Enershare

The Energy Data Space for Europe

# European Common Energy Data Space Framework Enabling Data Sharing - Driven Across – and Beyond – Energy Services

enershare.eu

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

# D7.1 ENERSHARE governance models and participatory business models

**Alpha version**

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

## Publication details

| | |
|---|---|
| Grant Agreement Number | 101069831 |
| Acronym | ENERSHARE |
| Full Title | European Common Energy Data Space Framework Enabling Data Sharing-Driven Across — and Beyond — Energy Services |
| Topic | HORIZON-CL5-2021-D3-01-01 ‘Establish the grounds for a common European energy data space’ |
| Funding scheme | HORIZON-IA: Innovation Action |
| Start Date | Jul 1, 2022 |
| Duration | 36 months |
| Project URL | enershare.eu |
| Project Coordinator | Engineering |
| Deliverable | D7.1 ENERSHARE governance models and participatory business models (1st version) |
| Work Package | WP7 – Data Space and data sharing governance and business models |
| Delivery Month (DoA) | M12 |
| Version | 1.0 |
| Actual Delivery Date | August 3, 2023 |
| Nature | R – Document, report |
| Dissemination Level | PU |
| Lead Beneficiary | 15 – NESTER |

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

| | |
|---|---|
| Authors | Nuno Fulgêncio (NESTER)<br>Alexandre Gouveia (NESTER)<br>Gonçalo Glória (NESTER)<br>Aleksandr Egorov (NESTER)<br>Ursula Kripser (EKL)<br>Ricardo Jorge Bessa (INESC TEC)<br>Gabriela Bodea (TNO)<br>Sonia Jimenez (IDSA)<br>Gregor Cvet (KPV)<br>Rui Martins (SEL) |
| Quality Reviewer(s) | Ricardo Bessa (INESC TEC)<br>Ursula Krisper (EKL) |
| Keywords | Data governance models, Business requirements, Data sharing incentives |

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

## Document History

| Ver. | Date | Description | Author | Partner |
|---|---|---|---|---|
| 0.1 | 22.03.2023 | ToC | Nuno Fulgêncio<br>Alexandre Gouveia<br>Gonçalo Glória | NESTER |
| 0.2 | 23.06.2023 | Draft | Nuno Fulgêncio et al. | All WP7 partners |
| 0.3 | 17.07.2023 | Consolidated version with comments | Aleksandr Egorov et al. | All WP7 partners |
| 0.4 | 24.07.2023 | Revised version | Aleksandr Egorov et al. | All WP7 partners |
| 0.5 | 26.07.2023 | Final version for internal review | Aleksandr Egorov et al. | All WP7 partners |
| 1.0 | 02.08.2023 | Final version after internal review | Aleksandr Egorov et al. | All WP7 partners |

Disclaimer

The sole responsibility for the content of this publication lies with the authors. It does not necessarily reflect the opinion of the European Union. Neither the CINEA nor the European Commission is responsible for any use that may be made of the information contained therein.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

# Table of Contents

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

# List of Figures

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

# List of Tables

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

# List of Acronyms

| | |
|---|---|
| ABAC | Attribute-Based Access Control |
| AI | Artificial intelligence |
| AMI | Advanced Metering Infrastructure |
| API | Application Programming Interface |
| B2B | Business-to-Business |
| CGMES | Common Grid Model Exchange Specification |
| CIM | Common Information Model |
| COSEM | Companion Specification for Energy Metering |
| CRM | Customer Relationship Management |
| DAP | Data Access Policies |
| DEB | Data Exchange Board |
| DEP | Data Exchange Platform |
| DER | Distributed Energy Resources |
| DERA | Data Exchange Reference Architecture |
| DG | Data Governance |
| DGA | Data Governance Act |
| DLC | Distribution Line Carrier |
| DSA | Data Space Authority |
| DSA | Digital Services Act |
| DSO | Distribution System Operator |

| | |
|---|---|
| eblX | Energy Business Information eXchange |
| EBSI | European Infrastructure for Blockchain Services |
| EC | European Commission |
| EDMS | Energy Data Management System |
| EDS | Energy Data Spaces |
| EHDS | European Health Data Space |
| EMS | Energy Management System |
| ENTSO-e | European Network of Transmission System Operators for Electricity |
| ESMP | European Style Market Profile |
| ESO | European Standardisation Organisation |
| EU | European Union |
| EV | Electric vehicle |
| FI-PPP | Future Internet Public-Private Partnership Program |
| GDPR | General Data Protection Regulation |
| GE | Generic Enabler |
| HDFS | Hadoop Distributed File System |
| HEMRM | Harmonised Electricity Market Role Model |
| HES | Head End System |
| IDS | International Data Spaces |
| IDSA | International Data Spaces Association |

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

| | |
|---|---|
| IOPS | Input/output Operations Per Second |
| IoT | Internet of Things |
| IP | Internet Protocol |
| IR | Commission Implementing Regulation |
| ISO | International Organization for Standardization |
| LCOE | Levelized Cost of Electricity |
| MC | Metering Center |
| MDMS | Meter Data Management System |
| MMS | Metering Management System |
| MoU | Memorandum of Understanding |
| NGSI-LD | Next Generation Service Interfaces - Linked Data |
| NIS | Directive on security of Network and Information Systems |
| O&M | Operation and Maintenance |
| OEM | Original Equipment Manufacturer |
| OSM | Other Service Module |
| P2G | Power-to-Gas |
| PLC | Power-Line Communication |
| PV | Photovoltaic |
| RAM | Reference Architecture Model |
| RBAC | Role-Based Access Control |
| RES | Renewable Energy Sources |

| | |
|---|---|
| SAREF | Smart Applications REFerence |
| SCADA | Supervisory Control and Data Acquisition |
| SDM | Smart Data Model |
| SGAM | Smart Grid Architecture Model |
| SLA | Service Level Agreement |
| SSAMd | System for uniform access to metering data |
| TCP | Transmission Control Protocol |
| TSO | Transmission Sysyem Operator |
| UC | Usage Control |
| UC | Use Case |
| VLOP | Very Large Online Platforms |
| VLOSE | Very Large Online Search Engine |
| WFM | Work Force Management |
| WP | Work Package |
| WPP | Wind Power Plant |
| XMPP | Extensible Messaging and Presence Protocol |

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

# Executive summary

This deliverable is an alpha version of the analysis of the governance models and participatory business models, that covers the topic of definition of data governance, data governance frameworks, regulation and requirements on both European Union and national level, identification of the gaps and the first sight on the data sharing incentives.

To make a clear view on the topic of Data Governance, the details of the definitions are analysed, taking into account structures from different association such as International Data Spaces Association (IDSA), BRIDGE or GAIA-X, different levels of the governance layers, also focusing on the differences for regulated and non-regulated domains and different Data Space Authority types. To ensure that the Data Governance Models in the scope of ENERSHARE project will be compliant with the European requirements and applicable to different operational context across Europe, the European Union regulations are analysed, as well as different initiatives, platforms and projects, which address the topic of data sharing and have the specific requirements for the data governance. Such initiatives and projects as IDSA, GAIA-X, FIWARE, OPEN-DEI, BRIDGE, OneNet, BD4NRG are analysed in order to find the similarities and differences in the data governance modelling, highlighting the advantages and disadvantages of using each approach.

To ensure that the Data Governance Models will touch all necessary topics and complaint with the national requirements, the questionnaire is prepared for the pilots in order to obtain more clear view on the data sharing mechanisms that will be used in the scope of ENERSHARE project and to design more detailed Data Governance Models to cover all the topics. This questionnaire template was created in close collaboration with the remaining horizontal WPs in order to incorporate and review governance-related key aspects that are essential for the pilot's perspective.

Detailed analysis of data governance was conducted based on the initiatives, projects, and the questionnaire template. This analysis aimed to identify potential gaps and provide recommendations for the comprehensive coverage of all aspects while designing the Data Governance Models within the ENERSHARE project.

In addition, the topic of data sharing incentive and business models design in the business-to-business (B2B) domain was analysed, focusing on both non-regulated and regulated domains. For non-regulated domains, different mathematical algorithms were introduces, that covers both monetary (data-by-money) incentive and non-monetary (data-by-data) and potential for data sharing incentives in the use cases in ENERSHARE project. Additionally, the incentives in regulated domain are analysed from Distribution System Operator (DSO), Transmission System Operator (TSO) and Multi-utility entities point of view.

# 1 Introduction

In today's data-driven world, data sharing has become a pivotal aspect of driving innovation, fostering collaboration, and making informed decisions. The exchange of information among organizations, governments, and individuals has opened up unprecedented possibilities for leveraging data's potential. However, with this surge in data sharing, the need for effective data governance has become increasingly crucial. Data governance in the context of data sharing involves establishing robust frameworks that ensure responsible, secure, and ethical practices. It addresses issues of data access, ownership, consent, privacy, and fair use, while adhering to legal and regulatory requirements. Data governance plays a pivotal role in navigating the complexities of the data sharing landscape, striking a balance between reaping the benefits of data collaboration and safeguarding against potential risks.

Another important topic that should be addressed in the context of data governance in the field of data sharing is the concept of "Data Spaces." Data spaces refer to interconnected ecosystems where data is stored, managed, and shared across various entities. These spaces foster collaborative environments, enabling seamless data exchange while maintaining control and compliance with governance principles. Within data spaces, stakeholders, including individuals, businesses, governments, and research institutions, participate in data sharing initiatives. Effective data governance models become instrumental in defining the roles and responsibilities of these stakeholders, ensuring transparency and accountability in data utilization.

The ENERSHARE project's primary goal is to integrate and customize the Data Space specifically for the energy sector. This integration involves combining data, storage, and computing infrastructures with the ultimate goal of creating compatible and interoperable resources. Furthermore, the project also focuses on developing data governance models in WP7 ("Data Space and data sharing governance and business models") that align with European requirements and are applicable in diverse operational contexts throughout Europe. The ultimate objective is to establish a neutral Energy Level Playing Field that facilitates data sharing among both regulated and non-regulated stakeholders. To achieve this, the project conducts an analysis of existing Energy Data Hub Governance Models, identifying any gaps that exist. Based on these findings, the project proceeds to develop Data Space Governance Models and incentive mechanisms, specifically geared towards promoting data sharing in the B2B domain.

The following chapters are organized as follows:

- Chapter 2 presents the general definitions of the Data Governance and applicable framework, considering different approaches to Data Spaces design, governance layers and topologies of Data Spaces, analysis of existing European Union (EU) regulations and analysis of initiatives, platforms and projects with various data sharing mechanisms in the context of data governance;

- Chapter 3 provides a description of the requirements of the data governance for the Pilots in the scope of ENERSHARE project, culminating in a questionnaire template to be sent to the Pilots in order to design adequate Data Space Governance Models within the project;
- Chapter 4 presents the identification of the existing gaps, based on the analysis of the initiatives, platforms and projects from Chapter 2;
- Chapter 5 provides the initial phase of creating a set of incentive mechanisms for data sharing in the B2B domain, which cover both regulated and non-regulated domains.
- Chapter 6 presents the main conclusion for the analysis of the alpha version of the Deliverable.

# 2 Data Spaces context and review in Europe

Energy Data Spaces (EDS) in Europe refer to digital ecosystems 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 consumption, 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 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.

In this section, the focus is on the currently known data governance (DG) modelling of the EDS, where these are discussed and described according to some of the already existent initiatives in Europe. This analysis serves as a starting point for the approach to be proposed in the ENERSHARE's EDS, in particular developed under task 7.2.

## 2.1 Data governance definitions and framework

For a secure, trusted and continue operation of the EDS, the governance layer must be addressed and defined for all components that are part of the process. It aims at covering not only a detailed and comprehensive view of the data life cycle, but also assure that the processes for data management included in the EDS are properly identified and follow the defined rules. In line with this, and before defining DG, in [1] it is presented the context behind the governance in the perspective of understanding what are the processes prone to DG, namely in the data-based domains. The three main concepts are presented:

- data/information management, for all technical and formal processes of managing data, i.e. business functions to execute the acquisition, control, protection, deliver and value enhancement of data/information;
- enterprise information management, referring to the enterprise-level vision or philosophy for the management of the data to improve business efficiency and value of the processes/data, by managing all involved parties (from technologies to people, organizations, data frameworks and principles, and other);
- data/information architecture, for a master set of data models and design approaches identifying the strategic data requirements and components of data management solutions.

On the top of any data management process, covered by the aforementioned layers, the DG is defined as the process that ensures the management actually takes place, and all definitions are properly followed. In [2], DG is defined as the exercise of authority, control and shared decision making (planning, monitoring and enforcement) over the management of data assets. The authors of [1], in turn, define it as the organization and implementation of policies, procedures, structure roles and responsibilities, which outline and enforce rules of engagement, decision rights and accountabilities for the effective management of information assets. In [3], the authors go further and refer to DG as all supporting mechanisms for decision making and responsibilities for processing related with information, adding it concerns any individual or group that has any interest in how data is created and how it is collected, processed, manipulated, stored, and made available for use/exploitation during the whole life-cycle.

In short, DG is defined by the use of authority combined with policy to ensure proper management of the data/information assets, distinguishing *data management* with *ensuring data is managed*. Figure 2-1 explores these two levels, with the left-hand side referring to governance (input to data and content life cycle with regards to rules and policies, ensuring data management process are occurring accordingly), and the right-hand side referring to data management (being the hands-on management of data). At the bottom of the two lines are the activities that operate the organization through maintaining information life cycles, as in the creation, use, manipulation and eventually disposal of data/information/content.

