household / block level) equipment contains unique identifiers that are potentially linkable to individual persons, implying that data protection challenges could occur. Specifically, the pilot included attack scenarios that comprised a DDoS attack (limited personal data processing), a smart meter attack to tamper and modify configuration files of smart meters and extract energy data (some personal data processing); and a customer phishing attack in order to steal private credentials (significant personal data processing).

The challenge was mitigated by a rigid application of the **data minimisation** principle, by relying on data for only a small sample of customers to conduct experiments on user consumption data, to test the preparedness of employees, and to conduct penetration tests. Where possible, piloting occurred on aggregate data only, i.e. by compiling data on a sufficiently large group of consumers in order to obfuscate the behavior of any individual household, thus making the data unlinkable to any individual. While the creation of aggregate data is also a form of processing of personal data, this allowed data protection risks to be significantly recued.

With respect to the **legal basis** of the data processing activities, the pilot could build on Article 6.1 (b) and 6.1 (f) of the GDPR, specifically:

- The **necessity of processing for the performance of a contract** to which the data subject is a party (specifically the energy service contract with the customer). In other words, the processing of a customer's personal data to detect security problems and to proactively action them is considered an integral part of the contractual obligations of the data controller. This argumentation could be reasonably contested in case of invasive detection mechanisms, especially when these may result in harm to the customer; but in the case of the CyberSEAS projects, the data processing activities were not invasive from a data protection perspective and could not have reasonably resulted in any detriment to the data subjects. For this reason, an appeal to article 6.1 (b) of the GDPR (contractual necessity) is justified.
- As a complementary legal basis, the project could fall back on **the necessity of processing for the purposes of the legitimate interests pursued by the controller or by a third party**, specifically the interest of the controller (i.e. the electricity provider or grid operator, depending in the situation) in ensuring the safety and security of its electricity network, both for its own business interests (as a controller) and to protect other customers (as third parties). This interest overrides any interests or fundamental rights and freedoms of the data subject, given that the negative impact on the data subjects is negligible in practice, and that the benefit for other data subjects is obvious. This legal basis was also applied with respect to personal data of employees.

The **finding of lawfulness** is furthermore corroborated when considering the **broader legal framework** within which electricity operators must work within the EU. Both the electricity legal package (see section 2.6) and the European security legislation (see section 2.3) include stringent and increasingly demanding obligations to ensure that electricity infrastructure is appropriately protected against attacks and abuse. This implicitly requires the processing of

personal data in instances where this infrastructure is used by individuals and households. Thus, the legislation further supports the finding that there is a legal basis already in European law for the processing of personal data as undertaken by CyberSEAS.

This finding was particularly important to facilitate the smooth initiation of piloting without having to obtain specific additional formal consents from individuals, which would have been administratively demanding, but also problematic legally: consent must be freely given, which means that data subjects must of course have the full freedom not to consent. This would imply in practice that individual households could opt out of the protection of electricity infrastructure. This would be legally and operationally problematic, since grid security is not a purely personal concern that should be subject entirely to personal freedom. Based on the argumentation above, additional consents could be avoided.

With respect to **transparency,** it was principally necessary to ensure that existing data protection policies were sufficiently comprehensive to cover the piloting activities as well, which was found to be the case. Additional information was made available via the general CyberSEAS website.

In terms of **data transfers and data sharing,** no data sharing outside of the EU/EEA occurred, so that no separate data transfer agreements were required, nor was it necessary to conduct any data transfer impact assessments. The data processing activities were conducted locally within the data controller's infrastructure – while findings were shared with other partners, personal data was not, in accordance with the principles outlined in the CyberSEAS ethics deliverables mentioned above. As a result, no data processing agreements were required. This is again an application of the principles of **data minimization and data protection by design**.

2.2 Energy Common Data Space: Data Governance Act, and potential future initiatives

2.2.1 Scope of the legal framework and general impacts

The recently adopted **Data Governance Act (DGA - Ref. 9)** is a key pillar of the European strategy for data (Ref. 7), which seeks to increase trust in data sharing, strengthen

mechanisms to increase data availability and overcome technical obstacles to the reuse of data. Crucially for CyberSEAS, the Data Governance Act supports the set-up and development of common European data spaces in strategic domains, involving both private and public players, in sectors such as *energy*, health, environment, agriculture, mobility, finance, manufacturing, public administration and skills. The objective of such Common European data spaces is to make data findable, accessible, interoperable and re-usable (the 'FAIR data principles'), while ensuring a high level of cybersecurity. The Data Governance Act entered into force on 23 June 2022 and, following a 15-month grace period, will be applicable as from September 2023.

A first chapter of the Act focuses on personal data and non-personal data, including data which is protected by commercial confidentiality, statistical confidentiality, intellectual property rights and/or data protection requirements, and is held by public sector bodies (Article 3.1). Article 2(17) defines 'public sector body' as "*the State, regional or local authorities, bodies governed by public law or associations formed by one or more such authorities, or one or more such bodies governed by public law*". 'Bodies governed by public law' are bodies that have the following characteristics:

(a) they are established for the specific purpose of meeting needs in the general interest, and do not have an industrial or commercial character.
(b) they have legal personality.
(c) they are financed, for the most part, by the State, regional or local authorities, or other bodies governed by public law, are subject to management supervision by those authorities or bodies, or have an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional or local authorities, or by other bodies governed by public law.[5]

Given this scoping, certain stakeholders in the electricity market – but not purely private electricity companies - will fall within the scope of the Act, either because they are established by public law (such as public utilities and regulators), or because they meet the funding or control criterion of the Act. The latter can be particularly important in Member States where national governments retain a controlling stake in the ownership of energy producing companies.

The Data Governance Act aims to boost the development of trustworthy data-sharing systems through 4 broad sets of measures. First, it includes mechanisms to facilitate the reuse

[5] Article 2(18) Data Governance Act.

of certain public sector data that cannot be made available as open data. According to Article 5, competent public sector bodies set out the conditions and procedure for the re-use of protected public data. The conditions should ensure that the protected nature of the data is preserved (notably with respect to personal data protection, intellectual property rights and commercial confidentiality). The Data Governance Act does not create a right to re-use of such data, but rather provides a set of harmonized conditions under which the re-use may be allowed. Article 7 obliges Member State to designate competent bodies to assist the public sector bodies which grant or refuse access for the re-use of the categories of data referred to in Article 3(1). It is possible for such bodies to be competent only in particular sectors (including the energy sector).

The new regulation sets out a notification regime for "data intermediaries" – intermediation service providers that will function as trustworthy organizers of data sharing or pooling within the common European data spaces. These providers will have to comply with a number of requirements set out in Article 12, in particular the requirement to remain neutral as regards the data exchanged. They cannot use such data for other purposes but to put them at the disposal of data users. At the time of submission of this Final SELP Report, four such intermediaries exist in the EU (Ref. 20) – one each in Finland, France, Hungary and Sweden.

The Data Governance Act also includes measures to facilitate "data altruism" – the making of data voluntarily available by individuals or companies for the common good. It establishes the possibility for organizations engaging in data altruism to register as recognized data altruism organizations (Articles 16-24). Such organizations may not use the data for other objectives than those of general interest for which the data subject or data holder allows the processing. Article 25 clarifies that in order to facilitate the collection of data based on data altruism, the Commission will adopt implementing acts establishing and developing a European data altruism consent form.

Finally, Articles 29-30 set out the rules for the establishment of a **European Data Innovation Board** which is to assist and advise the Commission. The Board is to propose guidelines for common European data spaces, including cross-sectoral standards for data use and cross-sector data sharing, adequate protection for lawful data transfers to third countries, adequate and non-discriminatory representation of relevant stakeholders in the governance of common European data spaces and adherence to cybersecurity requirements in accordance with Union law. Article 31 introduces special rules for international access and transfer of non-personal data under the scope of the Data Governance Act.

2.2.2 Specific impacts – lessons learned

In practical terms, the data space regulatory framework has had limited impacts on CyberSEAS. The Data Governance Act lays down the groundwork for the establishment of the Common European Energy Data Space (CEDS), and as such is relevant for CyberSEAS, which aims to contribute to enhanced security of the CEDS, and to improved governance and cooperation support. CyberSEAS has thus monitored the activities of the European Data Innovation Board, and the analysis and guidelines published in the context of the CEDS (notably the October 2023 Commission **Report on a Common European Energy Data Space** - Ref. 21). The Report provided useful guidance on **legal interoperability** needs and requirements; but these were principally relevant in maintaining principles for data sharing in the context of CyberSEAS' data management plans and strategies. Since the projects were executed between project partners at local sites, the impact of data sharing agreements and legal interoperability needs were limited. In case of broader initiatives that would require larger and structural data sharing, the legal interoperability recommendations would of course take a more prominent role.

With regards to **security**, the new DGA re-use rules can be relevant for CyberSEAS stakeholders that qualify as public sector bodies, since they contain explicit provisions in relation to the use of so-called "*pre-processed data*". The pre-processing of data by public sector bodies aims to anonymize or pseudonymise personal data or delete commercially confidential information before allowing it to be re-used by third parties, and to the use of secure processing environments (a legally defined concept6) when this is required to safeguard the interests in the data. In practice, these were not needed in the context of CyberSEAS, since no data sharing occurred outside of the project partners.

That is not to say that the use of pre-processed data or of secure processing environments as defined in the Data Governance Act have limited potential; however, they are principally

6 Article 2(20) Data Governance Act, 'secure processing environment' means the physical or virtual environment and organizational means to ensure compliance with Union law, such as Regulation (EU) 2016/679, in particular with regard to data subjects' rights, intellectual property rights, and commercial and statistical confidentiality, integrity and accessibility, as well as with applicable national law, and to allow the entity providing the secure processing environment to determine and supervise all data processing actions, including the display, storage, download and export of data and the calculation of derivative data through computational algorithms.

intended and useful for data sharing in a more open ecosystem (with an unbounded or unknown number of data recipients), whereas CyberSEAS only processed data internally.

In the future, the DGA's new framework for providers of data intermediation services (including the legal and procedural safeguards to ensure their independence and trustworthiness, and the quality of their services) could be used as an input for the creation of data intermediaries in the energy field that would intervene as a trusted third party that makes data accessible (including by pre-processing it where necessary or by providing dynamic data services) and establishes specific infrastructure for the interconnection of data holders with data users.

2.3 Security of network and information systems in general: the NIS and NIS 2 Directives

2.3.1 Scope of the legal framework and general impacts

On 6 July 2016, the first Directive on the security of network and information systems (NIS) was adopted (Ref. 8). A horizontal (i.e. non-sector specific) framework, it aims to establish a minimum level of security of network and information systems across the EU, particularly for those operating essential services. As defined in the Directive, 'security of network and information systems' is understood as "*the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems*".

The NIS Directive principally targeted the Member States (rather than energy companies directly), who were required to adopt a national strategy on the security of network and information systems; and to create a computer security incident response teams network ('**CSIRTs network**') in order to contribute to the development of trust and confidence between Member States and to promote swift and effective operational cooperation. The Directive also laid down obligations for Member States to designate national competent authorities, single points of contact and CSIRTs with tasks related to the security of network and information systems. It also created a **Cooperation Group** in order to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence amongst them. These obligations and cooperation

mechanisms were introduced to support Member States in achieving a higher level of security at a national and European level.

