

Comprehensive Governance Models for Energy Data Spaces: A Path to Secure and Interoperable Data Sharing in Europe

Aleksandr Egorov, Kamalanathan Ganesan, Gonçalo Glória, Raquel Segurado Silva, Nuno Souza e Silva
R&D NESTER
Sacavém, Portugal,
aleksandr.egorov@rdnester.com

Uršula Krisper
Elektro Ljubljana
Ljubljana, Slovenia

Abstract—Effective governance models for energy data are essential to support Europe’s strategic objectives in data sharing, trust, and interoperability. Building on initiatives like the Data Governance Act and the European Data Strategy, the ENERSHARE project develops a Data Space for the energy sector, introducing comprehensive Governance Models to address complex data-sharing requirements. This paper outlines eight interconnected models for managing energy-related data from metering, consumption, generation, and distribution systems across diverse contexts. These models emphasize security, compliance, data portability, and stakeholder lifecycle management, forming a robust framework for transparent and secure data exchange. Driven by a gap analysis of existing frameworks and structured surveys with key stakeholders, this approach reflects current needs while aligning with European regulations and fostering market innovation. By supporting both decentralized and centralized architectures, the Governance Models foster collaboration among TSOs, DSOs, data providers, and energy communities, ensuring data integrity, trust, and strategic progress.

Index Terms— Data Management, Data Space Interoperability, Energy Data Governance Models, Regulatory Compliance, Secure Data Sharing.

I. INTRODUCTION

Energy Data Spaces (EDS) offer significant potential for integrating diverse energy resources, optimizing consumption patterns, and driving innovation across Europe’s energy markets. However, the absence of consistent governance frameworks, especially in areas like data security, consent management, interoperability, and stakeholder coordination, continues to create challenges for secure and efficient data exchange. While legislative frameworks such as the General Data Protection Regulation (GDPR) [1] and the Data Governance Act [2] aim to address these issues, practical implementations often reveal gaps in defining roles, clarifying data ownership, establishing trust among participants, and aligning technical standards, as will be described in the Chapter II.

To address these governance challenges, the paper introduces a systematic approach specifically designed to the energy sector. An in-depth analysis of questionnaires gathered from pilot projects was conducted involving both regulated and non-regulated entities. This allowed to identify key practices, needs, and difficulties related to data sharing in real-world scenarios. Based on these findings, a set of Governance Models designed to ensure clear responsibilities, compliance with EU regulations, and seamless interoperability was developed. In the subsequent sections, the primary obstacles encountered in energy data sharing are explored and an explanation is provided on how the proposed models offer a practical solution for creating secure and interoperable Energy Data Spaces.

II. CURRENT INITIATIVES AND CHALLENGES IN ENERGY DATA SHARING AND INTEROPERABILITY

EDS in Europe refer to digital eco-systems that facilitate secure and efficient sharing of energy-related data among various stakeholders in the energy sector. These spaces are designed to enable integration of different energy sources with energy-related entities, optimize energy management, and foster the development of innovative energy services. In Europe, EDS has gained significant attention as a key component of the energy transition and the digital transformation of the energy sector. Several initiatives and projects [10] [11] [12] [13] [14] [15] [16] [17] have emerged in Europe to promote the concept of Energy Data Spaces and facilitate data sharing in the energy domain, by recognizing the importance of data and digital technologies in achieving these objectives and emphasizing the need for secure and standardized data sharing mechanisms. This analysis serves as a starting point for further development of governance models in energy data ecosystems, focusing on the conceptual and technical structures that help ensure data is handled according to well-defined rules. For a secure, trusted, and continuous operation of EDS, the governance layer must be addressed for all components in the data life cycle, aiming not only at a detailed and comprehensive view of data management processes but also at guaranteeing that these processes follow

rules established through policies, procedures, and accountabilities. Governance is thus the exercise of authority and shared decision making that distinguishes the mere existence of data from a system in which data is truly managed.