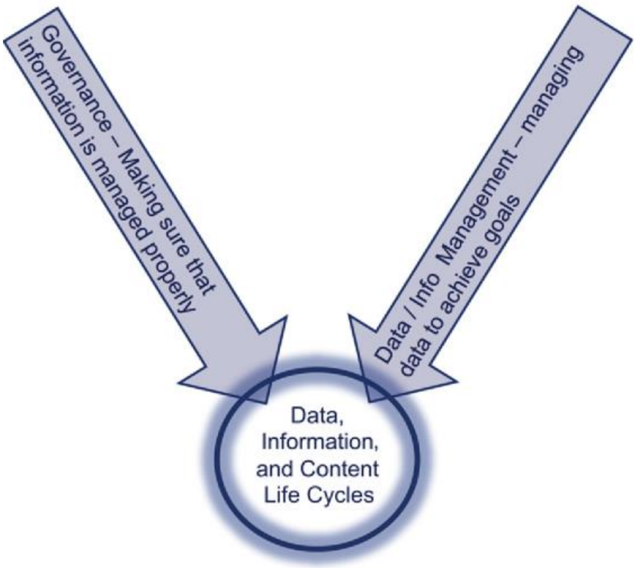

Governance – Making sure that information is managed properly
Data / Info Management – managing data to achieve goals
Data, Information, and Content Life Cycles

Figure 2-1 – Governance V, from [1].

The development of governance models for Energy Data Spaces is then of paramount importance. These models provide a framework for managing and regulating data sharing activities within the EDS ecosystem. Effective governance ensures that data sharing is carried out in a secure, transparent, and accountable manner, fostering trust among stakeholders and maximizing the potential benefits of data-driven energy solutions. One key aspect of governance models is the establishment of clear rules and standards for data access, sharing, and usage. These rules define the rights and responsibilities of data providers and users, ensuring that data is shared in a fair and non-discriminatory manner. Standardization of data formats, protocols, and interfaces is also crucial to facilitate interoperability and seamless data exchange between different stakeholders in the energy sector. Additionally, governance models for Energy Data Spaces should address privacy and data protection concerns. Compliance with regulations such as the General Data Protection Regulation (GDPR) in the European Union is essential to ensure that personal data is handled securely and in accordance with individuals' rights. Data anonymization and aggregation techniques can be employed to protect privacy while still allowing valuable insights to be derived from the data. Moreover, governance models need to consider issues related to data ownership, intellectual property rights, and fair monetization of data. Clear guidelines on data ownership and intellectual property help prevent disputes and ensure that data creators are appropriately recognized and incentivized. Mechanisms for fair and transparent data monetization can encourage data sharing and stimulate innovation in the energy sector. Collaboration and stakeholder engagement are also vital components of governance models for EDS. Engaging stakeholders from diverse backgrounds, including energy companies, research institutions, policymakers, and consumer representatives, fosters a collective decision-making process and ensures that the governance models reflect the interests and concerns of all relevant parties. Regular consultations, feedback mechanisms, and multi-stakeholder forums contribute to building consensus and fostering a sense of ownership among stakeholders.

In order to identify and structure all these requirements, the International Data Spaces Association (IDSA) establishes a set of layers to structure governance application that define the main action points to be integrated in the DG modelling [4]. These layers can be found in Table 2-1.

**Table 2-1 – Governance layers by IDSA, in [4].**

| **Layer** | **Description** |
|---|---|
| *Data space instance governance* | Executes and implements the governance practices and rules of a data space instance. Oversees data space functions and the rules. |

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

| | |
|---|---|
| *Data space ecosystem governance* | Defines the rules for the data space instance. Creates the intra data space trust between collaborating organizations. Complements standardization and regulation focusing on business-driven rules. Defines the inter data space interoperability practices. |
| *Data space domain governance* | Establishes sector-specific data space principles and mechanisms including semantic interoperability and domain-specific regulation. Leaves room for geographical differences while supporting maximum interoperability. |
| *Soft infrastructure governance* | Brings all the generic data space building blocks and concepts together, defines the legal basis and creates the common framework on which all data spaces are built. |

All these are proposed to ensure and enforce digital sovereignty. IDSA has also developed a reference architecture with role models for participation and a technical implementation that serves as technical base for the DS. DG models are then applied to the several building blocks in the perspective presented in Figure 2-2, that also captures another form of grouping the main sections for governance application:

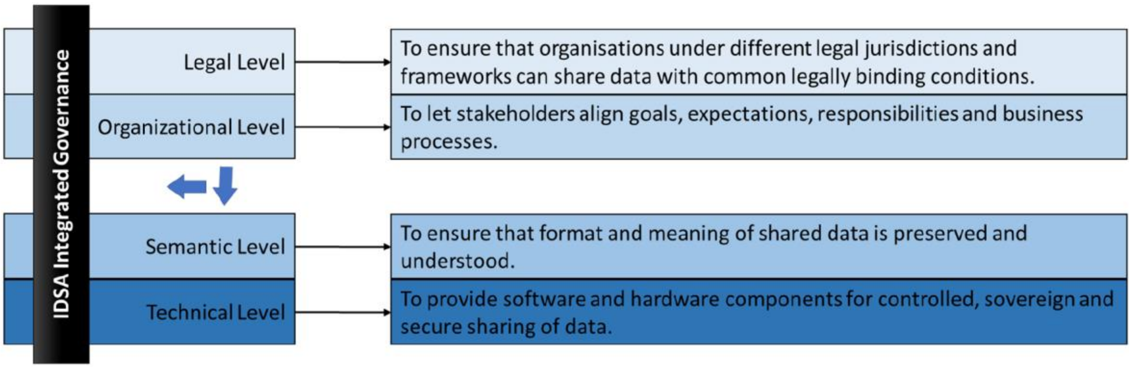

IDSA Integrated Governance
Legal Level
To ensure that organisations under different legal jurisdictions and frameworks can share data with common legally binding conditions.
Organizational Level
To let stakeholders align goals, expectations, responsibilities and business processes.
Semantic Level
To ensure that format and meaning of shared data is preserved and understood.
Technical Level
To provide software and hardware components for controlled, sovereign and secure sharing of data.

Figure 2-2 - Layered functional model for governance in IDSA, in [5]

The proposed framework distinguishes four functional levels under an overarching integrated governance approach [5]:

- Technical level, to provide software and hardware components for controlled, sovereign and secure sharing of data;
- Semantic level, to ensure that format and meaning of shared data is preserved and understood;
- Organizational level, to let stakeholders align goals, expectations, responsibilities and business processes;
- Legal level, to ensure that organizations under different legal jurisdictions and frameworks can share data with common legally binding conditions.

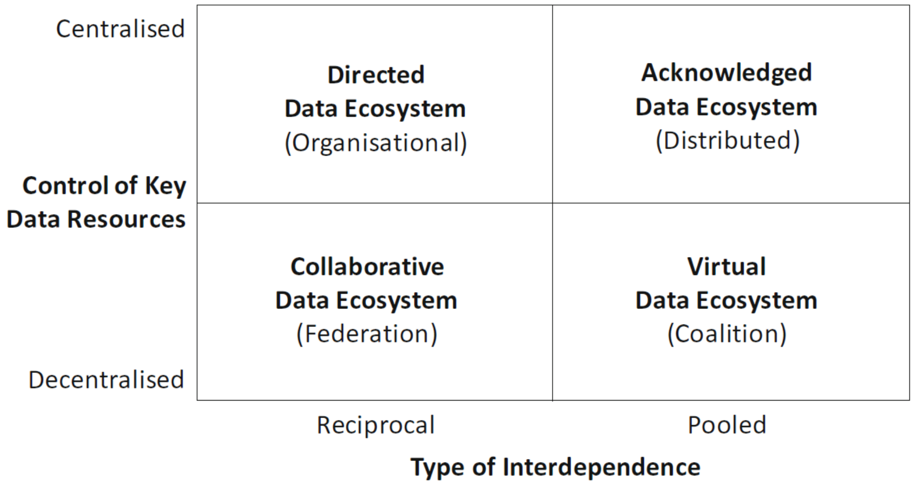
Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

In terms of designing EDS ecosystem in what respects to governance modelling, in [6] it is also suggested the main layers of DG, addressing some approach alternatives in terms of their design characteristics. These are presented in the following Table 2-2.

Table 2-2 – Governance approaches in Data Spaces design, from [6].

| Design characteristics | Solution design space | |
|---|---|---|
| Control | Centralised | Decentralised |
| Interdependence | Reciprocal | Pooled |
| Structure | Authoritarian | Democratic |
| Regulation | None | Enforceable |
| Independence | Controlled | Autonomous |
| Environment | Stable | Dynamic |

In relation with the Data Space coordination, the authors identify the relation between two of the critical criteria that most influence the design of the EDS and the relationships among the participants, presented in the previous table, that are related to the first two points of control and interdependence. This particular articulation is illustrated in the following Figure 2-3.



| Control of Key Data Resources | Reciprocal | Pooled |
|---|---|---|
| Centralised | Directed<br>Data Ecosystem<br>(Organisational) | Acknowledged<br>Data Ecosystem<br>(Distributed) |
| Decentralised | Collaborative<br>Data Ecosystem<br>(Federation) | Virtual<br>Data Ecosystem<br>(Coalition) |

Type of Interdependence

Figure 2-3 – Topology of Data Spaces, relating control and interdependence topics from Table 2-2.

In one side, there is the *Control of Key Data Resources* related to who controls the essential data resources in the data ecosystem, either a single main actor, or data resources are spread across multiple actors, ranging from centralised to decentralised, respectively. On the other side, it is the *Participant Interdependence*, related to the degree to which different participants in the DS must interact and exchange data for performing their activities - reciprocal interdependence requires high levels of coordination among the participants, while pooled interdependence enables loose coupling among participants.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

In line with this, and recognizing these as main and critical points defining the DG approaches (from Figure 2-3), IDSA defines the data space authority (DSA) which is responsible for establishing the policies and rules of the data space. This role can be carried out by one entity, but also by multiple or even all participants. These types of Data Space Authorities are presented in Figure 2-4. In a centralized data space, this could be the operating company. In a federated data space, this function would be performed by the federator(s) agreeing on the rules, while in a fully decentralized data space, various mechanisms are available to the participants. The mechanisms in a decentralized data space enable participants to agree on the set of policies and their enforcement, thus sharing responsibility for the data space authority function. Also in the authority layer, i.e. governance for policy enforcement, the IDSA proposes, under the DSA role, DG types aligned with the previous approaches [4].

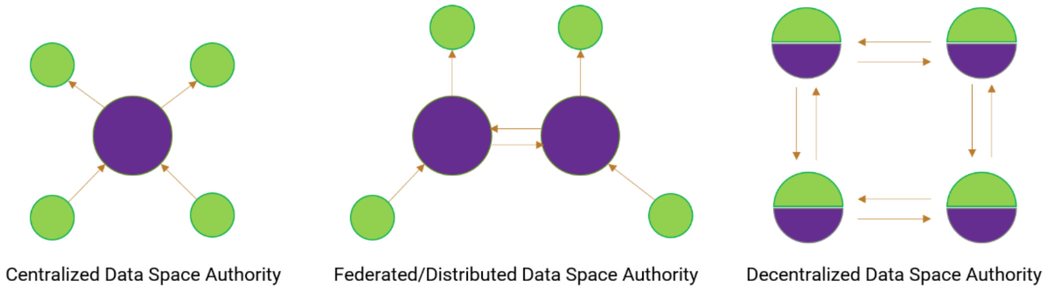

Centralized Data Space Authority
Federated/Distributed Data Space Authority
Decentralized Data Space Authority

**Figure 2-4 – Data Space Authority types, from [4].**

In a centralized data space governance structure, all operational services for the data space are managed by a single authority. These services encompass participant identification, onboarding, membership management, semantic models provision, data discovery, and optional features like marketplaces and audits. While the centralized model draws familiarity from existing aggregator platforms, it restricts the autonomy and sovereignty of participants. The entity controlling the centralized identity provider also exercises control over membership and resource access, enabling arbitrary decisions on inclusion or exclusion without regard for the data space's policies. In the worst-case scenario, the central identity service can disrupt data sharing between participants, resulting in severe consequences beyond the data space. A central catalog offers benefits in terms of data discovery, providing a designated location to find available data, with queries made at a single endpoint returning data contract offers from multiple participants. However, this approach carries the risk that the entity controlling the catalog also wields authority over its content, making arbitrary decisions on accessibility. Moreover, centralized services create a vulnerability as a single point of failure. An outage could render the entire data space inaccessible or non-functional, posing significant business risks for participants. Valuable data shared within a centralized component can attract malicious actors seeking unauthorized access, data manipulation, or disruption to harm specific targets. Concentrating substantial value in a centralized identity provider or catalog makes it an attractive target. Infiltration of such a central component can result in more extensive damage than an attack on a single participant. By thoughtful planning and appropriate choices in implementing a centralized data space, many challenges to participant autonomy can be mitigated or reduced. However, the design solution may limit the full autonomy of participants due to vital functional resources within the data space. Nonetheless, the significance of this limitation depends on the purpose and objectives of the data space.