More directly relevant to CyberSEAS were the rules in the NIS Directive that established security and notification requirements for operators of essential services and digital service providers. The NIS Directive defined in Article 4(4) '**operator of essential services'** as "*a public or private entity of a type referred to in Annex II, which meets the criteria laid down in Article 5(2)*". Crucially for CyberSEAS, the energy sector, namely electricity, gas and oil, were covered by Annex II. Other covered sectors include (1) transport, whether air, rail, road or water; (2) banking; (3) financial market infrastructures; (4) health; (5) drinking water supply and distribution; and (6) digital infrastructure, including Internet exchange points, domain name systems and top-level domain name registries.

For each sector and subsector referred to in Annex II, Member States were obligated to designate the operators of essential services with an establishment on their territory. According to Article 5(2), that should be the case when an entity provides a service which is essential for the maintenance of critical societal and/or economic activities, the provision of that service depends on network and information systems, and an incident would have "significant disruptive effects" on the provision of that service.

To determine the significance of a disruptive effect, Member States must consider the following criteria in Article 6(1):

(a) the number of users relying on the service provided by the entity concerned.

(b) the dependency of other sectors referred to in Annex II on the service provided by that entity.

(c) the impact that incidents could have, in terms of degree and duration, on economic and societal activities or public safety.

(d) the market share of that entity.

(e) the geographic spread with regard to the area that could be affected by an incident.

(f) the importance of the entity for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service.

The NIS Directive required operators of essential services take appropriate and proportionate technical and organization measures to manage the security risks posed to the services they operate (Article 14). To ensure the continuity of essential services, measures must be focused on limiting the impact of security incidents. Any significant impact on that continuity must be notified to the competent authority or the CSIRTs. In case of a cross-border impact, the competent authority or CSIRT must coordinate with the other Member States affected.

The NIS Directive was under revision for some time with the objective of further increasing its operational impact. In 2022, during the CyberSEAS project, the **NIS2 Directive (Ref. 18)** was adopted, and will repeal the first NIS Directive with effect from 18 October 2024 (i.e. after the submission of this deliverable).

The NIS 2 Directive expands the scope of the current (at the time of submission of this deliverable) NIS Directive by adding new sectors based on their criticality for the economy and society, and by introducing a clear size cap – meaning that all medium and large companies in selected sectors will also be included in the scope. Some flexibility is left for Member States to identify smaller entities with a high security risk profile. The NIS 2 Directive also eliminates the distinction between operators of essential services and digital service providers. Instead, entities are classified as either essential entities (referred to in Annex I) or important entities (referred to in Annex II) and subjected to different supervisory regimes. A registry of all essential and important entities in the EU will be created and maintained by ENISA.

Annex I, which identifies sectors of high criticality, specifically includes the electricity subsector, the latter encompassing:

— Electricity undertakings as defined in the Electricity Directive (see section 2.6), which carry out the function of 'supply' as defined in Article 2, point (12), of that Directive

— Distribution system operators as defined in Article 2, point (29), of the Electricity Directive

— Transmission system operators as defined in Article 2, point (35), of the Electricity Directive

— Producers as defined in Article 2, point (38), of the Electricity Directive

— Nominated electricity market operators as defined in Article 2, point (8), of the Electricity Regulation

— Market participants as defined in Article 2, point (25), of the Electricity Regulation providing aggregation, demand response or energy storage services

— Operators of a recharging point that are responsible for the management and operation of a recharging point, which provides a recharging service to end users, including in the name and on behalf of a mobility service provider

The emphasis is thus on infrastructural electricity service providers (as opposed to digital infrastructure services providers, which are covered elsewhere in NIS 2).

Thus, any service providers on this list which meet the EU level thresholds for medium or large enterprises, or which are designated by Member States irrespective of their size, are considered essential entities that must take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services. They must implement security risk management practices that are based on an all-hazards approach, which aims to protect network and information systems and the physical environment of those systems from incident.

As a rule, essential and important entities are deemed to be under the jurisdiction of the Member State where they provide their services (Articles 26-28). Member States are mandated to provide rules enabling entities to engage in cybersecurity-related information sharing within the framework of specific cybersecurity information-sharing arrangements (Articles 29 and 30). Articles 30-36 include rules on the supervision and enforcement of compliance with the directive.

The supervisory regime for essential entities (such as most electricity stakeholders) will be ex ante, meaning that they must systematically document compliance with cybersecurity risk-management measures; while for important entities - only ex post. Finally, the proposal updates the rules governing the CSRIST Network and the Cooperation Group, and formally establishes the EU CyCLONe – a network aimed at supporting the coordinated management of large-scale cybersecurity incidents and crises at an operational level and ensuring regular exchange of information among Member States and EU institutions (Articles 12-16).

2.3.2 Specific impacts – lessons learned

The NIS Directives establish important risk assessment, risk management and reporting/notification requirements for operators of essential services in the electricity sector.

The main innovation that the NIS 2 Directive brings when compared to the first NIS Directive is not the greater scope of the types of undertakings covered, but the fact that all medium and large entities listed in Annex I of the proposal would automatically qualify as 'essential entities'. In other words, they would need to comply with the new Directive's rules without the need to be assessed and identified as such by the Member States. This will have a significant impact on the total number of entities in the energy sector that will be mandated to implement the cybersecurity measures envisioned in NIS 2.

During the CyberSEAS project, the NIS 2 Directive had no immediate impacts yet, since the transposition deadline will not expire until CyberSEAS ends. Moreover, as noted above there are significant further steps needed before the Directive can achieve its full effect. Meanwhile however, **operators are improving their risk assessment and risk management plans to take into account the NIS 2 requirements**, notably with respect to (as listed in Article 21 of the NIS2 Directive):

(a) policies on risk analysis and information system security;
(b) incident handling;
(c) business continuity, such as backup management and disaster recovery, and crisis management;
(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;
(g) basic cyber hygiene practices and cybersecurity training;
(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;
(i) human resources security, access control policies and asset management;
(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

These obligations **did not yet apply directly to the CyberSEAS pilots**, given the later date of entry into application. Moreover, where piloting occurs only in isolated environments, separated from operational (live) systems, no particular compliance concerns arise. However, when deployment would be done on live/operational systems outside of tightly controlled parameters, execution should be within the scope of the security policies and plans of any project partners in CyberSEAS that are designed as operators of essential services under the NIS Directive.

This is not a new obligation as such, since the qualification as such an operator (and the applicability of national transpositions of the NIS Directive) is not linked to the CyberSEAS project: partners that are already subject to these rules will remain so and should in principle already be compliant; and there is no situation in which a partner would become subject to these rules merely as a consequence of their CyberSEAS activities. However, partners that do qualify as operators of essential services will need to verify whether CyberSEAS piloting affects their current policies and plans as described above. The results of this assessment, in line with the legal framework, are reflected in D8.5 – Recommendations and best practices for securing EPES against cyber threats report (v2).

As a Directive, transposition into national law is at any rate required, both under NIS I and NIS 2, and both the exact scope of assessment and reporting obligations are largely a matter of national law, both under current legislation and under NIS 2. For that reason, the principal lesson drawn in the CyberSEAS project is that operators need to have access to local legal expertise (and of course cybersecurity expertise) in order to determine whether they are already essential services under the current transpositions of the first NIS Directive, and what the resulting reporting and supervision obligations are towards the competent national authority.

The **CyberSEAS products and services can serve as inputs to substantiate compliance with the obligations under NIS I and NIS 2**, in the sense that the deployment of proven and tested EU level cyber security solutions can be a demonstration point in showing compliance with the obligations imposed by NIS laws. In that sense, CyberSEAS cannot clarify or simplify the legal framework, but it can provide tools to help comply with the legal framework.

At the present stage, these obligations are only defined at a relatively high level. However, in 2024 the **Network Code on Cybersecurity for the Electricity Sector** (Ref. 19) was adopted, which will provide more granular details on the precise obligations of operators of essential services. This Code is discussed in section 2.6 below).

Moreover and looking more towards future sustainability and governance actions, the abovementioned requirements of the NIS Directive and NIS2 Proposal should also inform CyberSEAS' efforts in the field of Certification, Governance, and Cooperation. They outline the main areas where the project can offer support to the energy sector by identifying best practices and techniques for compliance. In addition, the organizational structure of the different cooperation mechanisms in NIS and NIS2 (CSIRTs Network, Cooperation Group, EU-CyCLONe) can serve as an example of different approaches in setting up collaborative networks in the area of cybersecurity.

2.4 Cybersecurity governance and certification: Cybersecurity Act

2.4.1 Scope of the legal framework and general impacts

In order to strengthen the EU's resilience to cyber-attacks, as well as deterrence thereof and defences against such attacks, the European Commission proposed a new policy package in 2017.[7] The centrepiece of this policy package was a proposal to reform the European Agency for Network and Information Security (ENISA) into an EU Cybersecurity Agency, via the so-called **Cybersecurity Act** (Ref. 9) The goal of this Agency is to "*improve the EU's preparedness to react by organizing yearly pan-European cybersecurity exercises and by ensuring better sharing of threat intelligence and knowledge through the setting up of Information Sharing and Analyses Centres*", as well as to help Member States with the implementation of the NIS Directive.[8] At the same time, the Agency would "*help put in place and implement the EU-wide certification framework that the Commission is proposing to ensure that products and services are cyber secure*".[9]

Article 1 designates ENISA as the European Union Agency for Cybersecurity. Cybersecurity is to be understood as "*the activities necessary to protect network and information systems,*

[7] *europa.eu/rapid/press-release_IP-17-3193_en.htm.*
[8] *Id.*
[9] *Id.*

the users of such systems, and other persons affected by cyber threats".[10] Most of the other terms defined in the EU Cybersecurity Act follow the definitions from the NIS Directive.

Article 3 provides a mandate to ENISA as the European Union Agency for Cybersecurity to achieve a high common level of cybersecurity across the Union, while article 4 defines the objectives of the Agency. The Agency will assist and advise on Union policy in this field, as well as help Member States in implementing those policies.[11] The Agency will also support capacity-building (article 6), operational cooperation at the Union level (article 7), and cybersecurity certification and standardization (article 8). Furthermore, the Agency will develop and share knowledge in this field (article 9), raise public awareness and provide education (article 10), and advice on and participate in research and innovation (article 11). Overall, these provisions are fairly broad and general. They mainly serve to establish the broadest possible mandate for the Agency in the field of cybersecurity. For the purposes of the CyberSEAS project, the mandate is less directly relevant – while the eventual live implementation of CyberSEAS outputs may be of interest to ENISA under its general mandate, there are no immediate implications in the short term.

Of greater interest is Title III of the Act, which provides for a new, EU level **cybersecurity certification framework**. This framework aims to "*improve the conditions for the functioning of the internal market by increasing the level of cybersecurity within the Union and enabling a harmonised approach at Union level to cybersecurity certification schemes, with a view to creating a digital single market for ICT products, ICT services and ICT processes*" (article 46). It establishes European cybersecurity certification schemes to attest that ICT products, processes and services evaluated in accordance with such schemes comply with specified security requirements aiming to protect the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the functions or services offered by, or accessible via, those products, processes, and services throughout their life cycle. The European Commission will establish a work program to identify strategic priorities for future European Cybersecurity Certification schemes (article 47). The Agency may also be requested to draft a candidate European cybersecurity certification scheme (article 49).