Several key pieces of EU legislation affect data sharing in the energy domain. GDPR [1] is the main piece of EU legislation regulating personal data processing in all sectors, requiring obligations for lawfulness, consent, transparency, accountability, and data protection by design and by default. Data Governance Act [2] sets out rules for the reuse and resharing of public sector data, introduces the category of data altruism, and defines data intermediation services for establishing commercial relationships among data subjects, data holders, and data users. Commission Implementing Regulation (EU) 2023/1162 on interoperability requirements for access to metering and consumption data in the electricity sector [3] specifies how customers and eligible parties can access validated and non-validated data in a non-discriminatory manner, ensuring secure data exchange, clarity of roles, and technical procedures for interoperability. Digital Services Act [4] contains horizontal provisions for intermediary services that could apply to energy data spaces if they function as online platforms. Proposed legislation such as the AI Act [5] and the Data Act [6] will likely add new obligations for how artificial intelligence systems and Internet-of-Things devices process data, with particular emphasis on risk-based requirements and fair data usage. Concurrently, existing laws and directives are undergoing review. The ePrivacy Regulation [7], intended to replace the current ePrivacy Directive [8], is still under negotiation. The NIS 2 Directive [9] has expanded its scope to include more entities and to impose broader obligations for cybersecurity. In the future, additional sector-specific legislation may arise, for instance regarding cybersecurity requirements for energy systems or the governance framework for an energy data space, similar to the approach taken with the European Health Data Space. In this legal context, organizations implementing energy data spaces must address each applicable rule, remain flexible enough to adapt to forthcoming changes, and ensure continuous monitoring of legislation at EU and national levels.

Alongside these legislative frameworks, various initiatives and projects have contributed to defining architectures, roles, and best practices for energy data spaces. The International Data Spaces Association (IDSA) [10] has developed the IDS Reference Architecture Model, which includes a set of layers (business, functional, process, information, and system) along with three overarching perspectives on security, certification, and governance. GAIA-X [11] provides a federation framework aimed at ensuring European values such as openness, transparency, data protection, and portability, encouraging collaboration among cloud and data service providers. FIWARE [12] promotes open-source solutions and open standards, particularly through Smart Data Models that enable semantic interoperability in IoT-based applications. OPEN-DEI [13] has proposed design principles for data spaces that focus on data sovereignty, ensuring data owners maintain control over how their data is utilized, a data level playing field where competition is based on excellence rather than monopoly over data, the concept of decentralized soft architecture rather

than a monolithic system, and public-private governance that represents a wide range of stakeholders. OneNet [14] is an important project in which a fully replicable and scalable data exchange architecture is tested for the entire European electrical system, combining a decentralized approach with cross-platform interoperability while enforcing data ownership, privacy, trust, and security. BD4NRG [15] similarly addresses big data applications in the energy sector, employing DLT-based mechanisms for data sovereignty and governance that integrate IDSA [10] and GAIA-X [11] conceptual architectures. BRIDGE [16] is an initiative that brings together numerous Horizon 2020 and Horizon Europe Smart Grid and Energy Storage projects, coordinating working groups on data management, business models, regulations, and consumer engagement. A key product is the Data Exchange Reference Architecture (DERA), which builds on the Smart Grid Architecture Model and addresses five interoperability layers: business, function, information, communication, and component. Although governance is not fully covered in the current DERA report, it is expected to be addressed in more detail in future versions. The Living Energy lab initiative [17] further exemplifies approaches for collecting and analyzing energy consumption data in real-life contexts, handling participants' data in a secure manner while providing data-driven benefits and incentives for end users.

Despite this progress, certain gaps in data governance must still be addressed. One important gap concerns the precise distinction of roles for data ownership, provision, consumption, and usage. Many platforms focus on entities participating directly in the data space, without clarifying how external entities that do not directly join might still own or use the data. This omission can create confusion regarding the confidentiality and security of data transferred to or from third parties. Another gap relates to the issue of confidentiality and access consent, since the different roles often lack clearly defined or systematically implemented policies for specifying which data points are confidential or public, how consent is granted, revoked, or managed, and how long data can be lawfully retained or processed. Licensing and policy agreements among participants may not be comprehensively formalized, and such arrangements become especially relevant when regulated stakeholders like Transmission or Distribution System Operators (TSOs or DSOs) share data with unregulated ones such as retailers or energy communities. Logging and tracking of data, although recognized as important, remains underspecified in several reference architectures, which only generically acknowledge traceability without defining the exact methods, metadata, and procedures needed to maintain meaningful audit trails. Another persistent gap lies in interoperability and portability. Many initiatives adopt partial solutions or provide abstract guidelines, but they often do not thoroughly ensure that data exchanged within a project can be reused seamlessly in subsequent projects or by new data platforms. Tied to this is the topic of replicability, which entails guaranteeing that data quality, data models, and communication protocols support expansions, upgrades, or parallel developments of energy data services. Finally, general alignment across domains is a challenge. Projects like OPEN-DEI [13] encourage cross-sector interoperability, but energy data spaces must handle significant regulatory differences and