The decentralized or distributed model retains a certain level of centralized control while addressing technical and security challenges. In this model, functional responsibilities are distributed among a few federated nodes. Rather than a single entity providing services, multiple entities share the responsibility through individual synchronized nodes. This requires additional technical investment to ensure node synchronization, handle transactions, and perform queries across multiple services. While this model significantly enhances resilience and availability, it also introduces complexity. Implementing certain functional roles, such as identity, in a distributed environment can be more complex compared to others, like catalog management. However, it offers intriguing variations to the centralized design by enabling more sophisticated designs. For instance, a federated catalog can be implemented so that different sub-catalogs are available on different nodes, enhancing system performance and availability. If the objective of the data space is to maximize participant sovereignty and autonomy, the distributed model does not provide substantial improvements compared to the centralized design. In this model, a small group of entities would still have significant control over the data space, and participants would remain highly dependent on these entities, akin to a centralized data space. Nevertheless, a federated model can be the ideal solution for implementing data spaces based on closed group consortia with clear consortium leaders. Reasons beyond technical considerations, such as contracts and legal regulations, may necessitate adopting a federated or partially federated model for a data space. When discussing distributed data spaces, it's important to differentiate between the "Federation service" and "Federated service":

- The Federation service supports the federation functionality within a data space and serves specific functional roles like identity or catalog management.
- The Federated service describes the implementation of any service as a distributed service within a data space, encompassing various federation services and more.

To ensure maximum participant sovereignty and autonomy in a data space, each participant should be free to act without improper hindrance. Participants must adhere to rules and policies, but sovereign participants should be immune from unwarranted or arbitrary interference. Improper interference could include refusal to include a participant's data assets in the catalog, even if all requirements are met, or deactivating a participant's identity,

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

potentially disrupting their business. This interference may not be malicious and could result from errors or unstable software. A fully sovereign participant should be able to interact with other participants without relying on a third party once it is established that the participant is compliant with all rules.

Utilizing a decentralized design offers the highest level of participant autonomy and sovereignty. The fundamental component enabling participant autonomy is the decentralized identity system. In this system, each participant assumes the responsibility of maintaining their own identity information, which can be verified by other participants or the DSA (Data Space Authority), eliminating the need for reliance on a centralized identity provider. Once decentralized identities are established, other functional services can also be decentralized, minimizing or even eliminating obstacles to participant sovereignty. It is important to note that in a decentralized data space, a significant portion of the operational responsibility for essential functional roles shifts from the DSA to the participants. For example, in a centralized model, the DSA is responsible for managing the catalog of available data assets. However, in a decentralized model, each participant takes on the responsibility of directly publishing their available data, and in turn, they must inquire about the available assets from all other participants. Another benefit of a decentralized system is its resilience to errors or malicious actors. Problems occurring in individual nodes do not automatically affect all participants within the data space. Additionally, a decentralized system does not require an ever-increasing number of centralized services. Each node is self-contained and provides all the necessary endpoints for interaction. Consequently, a data space can grow and scale much more efficiently compared to a centralized design, where the resources for providing central services must grow exponentially [4].

In order to further define the DG concepts, in [3] it is presented a vision for the application of DG in the several components of a data space, namely a EDS, including two levels: organizational and technological. This is illustrated in Figure 2-5.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

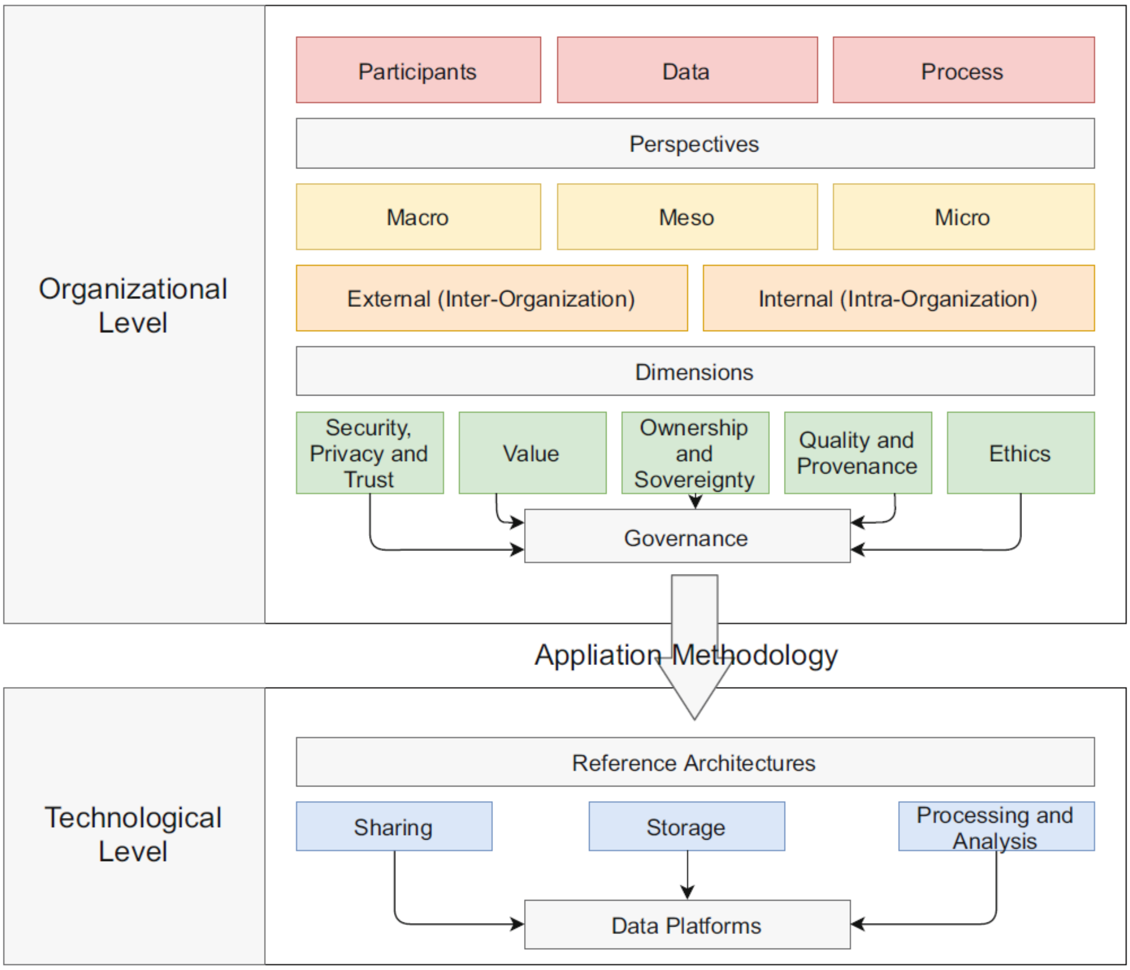


Figure 2-5 – Energy Data Space governance components, proposed by [3].

In the organizational part is it proposed two important aspects, the governance dimensions and perspectives. Dimensions refer to the scope of governance, either internal or within the organization, or external affecting ecosystems formed by multiple participants, such as Data Spaces. Perspectives refer to the areas of action, which are those tasks or fields that the governance measures and mechanisms must cover. The same authors group literature important points to characterize DG including their understanding of the grouping, as follows [3]:

- Ownership and sovereignty: data ownership is an important aspect when the intention is offering data and negotiating contracts in digital business ecosystems. Moreover, the associated term "data sovereignty" indicates the rights, duties, and responsibilities of that owner.
- Trust, privacy, and security: the data throughout its entire life cycle must be safe and come to add value without being compromised at any point. For this, it is important that throughout the cycle all participants are trusted.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

- Value: new digital economic models based on data as an asset of organizations are required. The concept of monetization of data, which seeks using data to increase revenue, is essential in this perspective.
- Quality and provenance: Data quality refers to the processes, techniques, algorithms, and operations aimed at improving the quality of existing data in companies and organizations, and associated with this comes the provenance, which indicates the traceability or path that the data travels through the organization.
- Ethics: which refers to systematizing, defending, and recommending concepts of correct and incorrect conduct in relation to data, in particular, personal data.

Additionally, it is also accounted the overview of the importance of the bid data life cycle, another layer of DG that must be accounted, besides the authority and enforcement of data management procedures. In [3], data life-cycle is defined as required in order to transform it into valuable information, in order to be better understood, as well as, a better analyse its nature and characteristics. The five phases of data life cycles are proposed and illustrated in Figure 2-6, including the collection, integration, persistence, analysis, and visualization, and how these phases should serve the mentioned five Vs: volume, velocity, variety, veracity and value. Data life-cycle management is a process that helps organizations to manage the flow of data throughout its life cycle — from initial creation through to destruction. Having a clearly defined and documented data life cycle management process is key to ensuring DG can be conducted effectively within an organization.

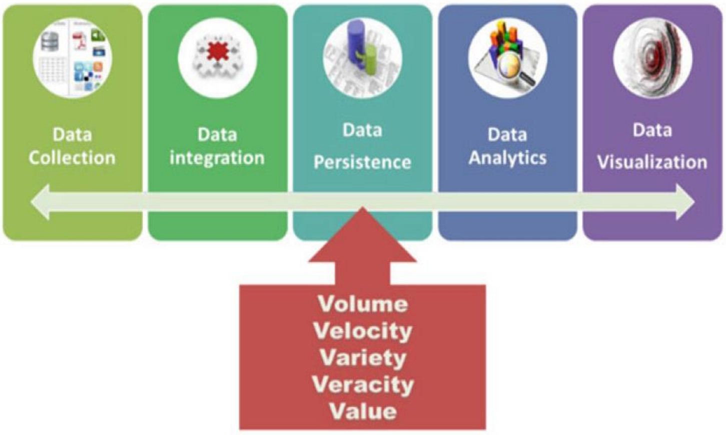


Figure 2-6 – Data life cycle, proposed in [3].

On top of this, and in order to serve the needs of DG within the data life-cycle management, which include all data management procedures from soft to hard implemented, the authors advance with the concept of *DataOps*, to redirect the strict guidelines established in the typical DG methodologies into a set of good practices that are easy to implement technologically. The outline of the DataOps is illustrated in the following Figure 2-7. The proposal states DG can execute continuously as part of development, deployment, operations, and monitoring workflows when governing the life cycle of the data exchanged into the EDS.

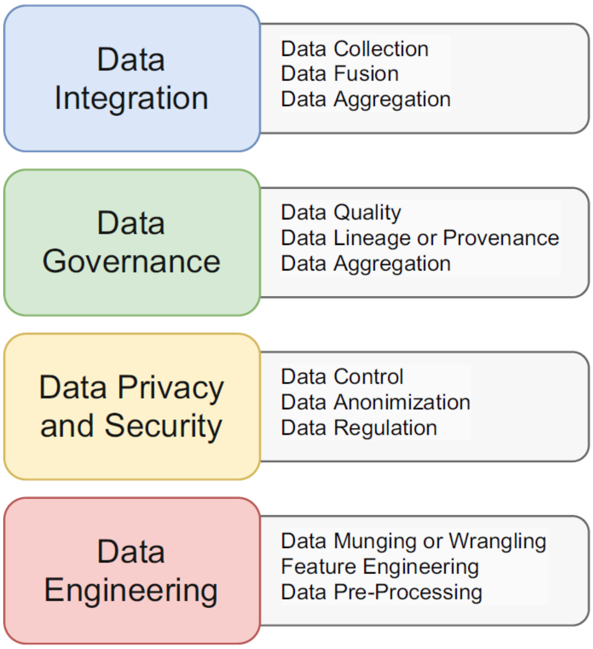


**Figure 2-7 – Main sections of DataOps, including the Data Governance layer for data life cycle, proposed in [3].**

As it can be seen in what is presented above, the development of governance models is then crucial for the successful implementation of Energy Data Spaces. These models provide the necessary framework to regulate data sharing activities, address privacy and data protection concerns, establish clear rules and standards, and foster collaboration among stakeholders. By ensuring effective governance, EDS can unlock the full potential of energy-related data, drive innovation, and accelerate the transition towards a sustainable and efficient energy system in Europe. In the following subsection and overview of the European-level considerations of the DG context of EDS is presented.

### 2.1.1 EU regulation

As described in the introduction, a data space is a complex socio-technical system. Governance of such systems will have to manage its inherent complexities, while taking into account all relevant characteristics of the systems. The legal, regulatory and policy environment in which such systems must function adds another layer of complexity, which will also have to be reflected in the governance framework. Furthermore, and for the purpose of the current deliverable, it provides the necessary background against which the gap analysis in chapter 4 will have to be performed. This is the subject of this section of the report.

The complexity and associated risks of the legal, regulatory and policy environment referred to in the previous paragraph can be further broken down in at least the following main categories:

- The applicability of both horizontal (i.e. non-sector specific, for example the General Data Protection Regulation) and vertical (i.e. sector-specific, such as the Directive on Energy Efficiency) laws and regulations;
- The applicability of EU as well as national, regional and local laws and regulations. While some will be relevant for the data space as a whole, others will be relevant only for specific elements of the data space;
- Legal and regulatory uncertainty owing to insufficient compatibility between the applicable laws and regulations;
- Legal and policy uncertainty owing to laws, regulations and policy measures of future relevance, but currently still in preparation (e.g. the EU Data Act), while the data space is already in development.
- Legal and policy uncertainty owing to existing laws, regulations and policy measures, but which are currently undergoing review (e.g. the ePrivacy Regulation proposed to review, update and replace the current ePrivacy Directive), while the data space is already in development.
- Emerging Properties of the data space – in other words, manifestations of the data space that would only become apparent in the future, but cannot be anticipated at the current stage of the data space development; and for which the applicable law is unclear.

All categories mentioned above are likely to have a significant impact on the design and functioning of the data space and would have to be accounted for in the governance framework and as part of the gap analysis, as presented in Table 2-3.