Article 51 defines the security objectives of the certification schemes. They must prevent unauthorized access to, or disclosure or removal of data. They must allow to check who accessed which data, services or functions. They must keep in mind the principles of security by design and security by default. Certification schemes can provide different assurance levels, commensurate with the level of risk associated with a process, product or service

[10] Article 2(1) EU Cybersecurity Act.
[11] Article 5 EU Cybersecurity Act.

(article 52). A basic assurance level aims to minimize known basic risks. A substantial security level assures minimization of known risks. A high security level shows minimization of risks of state-of-the-art cyberattacks. Cybersecurity certification schemes may allow for conformity self-assessment for the basic assurance level (article 53). The Act describes an extensive list of elements that should be present in a certification scheme, such as a description of standards, evaluation criteria, a description of the certificate, etc. (article 54). Certification principally occurs on a voluntary basis, but the Commission may decide to make particular schemes mandatory for certain products, processes or services (article 56). The sectors identified in Annex II to the NIS Directive will be given priority for such assessment.

The aim of the Act is to replace any existing national cybersecurity certification schemes with any European-wide scheme. Specifically, national schemes may only continue to function in the areas not covered by European schemes (article 57). National cybersecurity certification authorities must be designated to conduct supervision (article 58). To ensure equivalent standards, national certification schemes must be subjected to peer review (article 59). Conformity assessment bodies can be designated through a procedure established by the Annex to the Act (article 60). The Commission will for each European cybersecurity certification scheme be notified of national cybersecurity certification authorities (article 61). Representatives of these national cybersecurity certification authorities will form the European Cybersecurity Certification Group (article 62). The Act foresees in a right to complaint and remedy, as well as penalties (articles 62-64).

At the time of submission of this deliverable, work has been initiated on three EU level cybersecurity certification schemes: a general scheme for ICT products known as 'EUCC' (based on, and largely equivalent to, the existing international Common Criteria scheme); a second scheme (EUCS) for cloud services; and a third one (EU5G) for 5G networks. Only the EUCC scheme has been formally adopted thus far, via a specific Regulation, in January 2024 (the EUCC Regulation, Ref. 22).

Without going into detail, the **EUCC scheme** permits suppliers of ICT products (hardware, software or a combination thereof) to voluntarily undergo certification by conformity assessment bodies and national cybersecurity certification authorities, that have been authorized to do so under the Cybersecurity Act. The scheme is based on the international SOG-IS Common Criteria evaluation framework, and supports two levels of assurance ('high' and 'substantial'), based on the level of risk associated with the intended use of the product, service or process, in terms of probability and impact of an accident. State-of-the-art (SoA) documents have been prepared by ENISA to clarify the applicable evaluation methods, techniques and tools for certain types of products; but **no particular SoA or protection profile is presently available for energy products**.

Thus, no formal certification of ICT products targeting electricity products is presently available. This may change in the future, also under the influence of the proposed Cyber Resilience Act (Ref. 23). The latter would require, among many other points, that certain products with digital elements that are used by essential entities in the sense of the NIS 2 Directive, to be considered as so-called "critical products with digital elements", and thus to undergo a mandatory conformity assessment. However, the Cyber Resilience Act has not yet been adopted at the time of submission of this deliverable, nor is it clear yet how it would impact the electricity sector in the future.

2.4.2 Specific impacts – lessons learned

The **direct impact of the Cybersecurity Act on CyberSEAS has been very limited**: despite the progress on the EUCC, and notwithstanding the discussions around an EU level Cyber Resilience Act, **there is no EU level cybersecurity scheme that should (or can) be taken into account by the project**. The relevance of the Act thus doesn't lie in its direct application.

However, the outputs that CyberSEAS has created can provide relevant inputs for a future EPES cybersecurity scheme that could be adopted under the Act – either independently, or in the form of a SoA or a protection profile under the existing EUCC. In that way, CyberSEAS can contribute to the further elaboration of certification schemes; and inversely, the Act could be used as a support for CyberSEAS' sustainability and future exploitation once a certification scheme has been adopted.

For that reason, the project's security policies have taken into account the key elements of a security certification scheme as defined by the Cybersecurity Act. These are specified in Article 51 of the Act, and include as a minimum the following security objectives:

(a) to protect stored, transmitted or otherwise processed data against accidental or unauthorised storage, processing, access or disclosure during the entire life cycle of the ICT product, ICT service or ICT process.
(b) to protect stored, transmitted or otherwise processed data against accidental or unauthorised destruction, loss or alteration or lack of availability during the entire life cycle of the ICT product, ICT service or ICT process.
(c) that authorised persons, programs or machines are able only to access the data, services or functions to which their access rights refer.
(d) to identify and document known dependencies and vulnerabilities.

(e) to record which data, services or functions have been accessed, used or otherwise processed, at what times and by whom.
(f) to make it possible to check which data, services or functions have been accessed, used or otherwise processed, at what times and by whom.
(g) to verify that ICT products, ICT services and ICT processes do not contain known vulnerabilities.
(h) to restore the availability and access to data, services and functions in a timely manner in the event of a physical or technical incident.
(i) that ICT products, ICT services and ICT processes are secure by default and by design.
(j) that ICT products, ICT services and ICT processes are provided with up-to-date software and hardware that do not contain publicly known vulnerabilities and are provided with mechanisms for secure updates.

These elements can thus be seen as a requirement statement for any future inputs to a security certification scheme that builds on CyberSEAS' work, and have been taken into account in the drafting of D8.8 - Report on recommendations for certification, standardization and exchange of information at the EU level.

2.5 Critical infrastructure protection: ECI Directive and the CER Directive

2.5.1 Scope of the legal framework and general impacts

As a reflection of the importance of ensuring the resilience of critical infrastructures, the Commission adopted in 2006 the **European Programme for Critical Infrastructure Protection (EPCIP - Ref. 10)**, which sets out a European-level all-hazards framework for critical infrastructure protection. One of the central pillars of the EPCIP is **Directive 2008/114 (CIP Directive or ECI Directive - Ref. 11)**, which establishes a procedure for identifying and designating European Critical Infrastructures (ECIs) in the transport and energy sectors that, if disrupted or destroyed, would have significant cross-border impacts. The ECI Directive establishes a procedure for the identification and designation of ECIs, and a common approach to the assessment of the need to improve the protection of such infrastructures.

According to Article 2(a), 'critical infrastructure' is "*an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions*". A 'European critical infrastructure' or 'ECI', on the other hand, means "*critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure*" (Article 2(b)).

The primary and ultimate responsibility for protecting ECIs falls on the Member States and the owners/operators of such infrastructures. According to Articles 3-4, Member States identify and designate potential ECIs in the energy or transportation sector which satisfy both the cross-cutting and sectoral criteria set out in the Directive. For electricity, the relevant subsector consists of "*infrastructures and facilities for generation and transmission of electricity in respect of supply electricity*" (Annex I).

The cross-cutting criteria to determine the applicability and relevance of the Directive, referred to in Article 3, comprise of the following:

(a) the casualties criterion (assessed in terms of the potential number of fatalities or injuries).

(b) economic effects criterion (assessed in terms of the significance of economic loss and/or degradation of products or services; including potential environmental effects).

(c) public effects criterion (assessed in terms of the impact on public confidence, physical suffering and disruption of daily life; including the loss of essential services).

With respect to the implications of the application of the Directive (or rather, its national level transpositions), Article 5 introduces the obligation for an operator to establish a so-called 'operator security plan' (OSP), set out in greater detail in Annex II, that identifies the ECI's critical infrastructure assets, and which specifies which security solutions exist or are being implemented for their protection. It is up to the Member States to assess whether designated ECIs possess an OSP. Article 6 introduces Security Liaison Officers as contact points for security issues between owners/operators of ECIs and the relevant Member State authority. Article 10 mandates Member States to appoint also a European critical infrastructure protection contact point. The ECI Directive includes reporting obligations for Member States, namely report every two years to the Commission with summary data on the types of risks, threats and vulnerabilities encountered per ECI sector (Article 7).

In 2022, the new **Critical Entities Resilience (CER) Directive (Ref. 12)** was adopted, which aims to ensure greater coherence to the EU's overall approach to critical infrastructure protection and resilience. The Directive has not yet entered into force at the time of submission of this deliverable, since it must be transposed by 18 October 2024 (not coincidentally the same deadline as the NIS 2 Directive), at which point the ECI Directive will be repealed. None the less, for the sake of future proofing CyberSEAS, it is worth understanding how the CER Directive will change the critical infrastructure protection landscape in Europe.

According to Article 3, each Member State would need to adopt a strategy for reinforcing the resilience of critical entities. Article 4 states that competent authorities shall establish a list of essential services and carry out regularly an assessment of all relevant risks that may affect the provision of those essential services with a view to identifying critical entities.

Articles 10-13 include new rules on the resilience of critical entities. Article 10 states that critical entities shall regularly assess all relevant risks on the basis of national risk assessments and other relevant sources of information. Article 11 mandates critical entities to take appropriate and proportionate technical and organizational measures, and to ensure that these measures are described in a resilience plan or equivalent document or documents. Critical entities are also obliged to notify the competent authority of incidents that significantly disrupt or have the potential to significantly disrupt their operations. Articles 14-15 introduce rules for specific oversight over critical entities of particular European significance (providing essential services in more than 1/3 of Member States). A Critical Entities Resilience Group is set up with Article 16 to facilitate strategic cooperation and the exchange of information in the field.

2.5.2 Specific impacts – lessons learned

The ECI Directive and the more recently adopted CER Directive are important for CyberSEAS as a project, due to their focus on measures to increase resilience for critical infrastructures. Energy sector entities, and especially "*infrastructures and facilities for generation and transmission of electricity in respect of supply electricity*" are part of the EU's critical infrastructure and as such are subject to the requirements of these two texts. With respect to the types of entities that could be identified as critical in the electricity sector, the Annex[12] to the CER Directive proposal aligns them with the 6 types of entities that can provide essential electricity services under the NIS2 Directive. As such, most entities in the energy sector will

[12] Annex to the Proposal for a Directive of The European Parliament and of The Council on the resilience of critical entities. Available at: https://home-affairs.ec.europa.eu/system/files/2020-12/15122020_proposal_directive_resilience_critical_entities_annex-1_com-2020-829-1_en.pdf

likely qualify as both essential and critical and will thus need to ensure compliance with both legislative acts.

In particular, critical entities under the CER Directive will have to take the following measures to increase resilience, as outlined in Article 11 of the proposal:

(a) prevent incidents from occurring, including through disaster risk reduction and climate adaptation measures.
(b) ensure adequate physical protection of sensitive areas, facilities and other infrastructure, including fencing, barriers, perimeter monitoring tools and routines, as well as detection equipment and access controls.
(c) resist and mitigate the consequences of incidents, including the implementation of risk and crisis management procedures and protocols and alert routines.
(d) recover from incidents, including business continuity measures and the identification of alternative supply chains.
(e) ensure adequate employee security management, including by setting out categories of personnel exercising critical functions, establishing access rights to sensitive areas, facilities and other infrastructure, and to sensitive information, as well as identifying specific categories of personnel in view of Article 12.
(f) raise awareness about the measures referred to in points (a) to (e) among relevant personnel.

Thus – and this assessment is comparable to the findings relating to the NIS 2 Directive's application to operators of essential services – the **CER rules only become directly relevant when piloting would be done on live/operational systems**; in that case, the pilot execution should be within the scope of the security policies and plans of any project partners in CyberSEAS falling within the scope of the national transposition of the ECI rules.