specialized data types (for instance real-time consumption data or grid operation parameters), which complicates straightforward integration with other sectors. These shortcomings highlight the need for a comprehensive governance framework that systematically incorporates clarity in roles, confidentiality requirements, contractual mechanisms for data licensing, robust logging and provenance solutions, and rigorous criteria for interoperability, portability, and replicability. By addressing these gaps, energy data spaces can better align with existing EU legislation, integrate with diverse platforms and stakeholders, and accelerate progress toward efficient and secure data-driven services in Europe’s energy landscape.

III. PROPOSED GOVERNANCE MODELS FOR ENERGY DATA SPACES

The ENERSHARE project [18] has developed two questionnaires for gathering information from the pilot implementations about their data sharing practices, data sets, and overall readiness to participate in a data space environment. These questionnaires were intended to align pilots from Spain, Portugal, Slovenia, Italy, Finland and Latvia on a common level of understanding and to supply the necessary inputs for defining governance models. The first questionnaire (Q1) was composed of eleven questions, covering details such as data ownership, data security, consent and access control, data flow, and logging and tracking of the data, as well as interoperability, portability, and standardization. The second questionnaire (Q2) aimed to clarify additional aspects of identity management, governance authority, onboarding and offboarding of participants, and the extent to which a pilot already meets the definition of an integrated data space.

The main idea of Q1 was to collect structured information about the data sets and services that each pilot expects to implement and test within the project. This included identifying whether they were dealing with personal or non-personal data, whether data security measures such as Transport Layer Security (TLS) encryption or certificate-based authentication were used, and whether consent practices followed confidentiality requirements. Many pilots focused on regulated data (collected or processed by TSOs, DSOs, or public-sector entities) alongside non-regulated data, such as from consumers, prosumers, or retail companies. Responses also described data flows, distinguishing the source and final destination of data, whether the communication was end-to-end or platform-based, and whether local storage was involved. The importance of logging and tracking, where logs record information about data usage and any incidents, was highlighted by all pilots to ensure traceability and compliance with internal policies or external regulations. Q1 also inquired about interoperability and data portability in order to confirm whether standardized or open formats were adopted. Various data formats like JSON (JavaScript Object Notation), CSV (Comma-Separated Values), or XML (eXtensible Markup Language) were reported as being used, although the actual readiness for cross-project replication or reusability of the data was not always fully specified.

Q2 posed a smaller number of questions but with more detailed queries on the data space environment as a whole. Pilot representatives were asked if their pilot had already established an integrated data space with certain essential characteristics, such as a data platform for sharing and exchanging data, a data marketplace building block for publishing or discovering data and applications, and a federated identity management system that governed both individuals and technical connectors. Q2 responses revealed that identity management is predominantly realized through an Identity Provider solution, sometimes based on recognized approaches like International Data Spaces (IDS) connectors or Keycloak, with each pilot acknowledging that the formal governance authority and the final set of governance rules would be established later in the project. Nevertheless, the pilots confirmed that data provider and data owner rights, as well as data consumer obligations, are recognized and will be respected through contractual agreements and access-control mechanisms. The responses additionally clarified participants’ planned procedures for onboarding (including training, establishing access permissions, and participating in security briefings) and offboarding (revocation of privileges and secure data deletion or transfer). Although not all pilots were operating a fully formed data space, the questionnaires made it apparent that the fundamental components for a governance framework are already under consideration.