Table 2-3 – Risks and their impact on governance framework measures.

| Main category of issue or risk | Governance framework measure |
|---|---|
| Applicability of both horizontal & vertical laws and regulations | • Legal analysis of relevant laws and regulations<br>• Modification of governance accordingly, if and when necessary |
| Applicability of EU, national, regional, local laws and regulations | • Legal analysis of relevant laws and regulations<br>• Modification of governance accordingly, if and when necessary |
| Legal and regulatory uncertainty owing to insufficient compatibility between the applicable laws and regulations; | • Legal analysis of the interaction of relevant laws and regulations<br>• Modification of governance accordingly, if and when necessary |

| Main category of issue or risk | Governance framework measure |
|---|---|
| Legal and policy uncertainty linked to ongoing legal, regulatory and policy developments (new or recast) | • Continuous monitoring of legal, regulatory & policy developments<br>• Modification of governance accordingly, if and when necessary |
| Emerging properties of the data space | • Adoption of a precautionary approach & corresponding measures<br>• Contingency planning<br>• Continuous process of monitoring and assessment of the data space |

The following sub-sections will detail main takeaways from core EU laws, regulations and policies of direct relevance to the energy data space. These will serve as inspiration for constructing the governance framework and for conducting the gap analysis.

It should be stressed that this part of the report is not intended as an exhaustive analysis of the legal and regulatory environment, which is not part of this deliverable.

#### 2.1.1.1 The General Data Protection Regulation (GDPR)

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 (General Data Protection Regulation, **GDPR**) [7] is the main piece of EU legislation regulating the protection of personal data. An example of horizontal legislation, GDPR prescribes generic rules regarding the processing of **personal data**, applicable in all sectors, including energy, and in all EU Member States. GDPR was adopted in 2016, has applied since 25 May 2018, and has been implemented in the national legislation of all EU Member States.

A selection of GDPR provisions to inform the governance framework and the gap analysis are included below.

##### *i. Categories and uses of data*

Categories of data covered by GDPR are **personal data** (including **pseudonymised data**), defined as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". Furthermore, GDPR defines subcategories of personal data (i.e. **special categories of personal data,** such as health data) which can be processed only under special conditions. Special attention must also be paid to the processing of data of **children**.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

Important in the context of the data space are the rules governing the purposes for which the data can be processed. As such, GDPR distinguishes between the **primary purpose** for which personal data, according to specific rules, may be processed; and secondary or **further processing** of personal data, which is only allowed under certain conditions.

### *ii. Roles / Actors*

Next to **individuals** as data subjects, GDPR distinguishes two main categories of roles, namely that of **data controller** (who “ determines the purposes and means of the processing of personal data”) and **data processor** (who processes personal data on behalf of the controller), as well as their respective representatives (those acting on behalf of the data controller and data processor). Other categories of actors recognised by GDPR are **joint controllers** (where several parties act jointly as controller, a category particularly relevant for data spaces) and that of **third parties** who may process personal data but only with the permission and under the direct authority of the controller or processor.

### *iii. Rules and responsibilities*

The GDPR prescribes a number of obligations for those processing personal data, relevant from a governance perspective. Amongst these obligations:

- Obligations related to the **lawfulness** of personal data processing
- Obligations to provide data subjects with **information** about the processing of data obtained **directly or indirectly** from them; and used for the original or other, further purposes
- Obligations to facilitate **data subject rights**, such as their rights to access, transfer, correct, restrict processing, erase their data
- Specific obligations related to the **automated individual decision-making, including profiling**, which might produce legal or other significant effects on individuals.The obligation to assign a **data protection officer** by public authorities and businesses that engage in large-scale data processing, or the processing of special categories of data
- Obligation to apply **data protection by design and by default**
- The obligation to carry out **data protection impact assessments** when data processing poses risks to the rights and freedoms of individuals and when significant changes to the systems have taken place
- Obligation to **report personal data breaches** within 72 hours
- **Accountability** obligations (e.g. in the form of record keeping of personal data processing, certification etc.) are imposed on controllers, who are responsible and must be able to demonstrate compliance with GDPR

- Responsibility of controllers for their **suppliers** and the obligation to **contractually regulate** that suppliers comply with GDPR. The controller remains responsible for their suppliers not complying with GDPR.
- Obligation to adopt other **technical and organisational measures** for the protection of personal data, and corresponding to the roles and responsibilities of the parties involved
- Specific rules for **non-EU businesses** processing data of individuals in the EU, and obligations regarding **international personal data transfers**
- **Monetary penalties** for non-compliance with GDPR

#### 2.1.1.2 Data Governance Act

Regulation (EU) 2022/868 on European data governance (**Data Governance Act, DGA**) [8] was adopted in 2022 and will apply from 24 September 2023. DGS, is part of the European Commission's Strategy for Data [9], and sets out rules for the **reuse and re-sharing** of **public sector data**. According to the EC, "The new regulation will provide a good governance framework supporting the common European data spaces and will ensure that data can be made available voluntarily by data holders."

The governance framework of the energy data space and the gap analysis conducted as part of this deliverable should take into account the fact that in some EU Member States energy may be part of the public (national, regional, local) sector, whereas in other countries it may be part of the private sector.

##### *i. Categories and uses of data*

The categories of data to which DGA applies are primarily data held by the **public sector**. Data held by the public sector could include both **personal data** (as defined be the GDPR) and **non-personal data,** including data otherwise **protected** on grounds of commercial confidentiality, or intellectual property of third parties**.** DGA also introduces the category of **highly sensitive non-personal public data.**

DGA also provides for a variety of ways in which these data can be processed, primarily:

- **Data access** refers to uses of data "without necessarily implying the transmission or downloading of data"
- **Data sharing** referring to "the provision of data by a data subject or a data holder to a data user for the purpose of the joint or individual use of such data, based on voluntary agreements or Union or national law, directly or through an intermediary, for example under open or commercial licences subject to a fee or free of charge"
- **Data sharing among businesses**, "against remuneration in any form"
- **Data re-use** refers to the use of data for other commercial or non-commercial purposes "than the initial purpose within the public task for which the data were produced"

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

DGA also introduces a new category of data sharing, namely **data altruism** defined as the "sharing of data voluntarily and for no reward", based on the consent of the data subject (for personal data) or the permission of the data holder (for non-personal data). This category of data use is closely related with objectives of general interest, such as combating climate change or improving mobility.

DGA also includes provisions for data sharing with **non-EU countries** (i.e. third countries).

### *ii. Categories of actors / roles*

DGA distinguishes several categories of relevant actors, each assigned with specific roles, namely:

- **Data subject,** or natural person who, as per GDPR "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" [7]
- **Data holder** – a legal or natural person other than the data subject who "has the right to grant access to or share certain personal or non-personal data".
- **Data user** - a natural or legal person who has lawful access to certain personal or non-personal data and has the right in the case of personal data, to use that data for commercial or non-commercial purposes.
- **Data intermediation service,** which has as aim to "establish commercial relationships for the purposes of data sharing between an undetermined number of data subjects and data holders on the one hand and data users on the other, through technical, legal or other means, including for the purpose of exercising the rights of data subjects in relation to personal data".
- **Data cooperatives,** which are organisational structures set up with the purpose of supporting its "members in the exercise of their rights with respect to certain data", such as making informed choices before consenting to the sharing of personal data, or "negotiate terms and conditions for data processing on behalf of its members"

### *iii. Rules and responsibilities*

The DGA prescribes a number of obligations relevant from the perspective of data governance or overall governance of a data space. Amongst them are:

- Defining the conditions for data reuse on the principles **non-discrimination, transparency, proportionality, objective justification and not restricting competition, "**with regard to the categories of data and the purposes of re-use and the nature of the data for which re-use is allowed"

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

- Ensuring that, where applicable, “the **protected nature of data** is preserved”, for example by using anonymisation and aggregation techniques, contractually or by confidentiality or non-disclosure agreements
- Setting up a **verification** process to ensure that data use and reuse does not compromise the integrity of data
- Ensuring compliance with **intellectual property rights**.
- Adopting appropriate measures for data processing in **non-EU countries,** with special conditions applying to highly sensitive categories of non-personal data
- Defining the rules about the commercialisation of data and applicable **monetary compensations**
- Defining or observing specific procedures for interacting with the **competent bodies** (e.g. for access to data, to notify intermediation services, to register as a data altruism organisation)
- **Accountability** measures to demonstrate compliance with applicable laws and regulations.

#### 2.1.1.3 Requirements for access to electricity metering and consumption data [9]

Commission Implementing Regulation (EU) 2023/1162 on interoperability requirements and non-discriminatory and transparent procedures for access to metering and consumption data [9] (**IR**) was published on the 6th of June 2023 and will enter into effect on the 5th of July 2023 (the entry into force is still pending notification). First in a series of similar acts, it lays down specific rules for the energy sector, specifically the rules for implementing Directive (EU) 2019/944 on common rules for the internal market for electricity, and in particular Article 24 on Interoperability requirements and procedures for access to data. It defines the rules for customers in the **retail electricity market** and other eligible parties to **access and exchange metering and consumption data** (validated and not validated; historical and real-time); and ensures that suppliers and service providers gain seamless access to final customers’ data. Unlike Directive (EU) 2019/944, this Implementing Regulation is “binding in its entirety and directly applicable in all Member States”.

##### *i. Categories and uses of data*

This IR regards **several categories of data**, such as “**meter readings** of electricity consumption from the grid, or electricity fed into the grid, or consumption from on-site generation facilities which are connected to the grid” and includes **validated historical metering** and **consumption data** from 2019 onwards and **non-validated near-real time metering and consumption data** from conventional or smart metering systems.

In the sense of the GDPR, these categories of data could include both **personal** and **non-personal data**.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

In the sense of the GDPR, categories of processing foreseen by this IR include: **access, use** and **further processing** (i.e. secondary use or re-use of data for purposes other than the ones for which the data were originally collected).

### *ii. Roles / Actors*

The IR regards several **categories of actors**, both individuals as well as businesses (natural and legal persons).

The specific **roles** assumed by actors that are subject to this IR include those of:

- **final customers** in the retail electricity market, which could be individuals or businesses(natural and legal persons), also including citizen energy communities
- a variety of **eligible parties** to access the data and offer energy-related services to final customers, "such as suppliers, transmission and distribution system operators, delegated operators and other third parties, aggregators, energy service companies, renewable energy communities, citizen energy communities and balancing service providers";
- **metered data administrator** responsible for "storing validated historical metering and consumption data and distributing these data to final customers and/or eligible parties";
- **permission administrators** "responsible for administering a register of data access permissions for a set of metering points, making this information available to final customers and eligible parties in the sector, on request";
- **metering point administrators** "responsible for administering and making available the characteristics of a metering point, including the registrations of eligible parties and final customers linked to the metering point"
- **data access providers** "responsible for facilitating access, including in cooperation with other parties, to validated historical metering and consumption data by the final customer or by eligible parties;
- **identity service providers** who "manages identity information; issues, stores, protects, keeps up to date, and manages identity information for a natural or legal person and provides authentication services to eligible parties and final customers";
- **meter operators** "responsible for installing, maintaining, testing, and decommissioning physical meters".

### *iii. Rules and responsibilities*

Rules and responsibilities applying to electricity undertakings in the retail electricity market (including several categories of actors mentioned in the previous section) are formulated in the IR as **reference models.** These reference models are sets of procedures and their purpose is to provide technical and organisational directions for the implementation of interoperability requirements. They provide essential elements for the governance framework regarding, for example rules governing permission to use data and rules for secure access to and use of data; accountability rules, such as logging, notification and reporting on data access and use activities, etc. One of the reference models regards the access to validated historical metering and consumption data by an eligible party. The diagram of this reference model for illustration purposes is provided in Figure 2-8.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