In the meantime however, in the course of the CyberSEAS project, the **resilience requirements of the CER Directive have been taken into account in the regulatory compliance efforts as well**, notably by including the potential negative impacts of incidents in the DPIA template (see also Annex II of this deliverable), and in the security requirements defined in other deliverables.

2.6 The EU Energy Package – the Electricity Directive and Electricity Regulation

2.6.1 Summary – scope and general impacts

In 2019 the EU overhauled its energy policy framework, in order to move away from fossil fuels towards cleaner energy and to deliver on the EU's Paris Agreement commitments for reducing greenhouse gas emissions. This overhaul built on the Commission's November 2016 proposal for a Clean Energy Package (known formally as the Clean Energy for All Europeans Package), a legislative package that largely updated the previous one, the Third Energy Package, and other key EU environmental legislation.

The Clean Energy Package consists of eight different legislative proposals on energy efficiency, governance regulation, energy performance in building, renewable energy and electricity market design. A key part of the Clean Energy Package is to make the EU electricity market fit for the clean energy transition. It sets out the new electricity markets rules that are included in the four pieces of legislation: the Electricity Directive (EU) 2019/944 (Ref. 13), the Electricity Regulation (EU) 2019/943 (Ref. 14) and its Commission Delegated Regulation (EU) 2024/1366 establishing a Network Code on Cybersecurity for the Electricity Sector (Ref. 19), the Regulation on risk preparedness (EU) 2019/941 (Ref. 15), and the ACER (Agency for the Cooperation of Energy Regulators) Regulation (EU) 2019/942 (Ref. 16).

The new electricity market design is intended to better fit the future electricity markets, which will be characterized by more variable and decentralized production, an increased interdependence between cross-border systems, and opportunities for consumers to participate in the market through demand-side response, aggregation, self-generation, smart metering and storage.

Taking into account the objectives, scope, and priorities of CyberSEAS this section provides an analysis of the **Electricity Directive, the Electricity Regulation and the Network Code on Cybersecurity, and the Regulation on risk preparedness**.

The **Electricity Regulation (EU) 2019/943** (the Electricity Regulation) aims to adapt the existing market rules to new emerging market realities. The Electricity Regulation provides a set of fundamental principles for well-functioning, integrated electricity markets. These principles are directed to the main parties of the electricity market, including, Member States, regulatory authorities, transmission system operators (TSOs), distribution system operators (DSOs), market operators and delegated operators that must operate following the following principles:

- Market rules must encourage free price formation; enable the decarbonisation and the integration of electricity from renewable energy sources and provide incentives for energy efficiency; deliver appropriate long-term investment incentives for decarbonised and sustainable electricity systems, for energy storage, energy efficiency, and demand response; provide for regional cooperation and facilitate the trade of products; enable the efficient dispatch of generation assets, energy storage, and demand response.
- The electricity prices must be formed based on demand and supply, forbidding caps or floors on wholesale prices.
- Customers must be enabled to benefit from market opportunities and increased competition in retail markets and must be empowered to act as market participants in the energy market and the energy transition.
- Market participation of final customers and small enterprises must be enabled by aggregation of generation or load from multiple facilities to provide joint offers on the market.
- Barriers to cross-border electricity flow and transactions must be progressively removed.
- Safe and sustainable generation, storage, and demand are to participate on equal footing in the market.
- Market participants must have a right to obtain grid access on objective, transparent and non-discriminatory terms.
- All producers shall be directly or indirectly responsible for selling the electricity they generate.
- All market participants shall be responsible for the imbalances they cause in the system ('balance responsibility').

Furthermore, the Electricity Regulation lays down the obligations related to TSOs, including obligations to issue long-term transmission rights or have equivalent measures in place to allow market participants to hedge price risks. Long-term transmission rights must be allocated on a single allocation planform (Article 9). Following the revision of the Electricity Regulation, TSOs have the obligation to reach a minimum level of cross-zonal capacity to facilitate electricity trading across countries. Finally, the Electricity Regulation encourages TSOs to cooperate at Union and regional levels, as well as establish cooperation with DSOs in planning and operating their networks.

The Electricity regulation also establishes the European Network of Transport System Operators for Electricity (ENTSO-E), a European forum for the cooperation of Transmission

systems operators (TSOs), which is tasked with monitoring national TSOs and their EU-wide network development plans. The Regulation designates tasks for ENTSO-E and monitoring obligations for the European Union Agency for the Cooperation of Energy Regulators.

In the context of CyberSEAS, the Regulation is also – and perhaps principally – important as the legal basis for the adoption in 2024 **Network Code on Cybersecurity for the Electricity Sector** (Ref. 19 – formally the Commission Delegated Regulation (EU) 2024/1366). The Network Code aims to ensure a high, common level of cybersecurity for cross-border electricity flows in Europe. It defines the central requirements for a periodic cybersecurity risk assessment in the electricity sector. Such assessments are aimed at systematically identifying the entities that perform digitalised processes with a critical or high impact in cross-border electricity flows, their cybersecurity risks, and then the necessary mitigating measures that are needed.

More specifically, the Code requires certain operators to define and formalize cybersecurity risk assessment methodologies and reports, minimum and advanced cybersecurity controls, cybersecurity procurement recommendations , and a cyber-attacks classification scale methodology.

To support these efforts, the Code also defines a governance model that uses and is aligned with the mechanisms of the aforementioned NIS 2 Directive, thus promoting a common baseline, while respecting existing practices and investments as much as possible. While the Code has not yet entered into force at the time of submission of this deliverable, it is clear that it will apply to any use of cybersecurity technology in the electricity market.

The **Electricity Directive (EU) 2019/944** (the Electricity Directive) is coupled with the Electricity Regulation. This Directive focuses specifically on establishing an integrated, competitive, consumer-centred, flexible, fair, and transparent electricity market in the European Union. It outlines common rules for the generation, transmission, distribution, supply, and storage of electricity, together with consumer protection aspects. It contains also rules on the retail electricity market, promotion of regional cooperation between Member States and national regulatory authorities and sets out public service obligations for electricity undertakings.

Directly relevant to the CyberSEAS project are the requirements that the Electricity Directive lays down for the distribution system operators (DSOs) and transmission system operators (TSOs).

Particularly, DSOs are responsible for ensuring the long-term ability of the system to meet demands for the distribution of electricity, including the cost-efficient integration of new electricity generation installations, and especially the ones which produce electricity from renewable sources, as well as for providing system users with the information needed for efficient access and use of the system. They must publish network development plans setting out the planned investments for the following 5 to 10 years. Also, where part of a vertically

integrated undertaking, DSOs must be independent at least in terms of their legal form, organization, and decision-making from other activities not relating to distribution. DSOs are not allowed to own, develop, manage or operate storage facilities except where certain specific conditions are met.

Furthermore, the Electricity Directive requires TSOs to ensure the long-term ability of the system to meet demands for the transmission of electricity, in close cooperation with neighbouring TSOs and DSOs. TSOs must manage the secure operation of the system including keeping the balance between electricity supply and demand. Moreover, TSOs are not allowed to own, develop, manage or operate energy storage facilities, except where certain specific conditions are met.

Finally, the consumer is put at the centre of the clean energy transition and the new rules enable the active participation of consumers, through the citizen energy community, for instance. The citizen energy communities are legal entities based on voluntary and open participation of natural persons, local authorities, and small or micro-enterprises, which purpose is to provide environmental, economic, or social community benefits for their members or the local areas where they operate. The Electricity Directive puts in place a strong framework for consumer protection by reinforcing the existing consumers' rights and establishing new ones; these include the right to freely choose a supplier, the right to join or leave a citizen energy community and right to leave the community without penalties; the right to produce, consume, store and sell electricity, individually or through an aggregator; and the right to request the installation of a smart meter within 4 months.

Finally, another important piece of legislation that has been introduced by the Clean energy for all Europeans package and is relevant for the purpose of the research project is the **Regulation on risk preparedness in the electricity sector (EU) 2019/941** (hereinafter the Regulation on risk preparedness).

The Regulation on risk preparedness is a result of the Commission's independent report findings that Member States take very different approaches in assessing, preventing, and managing electricity crisis situations. This Regulation requires EU Member States to prepare plans for how to deal with potential future electricity crises, and put the appropriate tools in place to prevent, prepare for and manage these situations.

Hence, it sets out measures for risk assessments, risk- preparedness, and the management of any electricity crisis situations in the European Union at the level of both Member States and their regions. The Regulation also requires Member States to cooperate and coordinate with neighbouring Member States in a spirit of solidarity.

To summarise, the Regulation on risk preparedness sets out methodologies to:

- Assess the security of supply;.

- Identify crisis scenarios in the Member States and on a regional level.
- Conduct short-term adequacy assessments.
- Establish risk-preparedness plans and manage crisis situations.

2.6.2 Specific impacts – lessons learned

The Energy package was relevant principally as a complement to the NIS and NIS 2 Directives and their national transpositions. Under these frameworks as discussed above, certain types of entities in the electricity sector were already designated as operators of essential services, and thus subject to obligations in relation to risk preparedness and the management of incidents in order to ensure supply security of electricity.

The Network Code on Cybersecurity for the Electricity Sector in particular is much more detailed and granular on these obligations. However, it has not yet entered into force at the time of submission of this deliverable, and requires significant further elaboration on many points, including:

> - the preparation for a proposal, to be developed by the TSOs, with the assistance of the ENTSO for Electricity, in cooperation with the EU DSO entity and following a consultation with the NIS Cooperation Group, for the cybersecurity risk assessment methodologies at Union level, at regional level and at Member State level;
>
> - the Member State level performance, by their respective competent authorities, of a cybersecurity risk assessment on all high-impact and critical-impact using standardised methodologies;
>
> - the development by the TSOs, with the assistance of the ENTSO for Electricity, in cooperation with the EU DSO entity and in consultation with the Regional Coordination Centres and the NIS Cooperation Group, of a regional cybersecurity risk mitigation plan for each system operation region; and
>
> - the performance by each high-impact and critical-impact entity as identified by the competent authorities a cybersecurity risk assessment for all its assets in its high-impact and critical-impact perimeters.

While these elements still are to be developed, CyberSEAS collected inputs on how to link existing risk assessment methodologies to these legal frameworks, building on the feedback of CyberSEAS partners. Notably, Task 2.3 of CyberSEAS used the common asset list (based on

the outputs of Task 2.1) to conduct an extensive asset / MITRE attack technique mapping, in the context of analysing cyber threat scenarios and their impacts across the electricity supply chain. The outcomes that work, cross referenced against a common asset structure, were taken as a baseline to determine information security risks.

The CyberSEAS project also cross referenced these findings against the data protection risk categorization proposed in the ISO/IEC – 29134 standard. This exercise was deemed useful, since the Task 2.3 outputs do not focus specifically on data protection and privacy risks, and the emphasis on EPES may otherwise cause privacy/data protection risks to be overlooked.

The general finding was that the CyberSEAS partners already had risk management and risk assessment practices in place, built on common international practices and standards, but that these could be further detailed and instantiated in the course of piloting.

3 Ethical requirements

A fundamental requirement in any EU funded project is compliance with the European framework for fundamental rights, including the rights to privacy and data protection. Several tasks have been defined in CyberSEAS to identify ethical issues and mitigation strategies, even beyond mere legal compliance.