Below follows the set of governance models that were created as a direct result of analysing the pilots’ responses to Q1 and Q2 and taking into account previously identified gaps and core principles for energy data sharing. Each governance model includes a detailed description of the motivation and scope, followed by a set of rules or requirements that any participant in the data space must abide by. These governance models also clarify what responsibilities fall under a governance authority or equivalent role that may be established to monitor compliance, resolve disputes, and coordinate the evolution of the data space’s rules.

Each governance model is closely tied to one of the fundamental aspects of data sharing and exchange. The Governance Framework, consisting of eight governance models, is presented in Figure 1.

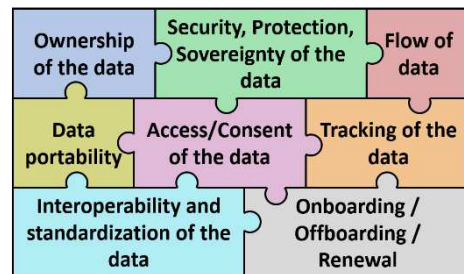


Figure 1. Governance Framework with eight Governance Models

The text is structured to address data ownership, security, protection, and sovereignty, consent and access, data flow, tracking and logging, interoperability and standardization, data portability, and finally onboarding/offboarding procedures. It also touches on the usage of applications for data flow and the broader set of governance policies and key actors. Overall, each governance model should be regarded as a set of

requirements for any organization wishing to join and participate in the data space, and as a blueprint for a governance authority that must enforce these obligations for the sake of a stable, secure, and trustworthy data ecosystem.

A. *Ownership of the data*

The first governance model focuses on ownership of the data and highlights that data ownership is a critical component of data governance, as it encompasses accountability and responsibility for data. It involves clearly identifying who owns the data, who is responsible for managing it, and who is authorized to access it. Data owners are accountable for the data in their domain, ensuring its accuracy, reliability, and security. They are expected to define data policies for quality, security, and access, and to oversee data protection measures that prevent unauthorized access. Data providers manage data on behalf of the owners, delivering accurate, complete, and reliable data that meets the standards set by data owners. They must transmit and store data securely, align with data owners' policies, and provide timely updates. Data custodians are responsible for storing, managing, and protecting data by ensuring regular backups, recovery plans, and adherence to data security requirements. Data users are individuals who access data as part of their roles. They must use data ethically and responsibly, follow the governance rules set by the owners and custodians, and report any issues with data quality or security. By clarifying these roles, the governance model for ownership ensures that each participant understands the scope of their obligations and that accountability is built into all stages of data handling.

B. *Security, protection, and sovereignty of the data*

The second governance model deals with security, protection, and sovereignty of the data. It underscores how data classification, access control, risk management, policy development, and incident response collectively form a framework that safeguards sensitive information. The classification of data, such as differentiating between personal and non-personal or between open/public and confidential, forms the foundation for selecting the appropriate level of protection. To secure data, participants must enforce communication channels such as TLS encryption or other secure transport mechanisms, implement device authentication or certificate-based authentication, and control user registration through recognized identity management processes. Data sovereignty ensures that organizations, governments, and individuals maintain control over how their data is collected, stored, shared, and used. It spans a spectrum, balancing the need to protect data with the need to share it for deriving value. The model addresses requirements to maintain logs, conduct risk assessments, comply with relevant legislation (such as GDPR [1]), and follow recognized data security governance frameworks. Furthermore, the sovereignty dimension ensures that data owners have the ultimate say over how their data is processed, which fosters trust among different stakeholders in the data space.

C. *Access / Consent of the data*

The third governance model focuses on access and consent of the data. It explains that data access governance involves

policies that limit data usage to trusted individuals, relying on identity management, authentication, and authorization. In situations where personal data is involved, consent must be freely given, specific, informed, and unambiguous, although the GDPR [1] provides several additional legal grounds for data processing that may not require consent. The model stipulates how confidentiality levels (public, confidential, and restricted) should be handled, specifying that public data can be made available read-only under a suitable agreement, whereas confidential or restricted data can involve read or write permissions limited by formal agreements. Consent rules, combined with identity management, define who can connect to the data space, under what conditions, and for how long data can be processed. These rules are essential to create a trusted environment in which data usage policies can be properly enforced.