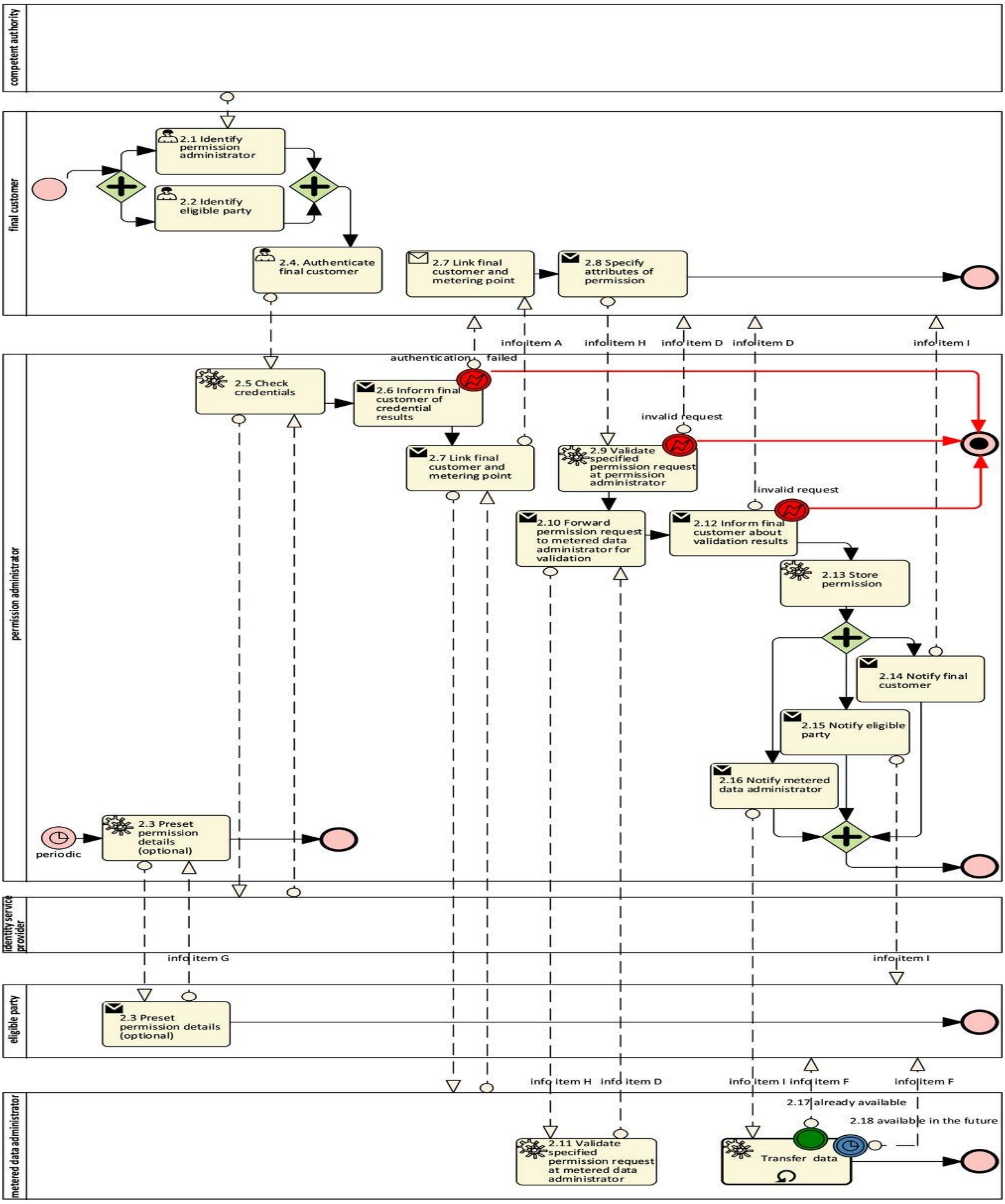

competent authority
final customer
2.1 Identify permission administrator
2.2 Identify eligible party
2.4. Authenticate final customer
2.7 Link final customer and metering point
2.8 Specify attributes of permission
info item A
info item H
info item D
info item D
info item I
authentication failed
permission administrator
2.5 Check credentials
2.6 Inform final customer of credential results
2.7 Link final customer and metering point
invalid request
2.9 Validate specified permission request at permission administrator
invalid request
2.10 Forward permission request to metered data administrator for validation
2.12 Inform final customer about validation results
2.13 Store permission
2.14 Notify final customer
2.15 Notify eligible party
2.16 Notify metered data administrator
periodic
2.3 Preset permission details (optional)
identity service provider
info item G
info item I
eligible party
2.3 Preset permission details (optional)
info item H
info item D
info item I
info item F
info item F
2.17 already available
2.18 available in the future
metered data administrator
2.11 Validate specified permission request at metered data administrator
Transfer data

Figure 2-8 - Diagram of the procedure 'Access to validated historical metering and consumption data by an eligible party'. Source: EC [10]

### 2.1.1.4 Digital Services Act

Regulation (EU) 2022/2065 on a Single Market For Digital Services and amending Directive 2000/31/EC (**Digital Services Act, DSA**) [11] defines the rules for the functioning of EU digital intermediary services (such as online marketplaces), to promote related market predictability, trust, fundamental rights, consumer protection and innovation. Another example of horizontal legislation (i.e. applicable across sectors, and thus also to the energy sector), the DSA entered into effect in 2022 and will start applying as of 17 February 2024. DSA is of relevance to energy data spaces, insofar as the data spaces offer digital intermediary services.

#### *i. Categories and uses of data*

Categories of data that could fall within the scope of the DSA include both **personal** and **non-personal data** that might be processed by intermediary services. More specifically, the types of processing (**uses**) of these data are directly related to the three categories of intermediary services covered by the DSA, namely: i) mere conduit (i.e. providing access to a communication network and transmitting data through the network); ii) caching (i.e. the temporary and automatic storage of the transmitted data for efficiency and security purposes); and iii) hosting (i.e. storage of data).

#### *ii. Roles / Actors*

The DSA defines several categories of relevant **actors** (individuals, private organisations, public organisations, etc.) interacting in various capacities or **roles** in intermediary services, such as:

- **consumers**, which are individuals (natural persons);
- **active recipients** of intermediary services (natural and legal persons);
- **traders** and their representatives (natural persons; legal persons, both public and private) who use the intermediary services in order to conduct their activities;
- **intermediary services** such as online platforms that “ at the request of a recipient of the service, stores and disseminates information to the public”.

#### *iii. Rules and responsibilities*

Most provisions of the DSA are formulated for very large online platforms (VLOPs) and for very large online search engines (VLOSEs) and might not apply to data spaces, at least not at this stage in their development. However, the DSA also outlines several rules applicable to all intermediary services, regardless of their size, rules also relevant from a governance perspective. Amongst them:

- limits to the **liability** of intermediary services
- **transparency and safety** obligations (e.g. assigning single points of contact; defining terms and conditions for the use of the services).

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

### 2.1.1.5 Upcoming new EU legislation (EU AI Act and EU Data Act proposals)

The governance framework and the gap analysis will have to take into account the potential effect of **upcoming EU laws and regulations**. This imposes flexibility and adaptability requirements on the governance framework which should be able to accommodate potentially significant but difficult to assess future changes. It will also impose requirements with regard to the continuous monitoring of such legal and regulatory developments. These should not be limited to EU-level laws and regulations, but should also consider relevant **upcoming initiatives at Member State, regional and local levels.**

Examples of upcoming EU-level laws and regulations relevant for ENERSHARE include:

1. The 2021 proposal for a Regulation on harmonised rules on Artificial Intelligence (**AI Act**) [12] which will define the rules for "placing on the market, putting into service and use of AI systems". The draft AI Act proposes a risk-based approach according to which AI systems will be classified; defines categories of AI-systems (such as high-risk or prohibited AI-systems); for which specific transparency, registration, reporting, conformity assessment and other rules and obligations would apply.
2. The 2022 proposal for a Regulation on harmonised rules on fair access to and use of data (**Data Act**) [13] which will define the rules for access, use and interoperability of data generated by the use of connected products or related services (e.g. Internet-of-Things). According to the European Commission: "the Data Act will contribute to more data being available, also for and within the sectoral data spaces. For instance, building on the Data Act, the common European energy data space will enhance the interoperability of energy assets and services, as well as the flexibility and the overall security and reliability of the energy system." [14] If adopted, the Data Act is likely to impose (new) obligations for data sharing in business-to consumer, business-to-business and business-to-government relations; obligations for data holders; obligations regarding conditions for switching between data services; impose interoperability requirements; impose requirements for international transfers of data and for cloud services providers, etc.
3. The 2022 proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements (**EU Cyber Resilience Act** [15]), which will define harmonised cybersecurity rules and requirements for hardware and software with digital components (e.g. Internet of Things devices), including their remote data processing solutions. If adopted, the EU Cyber Resilience Act is likely to impose new requirements for standardisation, certification, vulnerability disclosure, liability, use of open source, also relevant for the energy sector.

### 2.1.1.6 Upcoming recast EU laws and regulations

A further category of EU laws and regulations that will also have to be taken into account by the ENERSHARE governance framework and gap analysis is that of **recast EU laws and regulations.**

This category refers to EU laws and regulations already in force but currently undergoing a review process. As the review process is still ongoing, the outcomes are uncertain - in other words, it is unclear at this stage what their definitive provisions and requirements will be and how they compare to the current ones, and thus what their effects on the energy data spaces, including ENERSHARE, will be.

A few examples relevant for ENERSHARE include:

1. The proposal for a Regulation on Privacy and Electronic Communications (**ePrivacy Regulation)** and repealing the ePrivacy Directive which is currently in force. It complements the GDPR and sets the rules for the processing of electronic communications (personal) data and services. The new ePrivacy Regulation was proposed in 2017 and the legislative process is still ongoing.
2. The Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (**NIS 2 Directive** [16]) replacing the current NIS Directive. The NIS 2 Directive is of horizontal, cross-sectoral relevance (thus also relevant for the energy sector). Unlike the ePrivacy Regulation, the NIS 2 Directive has already been adopted and went into effect in January 2023. However, it will first have to be transposed by each EU Member State by October 2024. Potential differences in transposition could have a direct effect on the governance of ENERSHARE. NIS 2 expands the scope of the original NIS Directive, applies to more entities/actors, imposes expanded obligations (e.g. about incident and vulnerability disclosure; accountability; compliance)

### 2.1.1.7 Upcoming energy sector-specific EU legislation

The ENERSHARE governance framework and gap analysis would also have to take into account energy sector-specific legislative and policy initiatives. One such example has been provided in section 2.1.1.3 and regards requirements for access to electricity metering and consumption data. Other initiatives that can be anticipated regard cybersecurity and, particularly relevant for ENERSHARE, a proposed regulation for energy data spaces. The outline of a future proposal for an energy data space regulation has been provided in the 2022 EU Action Plan [17] on digitalizing the energy sector. To date, the only concrete sectoral data space legislative proposal has been for an EU health data space, a summary of which is provided below for illustration purposes.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

#### 2.1.1.8 European Health Data Space

The previous sections presented a small selection of current and upcoming laws and regulations of direct applicability to the energy data space. In addition, we are including the current section on the European Health Data Space (**EDHS**) [18]. EHDS, published in 2022, is the first proposal for a sectoral data space. As such, it might provide valuable hints as to the future provisions of the upcoming energy data space regulation. EHDS, like all future EU sectoral data spaces (including the one for energy) aims to establish interoperability platforms at EU-level for the primary and secondary uses of data; defining rules that apply uniformly across all EU Member States; with the ultimate goal of improving the functioning of the single market.

##### *i. Categories and uses of data*

Categories of data falling within the scope of the EHDS include both **personal** and **non-personal data.** Although EHDS concerns primarily data in **electronic** (digital) format, certain obligations could extend to **non-digitised** data as well (e.g. existing records in paper format).

EHDS foresees extended and diverse **uses** of data, most notably:

- for **primary** as well as **secondary** purposes (in other words, for the purposes for which the data were originally collected, as well as for a variety of additional purposes);
- for **research, innovation, regulatory purposes, policy-making, statistical and other** secondary purposes;
- for uses **across data spaces** (for example, where data from EHDS should be made interoperable and available for use in the energy data space).
- for uses within the Union, but also in **third countries** and **internationally** (uses by international organisations.
- for **direct access** or access via **intermediaries.**

##### *ii. Roles / Actors*

**Categories of actors** to which EHDS would apply are equally numerous and diverse, including both **natural and legal** persons, in both the **private and public** sectors: health organisations (and in the case of the energy data space, organisations in the energy sector, such as DSOs), research organisations, innovators, government organisations, statistical offices, international organisations.

EHDS also defines several categories of **roles** for these actors, in which they can exercise their rights and obligations within the data space, including those of:

- **data recipients** (i.e. those receiving data from another controller in the context of the primary use of digital data)

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

- **data holders** (i.e. those with control over the data and "the ability to make available, including to register, provide, restrict access or exchange certain data");
- **data users** (those who have lawful access to data for secondary use);
- and specifically for **personal data,** those of data subject, data controller and data processor in the sense of the GDPR

#### *iii. Rules and responsibilities*

EHDS foresees a number of obligations relevant from the perspective of data governance or the overall governance of a data space. Amongst them are:

- obligations regarding the (cross-border) availability, use and quality of data, minimum dataset specifications
- technical obligations regarding interoperability and security
- obligations regarding registration, conformity, marking, labelling and certification
- obligations regarding the handling of incidents
- obligations regarding certain administrative measures (such as obtaining permits for data uses, setting fees for data uses, etc.)

## 2.2 Initiatives, platforms, and projects

### 2.2.1 IDSA

The International Data Spaces Association (IDSA) is a global consortium that aims to revolutionize data sharing and facilitate secure and trusted data exchange in the digital ecosystem. The association brings together a diverse community of stakeholders, including industry leaders, research institutions, and policymakers, to collaborate on developing and promoting data sovereignty and data sharing standards. The primary aim of the IDSA is to establish the concept of International Data Spaces (IDS). An IDS is a decentralized and federated data architecture that allows individuals and organizations to maintain control over their data while enabling seamless data sharing and collaboration. By promoting the adoption of IDS, the IDSA seeks to empower data owners, improve interoperability, and foster innovation across industries.

As an entity that established the unified approach for the international data spaces and in compliance with the common system architecture models and standards (e.g., ISO 42010), the IDS's Reference Architecture Model (RAM) describes five layers that represent the diverse concerns and perspectives of stakeholders across different levels of granularity:

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

- The Business Layer defines and classifies the various roles that participants within the IDS can undertake. It outlines the key activities and interactions associated with each of these roles.
- The Functional Layer outlines the functional requirements of the IDS, along with the specific attributes to be derived from them.
- The Process Layer specifies the interactions among the various elements within the IDS.
- The Information Layer establishes a conceptual framework that incorporates linked-data principles to describe both the static and dynamic elements of the constituents within the IDS.
- The System Layer focuses on breaking down the logical software components, taking into account factors such as integration, configuration, deployment, and the ability to enhance and expand these components.

Along with five layers, the RAM presents three perspectives, which are needed to be implemented for all the layers: Security, Certification and Governance. The general structure of the RAM of IDSA is presented in Figure 2-9.