As was described in the introductory section of this report, relevant ethical and societal values that aren't directly related to data protection law are developed in the context of D3.2 (CyberSEAS technical requirements, SELP requirements and system specifications) by applying the theory of Value Sensitive Design, an approach which aims to integrate a wide range of human and moral values into the design of (information) technology (Ref. 5). Without repeating the contents of that deliverable, the value system is designed around the European Charter of Fundamental Rights (Ref. 17), as the principal underpinning of SELP protections for European citizens. The Charter applies a structure of six value domains:

- **Dignity**, notably individuals' right to be secure in their physical and mental integrity.
- **Freedoms**, comprising the rights to data protection and privacy, but also intellectual freedoms (education, expression, thought, religion and information) and social freedoms (assembly, marriage, asylum and property).
- **Equality**, including non-discrimination and rights of minorities and of societally more vulnerable parties.
- **Solidarity**, covering workers' rights and labour rights, social security, collective bargaining, health care and environmental protection.
- **Citizens' rights**, such as the right to vote, to proper administration, access to documents and freedom of movement.
- **Justice**, including access to fair trial and effective remedy, and the right to defence.

More tailored and specific SELP requirements were derived from more detailed normative frameworks with respect to fundamental rights protections. These include notably:

- Opinions of the European Group on Ethics in Science and New Technologies, including but not limited to EGE **Opinion n°28** - 20/05/2014 - Ethics of Security and Surveillance Technologies and the EGE **Opinion n°26** - 22/02/2012 - Ethics of information and communication technologies.

- The European Code of Conduct for Research Integrity, including but not limited to **section 1, Articles 2.1, 2.3, 2.4, 2.5**.
- EU Commission's 'Ethics and Data Protection' in research settings (2018), including but not limited to **sections II, VI, X and XIII**
- EU Commission's 'Ethics in Social Science and Humanities' (2018), including but not limited to **sections 3, 4, 6 - 10**

The resulting requirements were developed and addressed in detail across three deliverables:

- **D10.1 H - Requirement No. 1**. This deliverable contained notably an introduction to the human involvement in CyberSEAS, and incidental findings policy, and a template Informed Consent and Information Sheet
- **D10.2 POPD - Requirement No.2.** This deliverable contained notably the confirmation of the appointment of a qualified data protection officer (DPO) in CyberSEAS, as well as a description of anonymisation and pseudonymisation techniques, and a policy relating to the further processing of previously collected personal data.
- **D2.5 and D2.6 - Privacy Risk Mitigation Plan (v1 and v2).** These deliverables contained notably an initial data protection impact assessment in order to assess compliance with the General Data Protection Regulation. Moreover, it defines a monitoring methodology for the use cases, requiring each use case to self-assess its compliance with the project's requirements, and to obtain a prior approval from the Internal Ethics Committee (IEC) prior to starting the use case.

For more detailed information on (non-legally driven) ethical requirements, we refer to these deliverables. It is worth recognising that virtually all of these requirements focus on the safeguarding of the fundamental rights to privacy and data protection, for the simple reason that other fundamental rights are either unaffected by CyberSEAS (e.g. improving the resilience of the electricity infrastructure in Europe does not affect the rights to equality or solidarity); or that those rights are affected only in a positive sense (e.g. improved resilience prevents security incidents, which strengthens the right to dignity (by increasing access to high quality and dependable energy), and diminishes the need for recourse to justice (by reducing crime, rather than managing its further handling).

4 Best practices and lessons learned with respect to SELP compliance

4.1 Summary of the SELP framework

As the overview above shows, the security, ethics, legal and privacy requirements in CyberSEAS are driven by six major domains:

- Data protection and privacy, notably via the GDPR.
- Data governance, notably driven by the Data Governance Act.
- Security of network and information systems in general, notably via the NIS Directive and the NIS 2 Directive).
- Cybersecurity governance and certification via the Cybersecurity Act.
- Critical infrastructure protection, via the ECI Directive and the CER Directive.
- The EU Energy package, principally via the triad of the Electricity Regulation (including the Network Code on Cybersecurity for the Electricity Sector) , the Electricity Directive and the Risk Preparedness Regulation.

Beyond these, non-regulatory ethics requirements are driven by the EU's fundamental rights protection framework, and non-binding best practices documents.

The analysis shows that the principal binding requirements directly stem from data protection law, i.e. from the GDPR. With that in mind, much of the SELP implementation and compliance assurance procedures in CyberSEAS (explained in the following sections) focus on ensuring data protection compliance.

With respect to security obligations, the analysis also clearly shows that operators in the electricity markets are already quite heavily regulated, with strong obligations to document and implement security and risk management procedures. These obligations are even stronger if the operators are designated as providing critical infrastructure (under the ECI Directive) and/or as providers of essential services (under the NIS Directive). This implies that the piloting and testing procedures of CyberSEAS must not only undergo data protection compliance assessments, but also that electricity operators must assess whether the use of

the CyberSEAS solutions can have an impact on the security and capabilities of their infrastructure, and if so, evaluate and update their policies where needed.

This obligation applies only to operators in the electricity markets, not to the creators of software or hardware solutions that aim to improve the security of the electricity market. For this reason, compliance questions are best addressed at the pilot level, rather than at the more abstract project level as whole.

Finally, it is also worth underlining that there are many avenues in the existing and emerging legal frameworks to support the sustainability, exploitation and market value of CyberSEAS. CyberSEAS solutions could provide inputs for a specialised cybersecurity certification scheme under the Cybersecurity Act, and could facilitate compliance with the security and governance obligations for electricity operators under the NIS and ECI Directives, as well as under the Energy Package.

4.2 SELP implementation and compliance in CyberSEAS

Especially in a project with the scale and complexity of CyberSEAS, it is critical that compliance with SELP requirements is continuously monitored and evaluated. This is needed to ensure that the SELP approach is known and understood by all relevant CyberSEAS partners, and that they adhere to the SELP requirements in practice. A continuous validation, support and verification process was implemented that allowed all use cases and technologies to be monitored continuously.

In order to achieve this goal, CyberSEAS applied a mechanism that combined:

(1) self-evaluation and self-assessment by the pilot participants themselves, in which they will conduct their own risk assessment and report on exact SELP measures taken on the basis of a common template;
(2) An independent verification and support process by the CyberSEAS Internal Ethics Committee (IEC).

To support this approach, CyberSEAS applies a standard four tiered governance model:

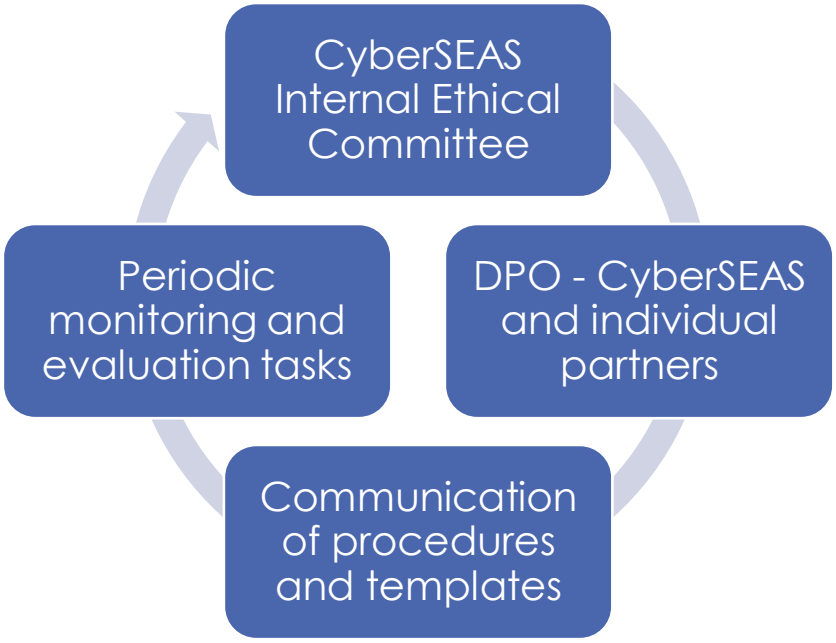

Figure 4: Monitoring and evaluation structure

- **Establishment of a CyberSEAS Internal Ethical Committee** (IEC), which has the assignment of ensuring clarity and consistency in communicating with CyberSEAS project partners on ethics issues, assessing compliance with SELP policies, and supporting interactions with the users. It has the responsibility for monitoring, ethical, privacy and data protection/SELP issues. In practice, the Committee consisted of the legal and ethics experts of CyberSEAS' legal and ethics partner (Timelex), with ad hoc support from other CyberSEAS partners where necessary to provide inputs on requirements, or to get updates on the pilot project status. The IEC assessed progress of the pilots and of the general EU level legal framework (including impacts on the project) on a monthly basis.
- **Appointment of Data Protection Officers** (DPOs) in accordance with the GDPR. The CyberSEAS project has nominated a project DPO (Hans Graux, from legal and ethics partner Timelex) to oversee data protection compliance. Moreover, a list of DPOs at the partner level was maintained throughout the project, to facilitate interaction with local end users, and to ensure that there is hands-on involvement at the partner level.
- **Communication of procedures and templates:** the ethics guidance from the WP10 deliverables are actively disseminated and explained towards all CyberSEAS partners,

to ensure that they are known and used in practice. Deviations are of course possible and permissible (including localization, translation and customization of templates), provided that the legal and functional goals set out in this deliverable are achieved.

- **Periodic monitoring and evaluation tasks:** Beyond the ethics reporting in the periodic activity reports, CyberSEAS defined specific tasks to conduct data protection impact assessments (T2.5) and to create and monitor SELP (Security, Ethical, Legal and Privacy) requirements (T3.2). These were maintained and updated via the aforementioned IEC monthly meetings, which were used to further detail, monitor and report on ethics compliance, and to take any corrective actions needed.

In this way, CyberSEAS has ensured compliance throughout the project's duration, by combining deep and tailored understanding of the pilot circumstances, with neutral and consistent assessment by the IEC.

In practical terms, partners were relatively self-managing throughout most piloting activities, since the principal ethics concern was the protection of privacy and personal data protection. However, most piloting activities did not imply the processing of personal data, and where such processing did occur, appropriate compliance and mitigation actions could be undertaken to minimise the ethics risks appropriately, as discussed in section 2.1.

4.3 Main lessons learned - SELP Manual for EPES deployment

Providing guidance and support on SELP matters in the project was a complex and demanding effort, for a multitude of reasons, all of which can be labelled as lessons learned.

Firstly, as the overview above has shown, the **regulatory framework for EPES and for cybersecurity in Europe is subject to rapid change.** In the course of the project, a very significant number of often complex new regulatory initiatives have been adopted, such as the NIS 2 Directive, the CER Directive, the first network code on cybersecurity for the electricity sector, and the EUCC cybersecurity certification scheme. All of these required careful assessment with respect to the objectives, obligations, applicability and future relevance. The exercise was made more complicated that some of these were Directives, which require transposition into national law (as opposed to Regulations that apply directly in all Member States). As a result, not only did the rules change, but the changes depended

on the Member States under examination. Thus, **significant efforts were needed to simply keep track of changes in the legal framework.**

Secondly, a known element is of course that both EPES and cybersecurity **require a combination of a multitude of skills. SELP compliance is thus only possible through a combination of profiles,** including of course legal and ethical expertise, but also market knowledge, standardisation knowledge, and operational risk management and security management expertise. Thus, **SELP compliance requires a multi-disciplinary compliance team that includes all of these skills.** In this manner, outputs covering multiple aspects of regulatory obligations could be covered, resulting e.g. in the creation of D8.5 – Recommendations and best practices for securing EPES against cyber threats report (v2); and D8.8 - Report on recommendations for certification, standardization and exchange of information at the EU level. Such a multi-disciplinary team was available in CyberSEAS, but this is not self-evident, and will likely not be the case in all projects.