D. *Flow of data*

The fourth governance model addresses the flow of data. It highlights that any participant collecting or transferring data must define the data's starting point, final destination, and whether the flow is unidirectional or bidirectional. This also entails documenting the presence of local storage, which can affect how and where data is temporarily or permanently retained. The primary goal is to remove ambiguity about how data travels from source to endpoint within a complex ecosystem that may include multiple platforms, devices, and services. By requiring each participant to describe the data flow in this structured manner, the data space avoids mismatches or misunderstandings when integrating new datasets or services. This is of particular importance in scenarios where regulated energy data is exchanged with non-regulated domains, allowing clarity in responsibilities for data integrity, timeliness, and possible updates.

E. *Tracking of the data*

The fifth governance model concerns tracking of the data, which includes gathering information on data processing, transformations, and data paths. Tracking must consider whether data contains different data formats, how it flows between endpoints, and whether any conversions occur along the path. ENERSHARE [18] pilots often combine both time-series (dynamic) and static data to support energy-related services. This model introduces the concept of logs, provenance, and traceability, typically associated with a Clearing House function. The Clearing House records data transactions, enforces policies, and monitors usage for billing or dispute resolution. Each participant is required to implement logging mechanisms that capture these data interactions in detail, which must be preserved in a secure manner. Traceability is vital for accountability, and logs must remain sufficiently detailed to prove compliance with regulations, contractual agreements, or governance frameworks. This ensures that if a security incident or conflict arises, there is reliable evidence of how data was handled.

F. *Interoperability and standardization of the data*

The sixth governance model addresses interoperability and standardization of the data, emphasizing that technical, semantic, and governance interoperability are essential for

ensuring that data from various systems can be exchanged and understood in a consistent way. The model highlights that data spaces require alignment with recognized standards such as Smart Appliances REFERENCE ontology (SAREF) [19], the Common Information Model (CIM), IEC 61970, IEC 61850, or others, as well as the adoption of a common ontology for describing data. A Vocabulary Hub can be introduced to list approved vocabularies, store information on the meaning and structure of data, and allow participants to validate their data against shared models. Collaboration among participants is crucial to maintain these vocabularies over time. Without active collaboration, a vocabulary can become fragmented as each stakeholder adds local variations. By consistently adopting and maintaining standardized data formats and semantic definitions, the energy sector avoids siloed solutions and fosters a landscape in which cross-platform integration becomes more straightforward.

G. *Data portability*

The seventh governance model is about data portability. It ensures that data can be moved from one environment, application, or cloud service to another without losing its meaning or structure. Within the ENERSHARE [18] pilots, data portability has been achieved through the adoption of structured and machine-readable formats such as CSV, XLSX, JSON, and XML. This practice reduces vendor lock-in and helps new services or applications integrate existing datasets more easily. The governance model requires participants to follow certain standardization guidelines for data formats, guaranteeing that the process of transferring data from or to the data space is facilitated and consistent. Ultimately, data portability empowers participants to collaborate in flexible ways, adapt to changing market conditions, or replicate solutions across projects without incurring excessive overhead.

H. *Onboarding/Offboarding/Renewal*

The eighth governance model covers onboarding, offboarding, and renewal. It defines how new participants, whether data owners, data managers, or data consumers, are introduced to the data space. Onboarding must be structured so that roles and responsibilities are clearly identified, access permissions are properly assigned, and participants are well-informed of data security protocols. The process can be codified in an Accession Agreement that stipulates the terms and conditions for data usage, clarifies any contractual requirements, and ensures that all relevant compliance checks are carried out. Offboarding is similarly governed by a formal procedure. When a participant leaves the data space, their credentials are revoked, data may be archived or deleted as appropriate, and any responsibilities for ongoing data usage or maintenance of logs are transferred or concluded. Offboarding is crucial for preventing unauthorized access after an entity has ceased to participate. Renewal is a mechanism for existing participants to reaffirm or update their roles, responsibilities, and access permissions at set intervals, reflecting continuous improvement and alignment with updated governance requirements. This governance model ensures that the overall lifecycle of participant interactions is transparent, secure, and adaptable, minimizing disruptions caused by entry or exit events and maintaining trust in the data space.