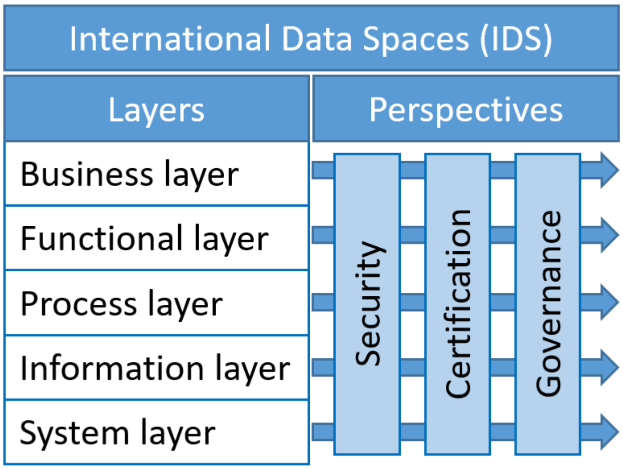


**Figure 2-9 – General structure of Reference Architecture Model**

The Governance perspective within the RAM provides a comprehensive view of the governance and compliance aspects within the IDS. It defines the roles, functions, and processes involved in ensuring secure and dependable corporate interoperability within the business ecosystem. The architecture of the IDS acts as a functional framework that provides adaptable mechanisms to meet the specific requirements of participating organizations. Within the IDS-RAM context, the Governance Perspective for the five layers.

The Business Layer

The Business Layer enables the creation and adoption of digital business models by the stakeholders involved in the IDS. It also defines the various key roles within the IDS, such as Data Owner, Data Provider, Data Consumer, Data User and App Provider. As such, it directly aligns with the Governance perspective by addressing the business standpoint on such topics as data ownership, data provisioning, and data utilization. Additionally to the key roles, the Business Layer defines the intermediary roles such as Broker Service Provider, Clearing House, Identity Provider, App Store Provider, Vocabulary Provider, Software Provider, Service Provider and Governance Body (and in this case IDSA is a Governance Body), which outlines essential service concepts such as data brokerage.

The Functional Layer

From the Functional layer point of view, the IDS Connector serves as the primary interface for enabling participation within the ecosystem. Regarding the Governance perspective, it is crucial to ensure interoperability and connectivity to ensure trust, security, and data sovereignty. In addition to the Clearing House and Identity Provider, which have a relation with governance, the functionality of certain technical core components (such as the IDS Connector or IDS App Store) also relates to the Governance perspective. In the scope of the Functional Layer, four functional levels are addressed in the IDSA procedures:

- Technical level, which focuses on provision of the software and hardware for controlled sharing of the data. I covers such topics as Identity and Authentication, Authorization, Data and Service Brokering, App Enabling, which are needed to be governed.
- Semantic level, which focuses on collaboration and minimization of the complexity of the interconnection between different key participants of the IDS and the mechanisms for semantic conversion need to be supported in the IDS architecture and controlled for enabling easy-to-use mapping between semantic models
- Organizational level, which focuses on how the expectations and procedures are aligned to achieve the aim for controlled data sharing, which includes the certification, aligned service level agreements (for example, for quality control) and aligned operations and customer processes to improve the efficiency of the IDS operation).
- Legal level, which focuses on the definition of the multi-lateral legal agreements between Data Providers and Data Consumers, joint legal agreement between all key participants of the IDS, verification of legal status for data transactions.

The Process Layer

The Process Layer presents a dynamic perspective of the architecture by illustrating the interactions among the various components within the IDS. Three main topic of the Process Layer, which are onboarding, data exchange, and publishing and using Data Apps, directly connects to the Governance Perspective. In terms of onboarding, the focus is on the interaction between Data Provider and Data User within the IDS. This includes activities such as acquiring identity, configuring the IDS Connector, provisioning and ensuring its availability, and establishing security setup for the IDS Connector. This setup involve using the Certification Authority certificate and identifying the respective IDS participant. As for the data exchange process, it involves governing the search of the Data Provider for the Data Consumer and invocation of the actual data operation. Regarding publishing and using Data Apps, guidelines are set for data processing or transformation within the IDS Connector, as well as for publishing data. These guidelines include adhering to the certification provided by the Certification Body to ensure proper storage and publication of data.

The Information Layer

The Information Layer outlines the Information Model, which provides a shared vocabulary for Participants to articulate their concepts. This framework establishes a basis for standardized collaboration and enables the utilization of the IDS infrastructure to establish individual agreements and contracts. The vocabulary employed within this layer holds significant importance within the Governance perspective due to its role in describing data through metadata within the IDS. Along with the vocabularies, this includes the governance of the Data App Interfaces.

The System Layer

The System Layer aligns with the Governance perspective as it encompasses the technical implementation of various security levels for the exchange of data among the Data Endpoints within the IDS. This includes the governance of the IDS Connector, its architecture, execution and configuration processes, IDS Data Broker and IDS Data Apps and App Store in order to meet the requirements specified on the Functional Layer.

### 2.2.2 GAIA-X

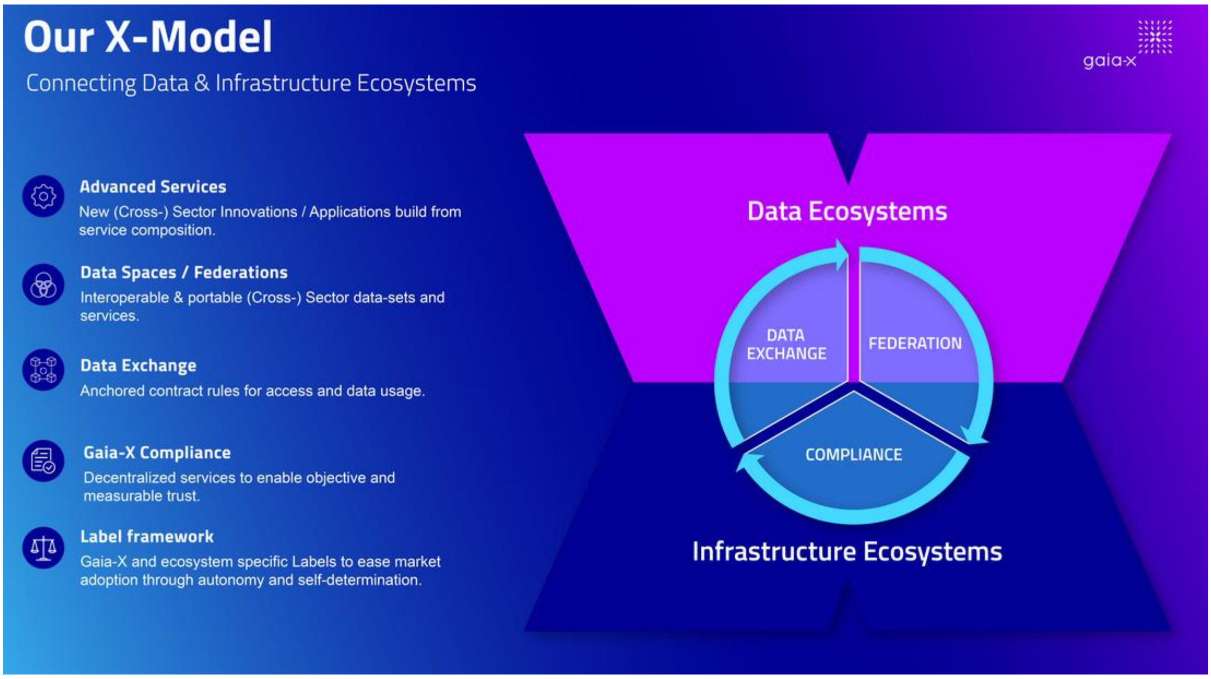
The Gaia-X Association for Data and Cloud AISBL (“Gaia-X”) is an international non-profit association incorporated in Belgium in 2021. The initiative for Gaia-X was taken in 2019 by the German and French Ministers of Economic Affairs, with the aim of developing a federated, sovereign, open and flexible data infrastructure, federated cloud services and a broader digital ecosystem based on open software, open standards and promoting European values. Gaia-X is in the process of developing common open standards, “technical specifications and harmonised rules for the secure sharing, interoperability and portability of users’ data between the different cloud service providers and users of cloud services.” [19] The role of Gaia-X is limited to that of offering facilities and services necessary for the function of the network/community, and which cannot otherwise be offered by the companies belonging to the network itself [20]. A federated network of Gaia-X hubs in several EU Member States function as one-stop-shops for the initiative. Gaia-X also supports the development of solutions for sector-specific data spaces, including energy data spaces. ENERSHARE project is one of the use cases.

Categories and uses of data

The infrastructure developed by Gaia-X supports the processing of **all categories of data**, both personal and non-personal.

- Gaia-X supports **sovereign data services, "**which ensure the identity of source and receiver of data and which ensure the access and usage rights towards the data".
- **Privacy-** and **security-by-design** are foundational principles of the Gaia-X architecture
- Gaia-X supports a **federation** of centralised and decentralised data sources
- Gaia-X facilitates interoperability and access to (personal) data **across data spaces**

Figure 2-10 and Figure 2-11 show Gaia-X model for connection data and general GAIA-X cross data space data sharing respectively.



Our X-Model

Connecting Data & Infrastructure Ecosystems

**Advanced Services**
New (Cross-) Sector Innovations / Applications build from service composition.

**Data Spaces / Federations**
Interoperable & portable (Cross-) Sector data-sets and services.

**Data Exchange**
Anchored contract rules for access and data usage.

**Gaia-X Compliance**
Decentralized services to enable objective and measurable trust.

**Label framework**
Gaia-X and ecosystem specific Labels to ease market adoption through autonomy and self-determination.

**Figure 2-10 - The Gaia-X framework for composable, interoperable & portable cross-sector data sets and services. Source: Gaia-X [21]**

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

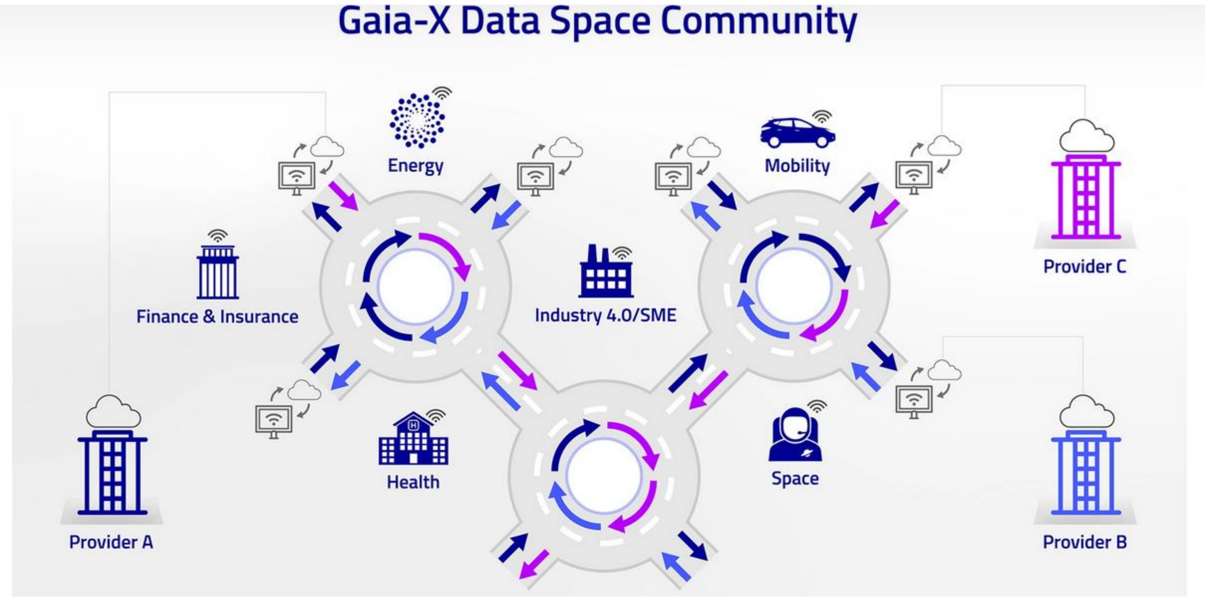


Figure 2-11 - Gaia-X cross data space data sharing. Source: Gaia-X [22]

Roles / Actors

Gaia-X defines two main categories of actors, namely: **users and providers**.

Gaia-X is open to membership by both **public and private organisations,** currently counting over 500 [23] **EU and non-EU members**.

The cooperation platform offered by Gaia-X is open to both **member and non-member** organisations.

Rules and responsibilities

Gaia-X employs a variety of technical and organisational measures to ensure the governance of data and processes. Amongst them:

- defining **guidelines, principles and standards** and corresponding objectives for maintaining neutrality, openness, transparency and data sovereignty.
- defining **minimum technical requirements** and services for the running of the federated Gaia-X Ecosystem, incorporating privacy-by-design and security-by-design principles
- defining **mandatory policy rules** [24] covering the European values of Gaia-X, and values including openness, transparency, data protection, security, and portability.
- defining a **compliance** framework and Certification and Accreditation services, and enforcing an automated compliance [25] mechanism, as part of the Trust architecture

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

- a Gaia-X **Data Space Business Committee** in charge of the development and application of Gaia-X deliverables in specific domains and of providing the link and support across the Gaia-X ecosystems
- a **General Assembly** consisting of all members with equal voting rights, except in certain occasions
- a **Board of Directors** composed exclusively of representatives of GAIA-X's European Members
- several **working groups** in charge of defining the Gaia-X requirements and made up of representatives of user groups and provider groups

The governance structure of GAIA-X association is presented in Figure 2-12.