Thirdly, there is a **significant difference between piloting / testing new cybersecurity products and services, and implementing them in live situations.** In CyberSEAS, much of the efforts were dedicated to piloting and testing, and while significant resources were dedicated to ensuring that these would be fit for the European market, this also implied that SELP requirements were often more trivial to satisfy than initially anticipated during the piloting itself. In order to facilitate future SELP compliance guidance, **careful planning is required that recognises the various stages (initialisation, testing, go-live, etc) of piloting, and that ensures that the SELP compliance measures are effective and proportionate.**

The present final SELP report has a 'best practice' goal, and aims to share the difficulties and solutions linked to SELP that have been encountered during the lifetime of CyberSEAS. As such, it provides a summary of the requirements that includes these new frameworks, reports on their implementation in the project, and describes the principal lessons learned.

In order to ensure that these lessons are made available and can be shared in a more easily digestible form, this deliverable includes in its Annex a high-level SELP Manual for EPES Projects, that captures some of the main lessons learned. While omitting a lot of the details of this deliverable, this Manual can be used to deploy CyberSEAS solutions in a secure and legally compliant manner even after the project's duration, and that can also be used as a tool to guide EPES deployments even outside the context of CyberSEAS projects and services. In this manner, CyberSEAS aims to provide a significant contribution to increased cyber resilience in European EPES, also from a SELP perspective.

5 Annex I – SELP Manual for EPES Projects

5.1 About this Manual

One of the central challenges in any EPES project is ensuring compliance with Security, Ethical, Legal and Privacy (SELP) principles. Based on its experiences, the CyberSEAS project has created this SELP Manual for EPES Projects (hereafter the Manual), that can be used when deploying and maintaining CyberSEAS products and services, or more generally when designing, deploying and managing cybersecurity products and services in a European electricity grid context.

The Manual has been designed to be accessible and understandable for a broad range of stakeholders. With this priority in mind, it necessarily oversimplifies a number of topics. Moreover, significant effort will be required to implement the Manual in practice. The objective of the Manual is not to provide a comprehensive handbook, but to define waypoints in any EPES compliance trajectory. With this in mind, the Manual will identify the main priority topics, and indicate why and how they should be implemented, and what the main pitfalls and challenges are.

In this manner, CyberSEAS aims to provide a significant and permanent contribution to the future of increased cyber resilience in European EPES, also from a SELP perspective.

Since this Manual aims to provide a procedural guideline, it is organised on the basis of the logical lifecycle of an EPES project. Thus, the Manual comprises four principal chapters, reflecting the phasis in this lifecycle:

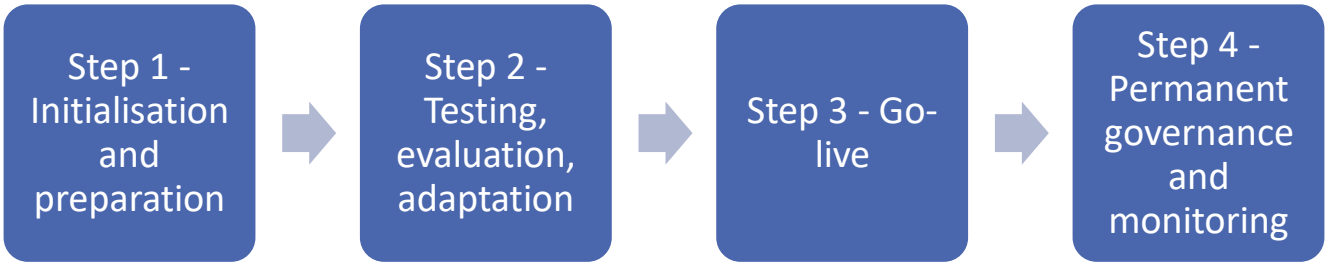

Figure 5: EPES SELP compliance steps

The SELP requirements and checks for each step are summarized below.

5.2 Step 1 – Initialisation and preparation

5.2.1 Scoping

The first and most labour intensive step is **defining the formal scope of the EPES project.** This step is complex, due to the need to connect functional and architectural choices to a specific legal qualification, which inherently requires a multitude of skills and competences.

At a minimum, the following scoping elements should be defined:

- Who are the organisations involved, and what will be their role?
- What is the intended goal of the project – i.e. what is it intended to achieve / improve?
- What is the foreseeable impact on the organisations, the infrastructure, and other stakeholders (notably customers if applicable, but also e.g. regulators or law enforcement bodies)? Both positive and negative impacts should be identified?
- Where will the project take place (Member States and precise location)? Since much of the legal framework is still linked to national law and/or national regulatory bodies, transborder projects are inherently more complex (especially projects with an extra-EU impact).
- What categories of assets are involved (data and infrastructure), including any use of AI? This influences the applicable legal framework, as well as general security and privacy sensitivity.
- How will the data flows (exchanges of information) be organised – which data will be shared with whom, for which purposes, and under which safeguards?

These issues are complex to chart in practice**. To facilitate the exercise, CyberSEAS has developed a DPIA template (included in Annex II of this deliverable), which formalises the questions, and which can be used to help complete and structure the responses, and to identify potential challenges**.

5.2.2 Identification of the legal framework and resulting requirements

The second stage is **determining the legal framework that applies and to identify the resulting requirements**. In an EPES context in Europe, this will almost inevitably entail a mix of EU and national level legislation; but in some instances local ordonnances and regulations (such as regional, provincial or communal decisions) may be relevant as well. To identify the legal framework, specialized legal expertise is necessary at a minimum from any location where the project will take place (at a minimum national level expertise; ideally complemented with sector level expertise comprising ICT, energy and administrative law).

Without aiming to be exhaustive, **the section hereunder provides a check list with typical frameworks that can apply to an EPES project.** The application of these frameworks needs to be assessed, and the resulting requirements need to be extracted from the framework, before the use case can be initiated. For more details on the legal obligations resulting from each of these frameworks, we refer to Section 2 of this deliverable:

☐ Data protection law at the EU level (GDPR)

The central question is whether the project involves the processing of personal data, which will usually be the case if data is collected at the household level. If personal data is collected, a legal basis must be identified – often based on contractual obligations, legal obligations, or legitimate interest. A data protection impact assessment will usually be required.

☐ Data protection law at the national level (national rules complementing or specifying the GDPR, and nominating competent data protection authorities)

National laws may impose additional requirements, such as the supervision by a data protection officer, requirements on anonymization or collection of statistics, or prior authorisation.

☐ The Data Governance Act

The Data Governance Act is a useful input to screen whether data sharing may be legally required under public sector information legislation, and/or whether data sharing can occur via secure processing environments or data sharing intermediaries, in order to facilitate data sharing while minimizing legal risks in relation to data protection, confidentiality and intellectual property rights. For 'closed' EPES projects that are inherently limited to one or few operators, this is usually not required.

☐ Information and network security law at the national level (notably national laws transposing the Network and Information Security (NIS) Directives 1 and 2).

Electricity operators can already be designated as providers of essential services under these legal frameworks. Where this is the case, the providers must implement comprehensive risk assessment and risk management strategies. Before proceeding with an EPES project, the operator should assess (i) whether they fall within the scope of such laws; (ii) if so, verify whether their current policies cover the EPES project already; and (iii) if not, amend the risk assessment and risk management practices and documentation before proceeding.

☐ Cybersecurity Act and security certification

The EPES project should verify whether it relies on ICT products that can be or must be certified for their security characteristics. At the time of finalization of this Manual, no applicable security certification scheme has been adopted at the EU level, but this may change over time. For completeness, it should also be assessed whether general (non-security specific) product conformity assessments have been defined at the EU level.

☐ Critical infrastructure protection law at the national level (notably national laws transposing the Critical Infrastructure Protection (CIP) Directive and the Critical Entities Resilience (CER) Directive).

Such national laws will normally require the critical entities to conduct risk assessments and to take measures to mitigate certain foreseeable impacts. The participants in the EPES project should assess (i) whether they fall within the scope of such laws; (ii) if so, verify whether their current policies cover the EPES project already; and (iii) if not, amend the risk assessment and risk management practices and documentation before proceeding. Since this obligation substantively overlaps with the NIS 2 obligations, these efforts should be closely coordinated.

☐ Electricity grid security law at the national level (notably national laws transposing the Electricity Directive, and the Network Code on Cybersecurity for the Electricity Sector.

These laws identify operators that are required to define and formalize cybersecurity risk assessment methodologies and reports, minimum and advanced cybersecurity controls, cybersecurity procurement recommendations, and a cyber-attacks classification scale methodology. If the EPES project involves an operator subject to these requirements, the relevant documentation should be reviewed (or implemented, if not yet available), to ensure that the EPES project is sufficiently covered.

5.2.3 Completing a preliminary DPIA

Under the GDPR, a data protection impact assessment (DPIA) must be conducted whenever "*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 scope and meaning of a DPIA is therefore innately tied to processing of personal data: if no personal data is processed, DPIAs make limited sense (other than as a tool to systematically verify that no personal data processing actually occurs), since no risks to the rights and freedoms of natural persons based on personal data processing can occur.

For this reason, it is advisable to assess at the onset (1) whether any personal data processing is expected to occur in the course of a project; and if so (2) to conduct an initial DPIA to set out initial expectations on risks and mitigation solutions.

5.2.3.1 Will personal data processing occur in the EPES project?

Under the GDPR, personal data includes any data that can be used to identify a specific natural person. Personal data is a broad term under EU data protection law; it comprises not only directly identifiable information (such as names, addresses, contact information, video or audio recordings), but also indirectly identifiable information (such as pseudonymous information where data can only be linked to a specific semantically meaningless number).

Any statement or information regarding a natural person can qualify as personal data, whether it be an objective statement – e.g. remarking on physical traits of a person – or a subjective one – e.g. remarking on a person's behaviour, such as their energy consumption patterns. The information must however 'relate to' a person. This means that it must be "about" that person and, therefore, there must be a relationship between the information and an individual. Lastly, the information must make a person 'identified or identifiable'. An identified person is distinguishable from other members in a group. An identifiable person has not been identified yet but could in principle be identified on the basis of the data. Identification can occur directly – meaning that it is made possible by information directly relating to that person – or indirectly – meaning that multiple pieces of information which do not directly relate to a person can be put together to identify that person. The threshold for putting together such information is any "means reasonably likely to be used".

Personal data must concern a 'natural person'. Information on a company, or on a broad group of electricity users, will therefore not be considered as personal data. Of course, in cases such as one-person companies or households that could be limited to one individual persons, information on such companies or households will include personal data, and the

GDPR will therefore still apply. A natural person must furthermore be alive to be protected by the GDPR - information on deceased people does principally not qualify as personal data.

Pseudonymized information is also personal data. Article 4(5) GDPR defines pseudonymization 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". Pseudonymization is normally reversible, meaning that upon reversal it will be possible to identify a natural person. Only when the pseudonymization is completely irreversible will it no longer be reasonably likely to identify a natural person.