Although not always a standalone model, the usage of applications for the data flow is also acknowledged as an integral part of energy data spaces. In practice, data spaces often include a control phase, where data exchange contracts and data assets are negotiated, and an operational phase, where data transfer is mediated by applications, connectors, or dedicated APIs. This approach aligns with recognized protocols, such as Next Generation Service Interfaces - Linked Data (NGSI-LD) for data transfer or the Dataspace Connector for contract negotiation and enforcement. Finally, the governance policies and key actors must be clearly identified to ensure that everyone in the data space understands how decisions are made and which policies prevail. Data governance policies typically address data quality, privacy, security, lifecycle management, and data ethics. In the ENERSHARE project [18] context, with regulated and non-regulated entities operating together, it is important to define which entity or collection of entities exercises authority over disputes, ensures compliance, and steers the evolution of the data space rules. By adopting these governance models, participants can establish trust in the data space's operations, while also benefiting from secure, interoperable, and adaptable data services that enable efficient integration of energy resources and innovations.

IV. CONCLUSION

This paper provides an in-depth analysis of the current challenges in energy data sharing and suggests a set of detailed Governance Models designed for Europe's evolving Energy Data Spaces. It starts by addressing the obstacles posed by complex legal requirements, fragmented responsibilities, and the absence of well-defined policies regarding roles and data handling. These issues emphasize the critical need for robust governance mechanisms that ensure security, ownership clarity, and seamless interoperability. Insights from extensive questionnaires applied to pilot implementations reveal how variations in data formats, privacy requirements, and participant profiles further highlight the necessity of a unified framework.

Eight Governance Models are then presented, each addressing a particular area of data management. These models cover topics such as clarifying data ownership, ensuring security, maintaining control over data, and managing consent. They also outline rules for data flow, tracking, interoperability, portability, and the process of participant onboarding or offboarding. By combining these models, the paper offers a structured approach to ensure compliance with EU legislation, foster trust among regulated and non-regulated entities, and promote seamless data exchange. When implemented together, these models act as a unified guide for building secure, interoperable, and future-proof Energy Data Spaces across various operational contexts.

ACKNOWLEDGMENT

This work has been funded by the European project ENERSHARE (HEU Grant Agreement No. 101069831).

REFERENCES

Periodicals:

- [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) [2016] OJ L 119, 4.5.2016, p. 1–88.
- [2] 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) [2022] OJ L 152, 3.6.2022, p. 1–44.
- [3] Commission Implementing Regulation (EU) 2023/1162 of 6 June 2023 on interoperability requirements and non-discriminatory and transparent procedures for access to metering and consumption data [2023] OJ L 154, 15.6.2023, p. 10–40.
- [4] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L 277, 27.10.2022, p. 1–102.
- [5] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS [2021] COM/2021/206 final
- [6] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act) [2022] COM/2022/68 final
- [7] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) [2017] COM/2017/010 final - 2017/03 (COD)
- [8] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L 201, 31.7.2002, p. 37–47
- [9] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) [2022] OJ L 333, 27.12.2022, p. 80–152
- [10] “International Data Spaces Association (IDSA)”, 2017, <https://internationaldataspaces.org/>
- [11] “A Federated Secure Data Infrastructure (GAIA-X)”, 2020, <https://gaia-x.eu/>
- [12] “A curated framework of Open Source Platform components to accelerate the development of Smart Solutions (FIWARE)”, 2016, <https://www.fiware.org/>
- [13] “The digital transformation of European industry (OPEN DEI)”, 2019, <https://www.fiware.org/project/open-dei.html>
- [14] “One Network for Europe (OneNet)”, 2020, <https://www.onenet-project.eu/>
- [15] “Big Data for Next Generation Energy (BD4NRG)”, 2021, <https://www.bd4nrg.eu/>
- [16] BRIDGE initiative, 2016, <https://bridge-smart-grid-storage-systems-digital-projects.ec.europa.eu/home>
- [17] “A Living Lab to design tomorrow’s energy (Living Energy lab initiative)”, 2017, <https://www.smartenergylab.pt/living-energy/>
- [18] “The Energy Data Space for Europe (ENERSHARE)”, 2022, <https://enershare.eu/>
- [19] “The Smart Applications REFERENCE Ontology (SAREF)”, 2014, <https://saref.etsi.org/>