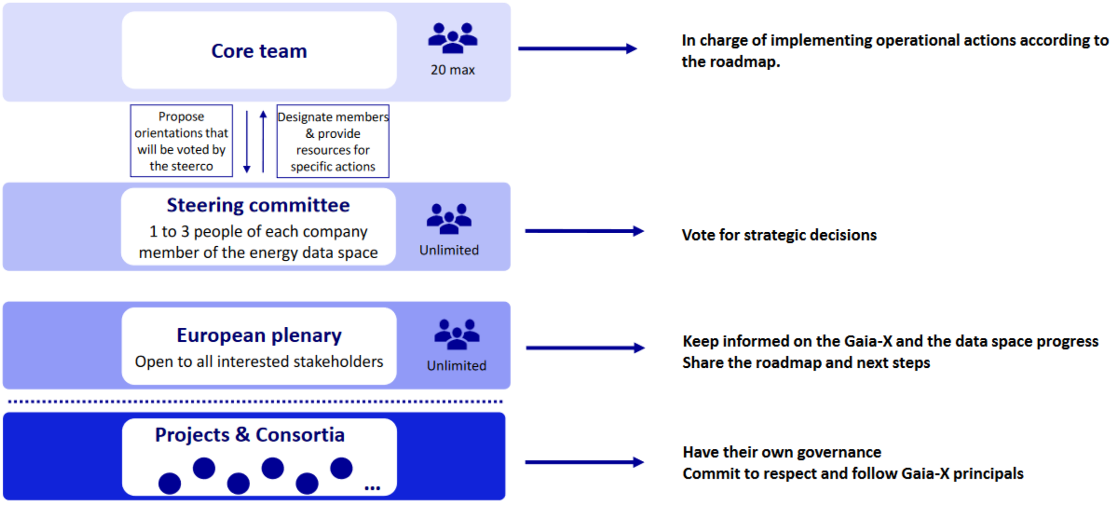

Core team
20 max
In charge of implementing operational actions according to the roadmap.
Propose orientations that will be voted by the steerco
Designate members & provide resources for specific actions
Steering committee
1 to 3 people of each company member of the energy data space
Unlimited
Vote for strategic decisions
European plenary
Open to all interested stakeholders
Unlimited
Keep informed on the Gaia-X and the data space progress
Share the roadmap and next steps
Projects & Consortia
...
Have their own governance
Commit to respect and follow Gaia-X principals

Figure 2-12 - Gaia-X governance structure for the definition and implementation of the energy data space strategy. Source: Gaia-V

### 2.2.3 FIWARE

The FIWARE Foundation is a non-profit organization that supports the development, promotion, and adoption of the FIWARE platform. It was established to provide governance, community management, and overall support for the FIWARE ecosystem. The foundation plays a crucial role in ensuring the sustainability and growth of FIWARE. It acts as a neutral entity that fosters collaboration and coordination among stakeholders, including developers, technology providers, end-users, and organizations interested in leveraging FIWARE.

FIWARE platform is an open-source platform that provides a set of standards, components, and tools for building smart applications and services in the context of the Internet of Things (IoT), smart cities, and other domains. It was initiated by the European Commission as part of their Future Internet Public-Private Partnership Program (FI-PPP). FIWARE offers a collection of

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

reusable software modules, known as Generic Enablers (GEs), which developers can utilize to build and integrate IoT-based applications and services more efficiently. These GEs cover various aspects of IoT, including data management, context processing, real-time processing, security, and user interface development.

One of the most important parts of the FIWARE ecosystem is Smart Data Models (SDMs) Program. It is an initiative that aims to provide a data modelling resources to allow connection between data coming from different sources and different industrial domains, such as smart cities, agriculture, transportation, energy, and more, provide data models tested in real case scenarios, provide answer to new data modelling needs at market speed and adopt open regulations and standards. It also allows actual data interchange between organizations by providing open licensed shared data models according to the principles of agile standardization. By integrating the SDMs within the FIWARE platform, developers can build smart applications and services that can easily exchange and process data using a common framework. This promotes interoperability, reduces integration efforts, and enables the development of scalable and reusable solutions in various domains.

The structure of the SDMs Program is presented in Figure 2-13.

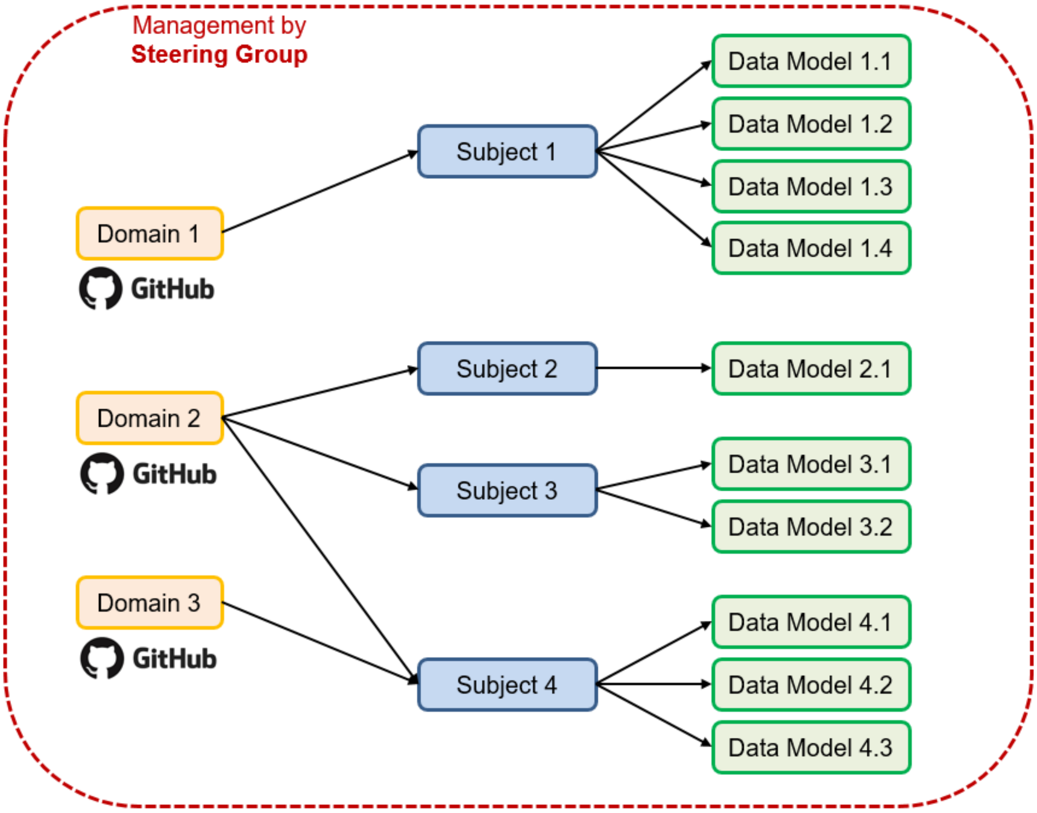


Figure 2-13 – Structure of SDMs Program

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

The SDMs Program has several “domains”, which represent different discipline or industrial sector, each “domain” has its own repository on GitHub. Each “domain” repository contains a number of sub-modules called “subject”, relevant to that “domain”, each “subject” has its own repository in the “domain” repository on GitHub. Important to mention that a “subject” can be linked from different “domain” repositories, for example “CrossSector Domain” allocate “subjects” that are not clearly assigned to a single “domain”. Each “subject” contains one or more “data models”. The Program is managed by a team composed by the Steering Group (FIWARE Foundation among the participants). Additional organizations may join globally or for specific application domains by signing a Memorandum of Understanding (MoU).

In order to license the data models, the preferable option for the SDMs Program is to use Creative Commons 4.0, which is a set of standardized licenses that enable creators to easily share their works while specifying the permissions and restrictions associated with them. If this licensing is not possible, the Apache 2.0 or other open licenses could be approved with several conditions: it is mandatory to recognize contributions, allow free use and modification of the data models and sharing the modifications, and do not impose other restrictions to use and adoption. In order for a contribution to be accepted, there are certain guidelines that every contributor must adhere to, considering both their perspective as a contributor and the perspective of the data model. Once all the guidelines have been followed, the administrators of the relevant "subject" being contributed to review and approve the modifications. Contributors will give a non-exclusive right for using their contributions according to the license, however these contributions can also be provided on other resources by the contributors with other licensing. Contributors guarantee that contributions are not subject to patents. Adoption of a Contribution License Agreement in line with the Project Harmony templates will be considered.

Additionally, the SDMs Program establish the coding standards and versioning policy in order to deal with all the potential needs of the data models and set of the guidelines for review of the data models to ensure the model consistency, such as:

- Application of coding guidelines
- Validation examples against data model schemas
- Completeness of documents associated to the data models
- Generation of CSV examples
- Etc.

The reports on the reviewing of data models will be sent to “subject” administrators with the request to fix the detected issues.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

### 2.2.4 OPEN-DEI

OPEN-DEI is a Horizon 2020 project aimed at harmonizing the digitalization of European industry, by aligning reference architectures, open platforms and large scale pilots, creating common data platforms based on a unified architecture and an established standard. The OPEN DEI project focuses on "Platforms and Pilots" to support the implementation of next generation digital platforms in four basic industrial domains: Manufacturing, Agriculture, Energy and Healthcare. The EU-funded OPEN DEI project operates within this framework to identify gaps, foster synergies, facilitate regional and national collaboration, and promote effective communication among the Innovation Actions that implement the EU Digital Transformation strategy.

OPEN-DEI's Position Paper titled *Design Principles for Data Spaces* [26], a collaborative effort between data space and industrial domain experts, established the fundamental design principles for constructing data spaces across sectors and initiatives. The significance of data spaces and the sovereign sharing of data in shaping the future data economy is emphasized in a position paper. It involved the active participation of over 40 data spaces and industrial domain experts, representing more than 25 organizations from 13 Horizon 2020 projects and related initiatives. This pioneering effort marks the initial step in defining the design principles, establishing agreements on the building blocks for a flexible infrastructure, and formulating governance guidelines for data spaces.

#### 2.2.4.1 Design Principles

The data space design principles defined in the paper are: Data Sovereignty, Data Level Playing Field, Decentralized Soft Architecture and Public-Private Governance.

<u>Data Sovereignty</u>

Data sovereignty refers to the inherent ability of individuals or organizations to exercise full control and autonomy over their economic data assets. This principle is a key and transformative concept that underlies the establishment of data spaces. Within the context of data spaces, data sovereignty offers two significant advantages to participants: firstly, it enables them to leverage enhanced capabilities in terms of data visualization, processing, management, and security; and secondly, it empowers them to retain control over their data while facilitating its accessibility to other entities.

<u>Data Level Playing Field</u>

To ensure fair competition among all participants in data spaces, it is essential to eliminate any insurmountable obstacles that new entrants may encounter, such as a quasi-monopolistic structure within the data ecosystem. A level playing field is established when players compete based on the excellence of their data and services rather than the quantity of data under their control. The creation of a level playing field for data sharing and exchange relies on fostering an ecosystem governed by cooperation rather than competition. This can be accomplished through meticulous design and robust maintenance of the underlying soft infrastructure that supports data spaces.

Decentralized Soft Architecture

The infrastructure supporting European data spaces will not be a centralized, monolithic IT system. Instead, it will comprise a diverse range of interoperable implementations of data spaces that adhere to a set of agreements encompassing functional, technical, operational, and legal aspects. This "soft infrastructure" will remain transparent to data space participants, encompassing both functional and non-functional requirements related to interoperability, portability, discoverability, security, privacy, and trustworthiness.

From a technical perspective, the soft infrastructure can be understood as a collection of interoperable IT platforms based on APIs (Application Programming Interfaces), wherein users have control over data flow through advanced mechanisms of identity and consent management. The design of the soft infrastructure will incorporate mechanisms that facilitate the economic exploitation of data sharing and exchange transactions, such as data monetization.

Importantly, the soft infrastructure for data spaces will be neutral to technology, granting actors the utmost freedom to make their own choices based on their engineering capabilities.

Public-Private Governance

To ensure the fair and effective design, establishment, and upkeep of a level playing field for data sharing and exchange, robust governance is crucial. It is essential that all stakeholder groups, including businesses, individuals, governments (both as data users and providers), technology partners, and IT professionals, feel adequately represented and engaged.

When building European data spaces, it is imperative to balance private interests with public values and interests. The representation of public values and interests can be achieved through appropriate legislation and regulation, with existing foundations already in place (eIDAS, GDPR, PSD). Further legislation and regulation, such as DGA, DSA, and DMA, are currently being prepared to address more specific aspects.

This public-private governance framework also assumes the responsibility of promoting widespread adoption of European data spaces. Effective communication of the concept to all stakeholders will require a significant and long-term effort. Additionally, establishing and maintaining a development community will be a critical focus area.

In the initial years of creating and maintaining the soft infrastructure and establishing data spaces on top of it, the public sector will play a vital role as an early adopter and provider of financial resources. As a critical mass is achieved, network effects will come into play, facilitating organic growth and adoption of European data spaces.

#### 2.2.4.2 Architectural Requirements

The paper also defines architectural requirements for the establishment of Data Spaces: Data-sharing empowerment, Data-sharing trustworthiness, Data-sharing publication, Data-sharing economy, Data-sharing interoperability, Data space engineering flexibility, Data space community.

Data-sharing empowerment involves ensuring that decisions can be made by the relevant stakeholders. This requires the availability of tools and organizational practices to support governance in data spaces, allowing the definition and monitoring of policies for data sharing. It also includes citizen engagement support, enabling citizens to participate in data sharing and exchange transactions. Additionally, data sovereignty support is necessary, granting stakeholders who own data the ability to govern its use. Lastly, federation plays a role by allowing the connection of multiple data platforms while retaining control over their respective operations.