The GDPR however does not apply to anonymous information, "namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable". This means that any kind of information should be assessed on a case-by-case basis to ascertain whether it renders a natural person identified or reasonably likely to be identifiable. Only when the threshold of personal data is not met it be concluded that there is anonymous data falling outside of the scope of the GDPR. This can be the case for large scale energy consumption patterns that cannot reasonably provide information on individual persons, companies or households. However, true and consistently effective anonymization is rare, especially for data that was not aggregated to begin with. Many anonymization techniques can be reversed and can thus result in information that could make a natural personal reasonably identifiable.

If, on the basis of these criteria, personal data will be collected, analysed or otherwise processed, a DPIA should be conducted.

5.2.3.2 Conducting a DPIA

There are many tools and ways to conduct a DPIA in a manner that satisfies the requirements of the GDPR, and most EPES stakeholders will already have their preferred method.

Those that do not may use the template in Annex II as a starting document – while basic and succinct, it has been developed taking into account existing practices and standards in relation to EPES projects.

5.3 Step 2 – Testing, evaluation, adaptation

5.3.1 Phasing

Most projects undergo multiple development and testing steps prior to a go-live. A best practice – where feasible – is to first undergo low risk laboratory testing with fictitious data; to then proceed with medium risk testing using either fictitious data, or very limited quantities of real data; before proceeding to a phased go-live.

- **Low risk piloting activities** include piloting activities that involve only fictitious persons, fictitious data, and test procedures. All three of these requirements must be met, or the piloting activities are qualified as medium risk.
- **Medium risk piloting activities** include piloting activities that involve any one or two of the following factors (but not all three cumulatively, since that would qualify as high risk):
    - Real-life persons
    - Real-life personal data
    - Production environments
- **High risk piloting activities** including piloting activities that cumulatively involve real-life persons, real-life personal data, and production environments.

For the purposes of this Manual:

- Fictitious persons are natural or legal entities which do not exist in real life. The persons are made up for testing purposes (although they should appear credible and some of their characteristics (e.g., their names) could theoretically correspond to real-life persons).
- Fictitious data is any personal data that has been generated for testing purposes in relation to a fictitious person. Fictitious data should appear credible and could theoretically correspond to real-life data but has not been copied from real-life data.
- Test procedures are any procedures that are clearly distinguishable as such by all parties involved in the piloting activities, and which run exclusively on non-production environments - i.e., they cannot result in any legal effects or practical impacts on any real-life persons.
- Real-life persons are natural or legal entities which exist in real life.
- Real-life data is any personal data relating to a real-life person.
- Production environments are any ICT systems (or components thereof) which are used for real-life EPES processes, i.e., processes that can result in legal effects or practical impacts for real-life persons, or that can impact the accuracy or integrity of EPES data and systems.

In low-risk piloting activities, virtually no measures (i.e., technical, legal and organisational measures limiting the impact of the activities on the fundamental rights and freedoms of real persons) must be applied, since no negative impacts can realistically occur in relation to real-life persons, procedures or systems.

In medium-risk piloting activities, some measures apply as will be explained below, since some negative impacts can occur in relation to real-life persons, procedures or systems.

In high-risk piloting activities, it is required to apply more significant measures as will be explained below, since significant negative impacts can occur in relation to real-life persons, procedures or systems.

5.3.2 Risk minimisation - updated DPIA

During this step, risk minimisation measures must be identified and implemented to the maximum possible extent. These should include elements from the following checklist wherever feasible:

☐ **Data minimisation**, including anonymisation and pseudonymisation: the data to be collected and exchanged should be anonymous, aggregate or fictitious wherever possible. Only if this is not feasible, should personal information be used. In these instances, the data should be minimised, including pseudonymised, wherever possible.

☐ **Confidentiality and data sharing**, including by making the data only accessible to persons and systems that strictly require access to achieve the documented goals of the EPES project. Data flows must be documented and strictly controlled.

☐ **Asset qualification.** All assets to be used in the EPES project must be documented and well understood. This is necessary to understand what the risks to be expected are likely to be. The DPIA template in Annex II provides standardized EPES asset classes that can be used for inspiration.

☐ **Risk assessment and mitigation:** plausible incidents and impacts on the relevant stakeholders must be made explicit and documented. The DPIA template in Annex II provides basic risk categories and a list of possible stakeholders that can be used for inspiration.

☐ **DPO supervision**, which includes structural evaluation of the DPIA

5.4 Step 3 – Go-live

A formal go-live on an operational environment involves (i) real users or usage situations, (2) real data, and (3) real infrastructure. SELP risks and obligations are thus substantially higher. With this in mind, prior to a go-live, the project should undergo a full new cycle of verifications with respect to:

☐ **Legal compliance**: deployment outside of lab/testing conditions will trigger new regulatory requirements, in terms of risk assessment, risk mitigation, transparency, and/or prior authorizations. The full list of regulatory frameworks under Step 1 should be revisited and re-assessed, as new and significantly more extensive requirements will usually apply.

☐ **Data collection, data sharing, data analysis frameworks and contracts**: a go-live implies that more, or more sensitive data will be collected, shared and analysed. Appropriate contractual frameworks and policies need to be implemented between all project participants (such as data sharing agreements, data processing agreements, data governance agreements, and so forth). Responsibilities, limitations and liabilities must be explicitly defined a documented before proceeding.

☐ **Information dissemination**: it should be assessed whether the go-live implies activities that users or other stakeholders should be aware of (e.g. as a result of data protection law, consumer protection, or simply because of contractual obligations). If so, the relevant notifications must be made available before proceeding.

☐ **DPIA maintenance**: if a DPIA is required, it should be revisited and updated. It should be reviewed by a duly trained DPO, and approved by management before proceeding.

5.5 Step 4 – Permanent governance and monitoring

For any EPES project, a continuous SELP governance system should be established that performs at least three tasks: project monitoring, community management, and incident management. The following checklist can be used:

☐ **Project monitoring** implies that any changes in the project can be identified and evaluated, notably to determine whether the changes comply with the SELP requirements. The project monitoring team should also monitor changes in the legal framework that trigger

new or changed SELP requirements, and maintain the required documentation to show that the project remains fully in line with the SELP requirements, including by amending the DPIA as needed. It goes without saying that the project monitoring also needs to liaise with domain specific experts as needed to satisfy the legal requirements of the applicable frameworks, and to interact with supervisory bodies, competent authorities and regulators, as needed.

☐ **Community management** ensures transparency and explainability, thus contributing to the trust in the project. It implies:

- ☐ an active component – i.e. making sure that any stakeholders are informed in a proactive and appropriate manner on the planning and progress of the project, e.g. via newsletters, discussion fora, dissemination events, collaborative workshops, and any regulatory notices required (such as privacy policies, terms and conditions, etc).
- ☐ a passive component – i.e. making sure that contact information is available in case of questions from the stakeholders, and that appropriate expertise is available to respond to questions.

☐ **Incident management** is arguably a form of project monitoring since it also is usually required under applicable legislation; but it is listed separately since it is such a crucial component of resilience obligations in EPES. Incident management implies that appropriate channels, teams and procedures are established to make sure that incidents can be detected, reported, analysed and (if required) notified to competent authorities and any other stakeholders. Incident management and data breach notifications are usually obligatory under multiple legal frameworks (GDPR, NIS2, CER, etc.), and this may require multiple different notifications to multiple authorities.

6 Annex II – DPIA template

6.1 DPIA scope and governance

6.1.1 Scope and objectives

This Annex contains a template and process to be used to:

(1) Capture and summarise the key characteristics of any EPES project, including its risks and mitigating measures;

(2) Obtain approval from the SELP Committee prior to initiating the EPES project.

The objective of this Annex is to ensure that each EPES project is conducted in a legally and ethically compliant manner, including in particular from the perspective of data protection law in the European Union as enshrined in the General Data Protection Regulation 2016/679 ("**GDPR**").

6.1.2 Summary of the procedure for approval

1. Prior to initiating an EPES project, the project participants should jointly complete subsections 6.2 to 6.8 of this Annex.
2. Once a draft Annex is internally approved by all the participants in the particular EPES project, the draft Annex can be presented to the SELP Committee for approval.
3. Only when the draft Annex has been approved by the SELP Committee, the EPES project can be initiated.
4. Any challenges, doubts or points of non-compliance, even those raised after the approval of the Annex, should be signalled to the Internal Ethics Committee as soon as reasonably feasible until the end of the project, including any extensions to the project.

6.2 Description of the use case

6.2.1 Intended goals and outcomes of the use case

Describe briefly and concisely what the use case is intended to achieve. In particular, why is data being collected? What is the general goal of the use case?
[free text description]

6.2.2 Date and location of the use case data collection

Planned running dates	[start date – end date]
Location / site 1	[address]
Location / site 2	[address]
Etc.	[address]

Note: this information relates only to the place where data is **collected,** not where it will be **analysed or used** (which may be a different site) for the purposes of the EPES project.

6.2.3 Contact point(s)

For the EPES project in general:

Lead contact person	[name]	[company]	[e-mail address]

If the EPES project is operated across multiple geographical sites, provide a contact person per site:

Location / site 1	[name]	[company]	[e-mail address]
Location / site 2	[name]	[company]	[e-mail address]

6.3 Description of the data to be collected

6.3.1 Description of the profile of persons concerned

Describe briefly and concisely which data will be collected. If it relates to individual persons (including individual households, or their devices/equipment), describe the types of persons.
[free text description]

To which EPES asset classes does the EPES project relate? Tick all that apply.
☐ **Power and Energy System (PES) Components: These assets are mostly tangible and physical in nature. Assets, which are associated to the process zone and component layer of the SGAM architecture, are considered under PES Component asset class. Examples include generator, transmission line, transformers and loads.**
☐ **Information Management (IM) Components: These assets are mostly tangible and physical in nature. Assets, which are associated to the zones field, station, operation, market or enterprise and to the component layer of the SGAM architecture, are considered under IM Component asset class. Examples include relays, PLC, IEDs, physical communication links, routers, gateways, computers and servers.**
☐ **Communication: This asset class is derived by mapping logical communication networks across the SGAM grid plane to the communication layer of SGAM reference architecture. Therefore, such assets are considered under Communication asset class. These assets are mostly intangible and cyber or logical in nature. Examples may include wide area network (WAN),** neighbourhood **area network (NAN) and field area network (FAN).**
☐ **Information: This asset class is derived by mapping various data created and exchanged across the SGAM grid plane to the information layer of SGAM reference architecture. Therefore, such assets are considered under Information asset class. These assets are intangible and cyber in nature. Examples include measurement data, grid data, market data, customer information data, contractual agreements and various databases.**

☐ **Functional: This asset class is derived by mapping various software executing different functionalities across the SGAM grid plane to the functional layer of SGAM reference architecture. Therefore, such assets are considered under functional asset class. These assets can be intangible and cyber in nature. Examples include state estimation programs, SCADA functions, optimal power dispatch programs and aggregation software.**

☐ **Business: This asset class is derived by mapping various policies, processes, procedures and objectives across the SGAM grid plane to the business layer of SGAM reference architecture. Therefore, such assets are considered under business asset class. These assets are mostly organizational in nature. Examples include patching processes, asset management processes.**

☐ **Human: This asset class consists of various personnel involved in different roles across the SGAM grid plane. Therefore, such assets are considered under human asset class. Examples include state network operators, maintenance personnel, customer service personnel and database administrators.**

In your opinion, is any part of the data linkable to individual persons (including individual households, or their devices/equipment)
☐ Yes
☐ No

IF THE ANSWER TO THE QUESTION ABOVE IS 'NO', THE QUESTIONS BELOW ARE INAPPLICABLE, SINCE THEY RELATE TO PERSONAL DATA ONLY. IN THAT CASE, YOU MAY PROCEED DIRECTLY TO SECTION 6.9 OF THIS ANNEX, AND SUBMIT YOUR RESPONSE/ASSESSMENT TO THE ETHICS COMMITTEE. YOU MAY LEAVE THE OTHER QUESTIONS BLANK.

Are some of the persons identifiable as vulnerable? Possibilities include:
☐ Minors (under 18)
☐ Physically impaired persons
☐ Mentally impaired persons

☐ Financially vulnerable persons (e.g. persons who are known to have a lower income)

☐ Other: [free text description]

☐ N.A.: none of the persons can be considered vulnerable, or they are not identifiable as such.

6.3.2 Description of the data concerned

Describe briefly and concisely what kind of data will be collected. The categories below can be used as a starting point, but specify the data enough to make the description meaningful.

General description:

[free text description]

Relevant categories of data:

☐ Basic identity information (name)

☐ Contact information

☐ Family situation (married, children, …)

☐ Financial situation (income)

☐ Energy consumption data

☐ Energy equipment data

☐ Energy usage patterns or profile

☐ Prior incident data

☐ Physical characteristics

☐ Health information prior to the EPES project

☐ Health information during the EPES project

☐ Video imagery during the EPES project

☐ Audio recordings during the EPES project

☐ Geolocation during the EPES project (specific to the individual, not just by inferring where the EPES project takes place)

☐ Other: [free text description]

6.3.3 Estimated number of persons concerned

Provide a best estimate of how many persons are expected to be impacted – i.e. how many persons' data will be collected? If applicable: break down into categories
[free text description]

6.3.4 External recruitment of research participants

Will the EPES project only involve internal persons of the EPES project partners?
☐ Yes, only employees, fixed contractors, directors, etc.
☐ No, also persons who have no permanent link to such **partners**.

6.3.5 Selection criteria

On what basis are the persons selected?
☐ Everyone who is relevant will participate, e.g. all employees working with a particular device or on a particular site
☐ We will preselect persons who are relevant on the basis of the following criteria: [specify]
☐ Only persons who volunteer
☐ Only persons who don't opt out
☐ Other – please specify

6.3.6 Data collection methods

How is data collected?
☐ Self reporting by the participants Self reporting will, however, be limited in the present case to a preparatory interview. ☐ Fully automatic measuring / observation / recording without human intervention during data collection or clean-up ☐ Automatic measuring / observation with human intervention (e.g. to add comments, observations, or clean data) Via video footage and eye-tracking technologies. ☐ Other – please specify

6.4 Description of the intended use of the data, including data sharing

6.4.1 Intended use

Describe briefly and concisely what the EPES project participants plan to do with the data. If possible, indicate which organisation will do what – e.g. X will collect, Y will analyse, Z will provide recommendations, etc.
[free text description]

6.4.2 Intended recipients (data sharing)

Who will obtain access to the raw data (i.e. unprocessed original data, without undergoing any kind of redaction or editing, including any pseudonymization or anonymization)
☐ The site owner

☐ The following EPES project participants: [names or acronyms of the partners]

☐ The following partners who are not directly involved in the EPES project : [names or acronyms of the partners]

☐ The following service providers who are not EPES project partners [specify name and role – e.g. data collection services, data analysis, researchers]

☐ The persons whose data is being collected (if they request it)

☐ Other – please specify

Will the data be sent to a destination (a company or infrastructure) located outside the European Economic Area (i.e., the EU Member States, Iceland, Liechtenstein or Norway)?

☐ No

☐ Yes : [specify the countries and reason for transfer]

6.4.3 Anonymisation or pseudonymisation (if any)

Will the data be anonymised or pseudonymised at any stage?

Anonymisation means that it is impossible to link data back to a person, irrespective of who is trying to re-link the data. Fully statistical data is typically anonymous.

Pseudonymisation means that the data cannot be directly linked to a person by the recipient, but it could still be linked back to the person with assistance from another party than the recipient. E.g. blurred video images or gait analysis data without direct identifiers referring to the person would qualify.

If either box is ticked, specific when and why the process is used (e.g. prior to sharing it with other EPES project participants, to allow analysis without easy identification of the participants).

☐ The data is anonymised using the following approach: [specify]

☐ The data is pseudonymised using the following approach:

6.4.4 Intended retention

For how long will the data be kept?
☐ For the duration of the EPES project; then it will be deleted or anonymised (as defined in the preceding question).
☐ For a fixed duration beyond the EPES project: [specify the term, e.g. x years after the end of the EPES project]
☐ For a different duration: [specify expected date or criterion]

Who will keep the data?
☐ The site owner
☐ The following EPES project participants: [names or acronyms of the partners]
☐ The following partners who are not directly involved in the EPES project [names or acronyms of the partners]
☐ Others: [free text description]

6.5 Potential risks for the persons concerned

Describe briefly and concisely what the potential risks are for the persons concerned, taking into account the measures that you will implement – i.e. it is not necessary to report theoretical risks that you've eliminated because of the measures you've taken. The categories below can be used as a starting point, if desired.

☐ Energy outages
☐ Reputational risks
☐ Financial risks
☐ Physical health risk
☐ Mental health risk (increased risk of stress, anxiety, discomfort)
☐ Other – please specify

Are there risks to third parties (persons other than the person whose data is collected)? If so, please elaborate.

☐ Other household members of the person
☐ Visitors of the person
☐ Site visitors
☐ Other – please specify

6.6 Lawfulness of the processing (including consent)

The EPES project will proceed on the basis of:

☐ **Consent**. This implies that persons have the free choice not to participate, volunteer to do so, and can withdraw their consent at any time. This option is **not available when collecting data of employees**, since they are legally presumed to be subject to pressure to consent.

☐ The **necessity to process the data for the performance of a contract** between the person concerned and the organisation collecting the data.

☐ The **necessity to process the data for compliance with a legal obligation** of the organisation collecting the data.

☐ The **necessity to process the data to protect the vital interests of individual natural persons.**

☐ The **legitimate interest** of the organisation collecting the data. **This box should be ticked when employees are involved**, or when the options above are not available.

6.7 Transparency towards the persons concerned

The following measures are taken to ensure transparency to the persons concerned:

☐ They are provided with an information sheet in a language that they understand, using terminology that the person concerned will understand.

☐ They are given an additional spoken explanation by the organisation(s) collecting the data, and invited to ask any questions for clarification.

☐ They can opt out at any time, and may ask that their data is deleted.

☐ They are allowed to ask for a copy of their data until it is deleted or fully anonymised.

6.8 Mitigation and protection measures taken

The following measures are taken prior to initiating the EPES project (in addition to obtaining approval of the SELP Committee):

☐ There is a prior consultation with representatives of the persons concerned

☐ There is a separate approval procedure (in addition to obtaining approval of the SELP Committee): [specify]

☐ The EPES project will use certified or audited technologies: [specify]

☐ The EPES project will be executed under the supervision of a DPO: [provide contact details]

☐ The EPES project will be executed under the supervision of another qualified and independent professional, such as a CIO or ombudsman

☐ Data will be anonymised prior to sharing it with third parties

☐ Data will be pseudonymised prior to sharing it with third parties

☐ Access control measures are in place to ensure data can only be accessed by specifically mandated persons

☐ Logging measures are in place to ensure data access or use (including modification or deletion) can be detected

☐ All research data will be encrypted and stored on a password protected system or in a secure location

☐ All researchers are competent to carry out the research and have received appropriate training.

☐ All researchers are aware of their confidentiality obligations

☐ Appropriate insurance and indemnity is in place for this research, at all participating sites and for each investigator.

☐ Other – please specify

6.9 Approval process and log

6.9.1 Application submission

Applicant's Name	Version number of the application, and date of submission for approval	Applicant's signature

6.9.2 Application process and log

Phase	Date	Action or decision
Feedback from the Ethics Committee (if any)		
Resubmission (if any)		
Approval by the Ethics Committee		

6.9.3 Application approval by the Ethics Committee

Committee Member's Name	Version number of the application, and date of approval	Committee Member's signature

If any part of the EPES project changes in a manner that raises doubts on the completeness or accuracy of this description, or that causes ethics or compliance doubts, the opinion of the Ethics Committee should be sought.

7 References

Ref. 1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), http://data.europa.eu/eli/reg/2016/679/oj

Ref. 2. CyberSEAS, H2020- 101020560, Grant Agreement, 2021.

Ref. 3. Article 29 Data Protection Working Party, Guidelines WP 248 rev.01 on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, adopted on 4 October 2017, https://ec.europa.eu/newsroom/article29/items/611236

Ref. 4. Opinion 4/2007 on the concept of personal data, WP 136, adopted on 20 June 2007, see https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

Ref. 5. Responsible research and innovation - Europe's ability to respond to societal challenges, European Commission - DG Research and Innovation, 2012; see https://op.europa.eu/en/publication-detail/-/publication/bb29bbce-34b9-4da3-b67d-c9f717ce7c58/language-en

Ref. 6. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act); see https://eur-lex.europa.eu/legal-content/EN/TXT/?pk_campaign=todays_OJ&pk_content=Regulation&pk_keyword=data+governance+act&pk_medium=TW&pk_source=EURLEX&uri=CELEX%3A32022R0868

Ref. 7. Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European strategy for data, COM/2020/66 final.

Ref. 8. 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, OJ L 194 of 19.7.2016; see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L1148

Ref. 9. 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); see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019R0881

Ref. 10. Communication from the Commission of 12 December 2006 on a European Programme for Critical Infrastructure Protection, COM/2006/786 final.

Ref. 11. Council Directive 2008/114 of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection; see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008L0114

Ref. 12. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC; see https://eur-lex.europa.eu/eli/dir/2022/2557/oj

Ref. 13. Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU; see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.158.01.0125.01.ENG&toc=OJ:L:2019:158:TOC

Ref. 14. Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity; see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.158.01.0054.01.ENG&toc=OJ:L:2019:158:TOC

Ref. 15. Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC; see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.158.01.0001.01.ENG&toc=OJ:L:2019:158:TOC

Ref. 16. Regulation (EU) 2019/942 of the European Parliament and of the Council of 5 June 2019 establishing a European Union Agency for the Cooperation of Energy Regulators; see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.158.01.0022.01.ENG&toc=OJ:L:2019:158:TOC

Ref. 17. EU Charter of Fundamental Rights; see https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights_en

Ref. 18. Directive on measures for high common level of cybersecurity across the Union (NIS2 Directive); see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555

Ref. 19. Network Code on Cybersecurity for the Electricity Sector (Commission Delegated Regulation (EU) 2024/1366 of 11 March 2024 supplementing Regulation (EU) 2019/943 of the European Parliament and of the Council by establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows); see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL_202401366

Ref. 20. EU register of data intermediation services; see https://digital-strategy.ec.europa.eu/en/policies/data-intermediary-services

Ref. 21. October 2023 report on a Common European Energy Data Space; see https://op.europa.eu/en/publication-detail/-/publication/43b8d2d1-6975-11ee-9220-01aa75ed71a1/

Ref. 22. Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC); see https://eur-lex.europa.eu/eli/reg_impl/2024/482

Ref. 23. Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (Cyber Resilience Act); see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0454