Data-sharing trustworthiness entails ensuring that data spaces operate in accordance with expected requirements. This requires the development of data-sharing applications that support security-by-design, including the safeguarding of data space assets and the establishment of non-repudiable and unambiguous agreements. Additionally, privacy-by-design principles must be integrated into the development of data platforms and data-sharing applications, considering privacy concerns. Furthermore, assurance-by-design practices are necessary, incorporating security and privacy assurance requirements into the development process of data platforms and data-sharing applications.

Data-sharing publication revolves around the facilitation of data being made available for publication, thereby enabling data consumers to easily locate and access it.

Data-sharing economy focuses on creating the necessary conditions for data sharing and exchange. This requires the implementation of non-financial incentive mechanisms to encourage participation, as well as financial incentive mechanisms that include developing models for data monetization and methods for determining data value. Additionally, agreement mechanisms play a vital role in facilitating clear and effective arrangements for data sharing.

Data-sharing interoperability aims to enable seamless data exchange among applications within data spaces. This requires the establishment of data exchange APIs and data models that support semantic interoperability, ensuring a shared understanding of data meanings. It also

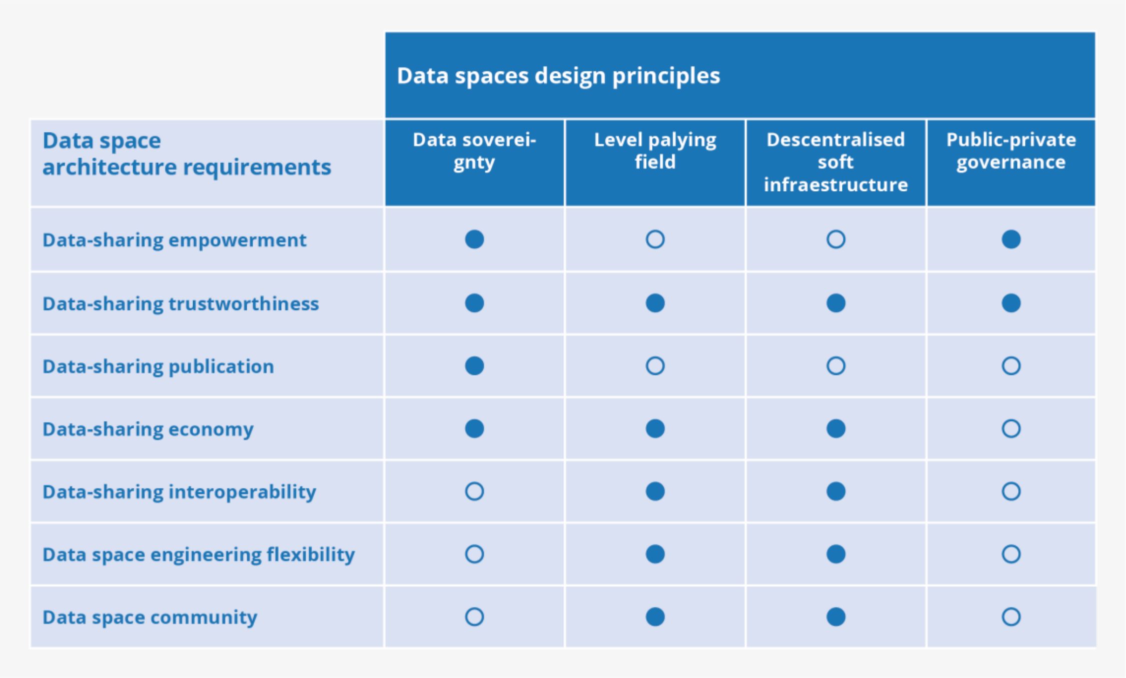
Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

entails behavioural interoperability, where the actual outcomes align with expected results when utilizing data exchange APIs. Additionally, policy interoperability ensures compliance with legal, organizational, and policy frameworks while maintaining interoperability among participating systems. By addressing these aspects, data-sharing interoperability enables effective and efficient data utilization and exchange within diverse application environments.

Data space engineering flexibility entails providing engineers with the capability to customize data-processing applications and platforms. This enables them to enhance data spaces in terms of interoperability, trustworthiness, and data processing. Interoperability flexibility allows for the extension of data spaces with specific interoperability capabilities. Trustworthiness flexibility involves incorporating tailored security, privacy, and assurance features into data spaces. Furthermore, data processing flexibility empowers engineers to augment data spaces with additional data-processing capabilities. By embracing these aspects of flexibility, engineers can adapt and optimize data spaces to meet specific requirements and improve their overall functionality.

Data space community aims to promote the widespread reuse of data space solutions by emphasizing several key aspects. This involves advocating for open solutions, ensuring that data space platforms and data-sharing applications are built on open specifications. Reusability is emphasized to enable easy replication of capabilities from existing data and marketplace platforms, as well as data-sharing applications. Open-source principles are encouraged, granting free access to data and marketplace components developed by communities. Lastly, sustainability of solutions is prioritized, providing assurance that solutions will remain available and maintained over an extended period. By focusing on these elements, the data space community fosters maximum utilization and longevity of data space solutions.

These requirements are correlated with the design principles defined previously, as shown in Figure 2-14.



| | Data spaces design principles | | | |
|---|---|---|---|---|
| **Data space architecture requirements** | **Data sovereignty** | **Level palying field** | **Descentralised soft infraestructure** | **Public-private governance** |
| Data-sharing empowerment | ● | ○ | ○ | ● |
| Data-sharing trustworthiness | ● | ● | ● | ● |
| Data-sharing publication | ● | ○ | ○ | ○ |
| Data-sharing economy | ● | ● | ● | ○ |
| Data-sharing interoperability | ○ | ● | ● | ○ |
| Data space engineering flexibility | ○ | ● | ● | ○ |
| Data space community | ○ | ● | ● | ○ |

**Figure 2-14 – Correlation the data space requirements with the design principles from OPEN-DEI's *Design Principles for Data Spaces***

### 2.2.4.3 Building Blocks

The project's position paper also establishes the building blocks required to build a Data Space that meets all their design principles and requirements and is in line with EU regulation. It divides these in two main groups: technical and governance building blocks.

Technical building blocks form the foundation for constructing the technical architecture of a data space. They consist of network protocols, middleware components, standardized APIs, and other relevant elements that enable secure and trustworthy data sharing among diverse parties. Various technical components have been developed or embraced by different European initiatives, such as FIWARE, Platform Industrie 4.0, CEF Digital, and the International Data Spaces Association. These advancements contribute to the creation and implementation of effective data spaces in Europe. The technical building blocks play a crucial role in facilitating the seamless integration of various systems and platforms utilized by participants within a data space, extending beyond the security boundaries of individual participants. Additionally, optional technical building blocks can be considered to enable the creation of systems that seamlessly connect to a data space, such as implementing big-data analysis, supporting data visualization and analytics, or providing interfaces with IoT networks. These building blocks empower data space participants to leverage data beyond their current business capabilities, unlocking new business cases and expanding the range of data usage scenarios. By leveraging these technical building blocks, data spaces can foster innovation and unlock the full potential of data for participants.

Governance building blocks are required, since integrating building blocks within data spaces, various sets of structuring principles can be applied, depending on specific domain or technical requirements. For instance, considerations may include streaming of data, high-frequency data, or event processing. However, regardless of the specific implementation, there are essential guiding principles that must be respected universally. These principles include decentralization, ensuring that control and decision-making are distributed across the data space; scalability, allowing the system to handle growing amounts of data and users; collaboration support, facilitating cooperation among participants; federation, enabling the connection of multiple data spaces; interoperability, ensuring seamless interaction between different systems and platforms; compatibility, promoting the ability to work together without conflict; trust management, establishing mechanisms for data trustworthiness and security; and auditability, providing the means to track and verify data actions and transactions. By adhering to these guiding principles, data space implementations can effectively address common requirements and promote successful integration.

Governance related roles in a data space are defined, with the following stakeholders being identified:

A **Data Owner** is an entity with the authority to control how their data is used by external parties. They can acquire data independently or through third-party tools and services. Data may be stored on-site, at the edge, or in the cloud. Data Owners have the option to keep their data private for internal use or share it publicly or with a limited number of third parties. When making data available to others, there are rights, obligations, and terms and conditions involved, typically outlined in Data Usage Policies. Data Owners can choose to provide data for free to promote scientific advancement and innovation or charge a fee based on their business model.

A **Data Acquirer or Data Provider** is an entity that collects and preprocesses data on behalf of a Data Owner. They offer services to the Data Owner. While the Data Provider handles the collection, processing, and storage of the data, the client (Data Owner) typically retains control over its subsequent usage. Recently, new business models have emerged where Data Providers offer their services at reduced prices in exchange for utilizing anonymized client data to improve existing services or create new ones. The Data Provider facilitates secure data exchange and sharing among participants in the data space, including data usage monitoring if requested by the Data Owner.

A **Data Processor** is an entity that utilizes specific types of data to create and offer new services in the market. These services can range from domain-specific applications to cross-domain

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

solutions. The value of the data used depends on its accuracy, availability, and relevance to the processing algorithms employed. The estimation and agreement of data value upfront can limit the data owner's ability to fully monetize their data, as they may not fully understand the additional value created or the value the new services hold for users. Control over data usage is typically governed by traditional contract documents, leading to manual operations and slowing down the complete utilization and monetization of data.

A **Data Marketplace Operator** is an entity that provides infrastructure and governance for data marketplaces. They offer various types of infrastructure and data-processing tools. The operator is responsible for marketplace governance, such as defining terms and conditions, managing datasets and participants, and providing support services. Data marketplaces are emerging as a new type of business that aims to facilitate seamless and automated data usage, eliminating the need for complex contracts. They can be cross-domain or domain-specific, focusing on specific industries or use cases. The primary role of a data marketplace is to ensure easy data discovery through standardized data models and transparent tracking of data transactions. Compliance mechanisms are implemented to enforce data usage policies, including restrictions on usage time, count, and application fields.

Figure 2-15 summarizes interactions between the business roles described above, as well as characterizing the data flow between them.

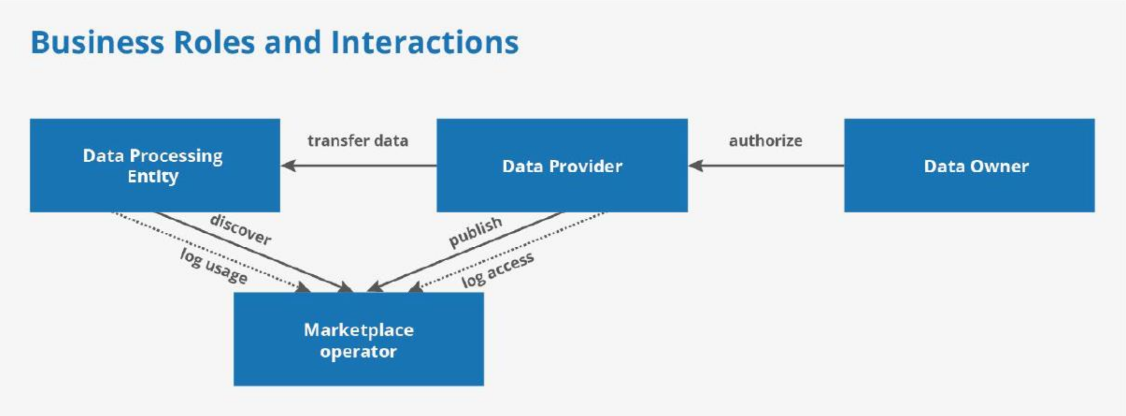


Figure 2-15 – Business roles and interactions, from OPEN-DEI's *Design Principles for Data Spaces*

In a data-driven business, the quality of data is crucial for its success. The responsibility for ensuring data quality starts with the Data Owner and then goes over to all parties involved in the data value chain. This includes proper installation and calibration of sensors, as well as the correct application of data-processing algorithms. To maintain a reliable data value chain, service level agreements (SLAs) can be established between stakeholders. These SLAs, often incorporated into smart contracts, govern the provision of services and can complement data usage policies. Compliance with rules regarding data usage by third parties is an important

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

aspect of business relationships. However, Data Owners have limited control over how their data is used. Enforcing data usage restrictions requires a combination of organizational rules, legal contracts, and technical solutions. Control points at different layers of data-processing systems are necessary for comprehensive usage control, varying in complexity depending on the specific context.

Still under the governance umbrella, the business building blocks that are required for a data space and which will establish the business relationships between the different actors with different business roles are specified. These include Operational SLA, Accounting Scheme, Billing/Charging Scheme, Data Valuation method and Smart Contracts:

Operational SLA: Provides specification of a service and the standards that it should meet

Accounting Scheme: Specifies data-sharing parameters to be recorded and reports to be produced

Billing/Charging Scheme: Specifies rules that lead to the billing/charging of services provided over the data space

Data Valuation method: Estimates the value of data shared by organizations in the data space

Smart Contracts: Provides a protocol for implementation of an agreement between two or more parties

In order to have a functioning and healthy Data Space, data sovereignty, trust and security are key, as they are necessary conditions for organizations to be willing to share their data, with the guarantee that it won't be misused. Data sovereignty in data sharing and exchange necessitates the establishment of both organizational and operational agreements. These agreements not only facilitate the implementation of data usage policies but also instill trust in the entire data ecosystem by serving as a foundation that bridges the physical and digital realms. The interoperability of the overall system relies on agreements that ensure compatibility among all participants. It is crucial to maintain and synchronize an appropriate interoperability scheme across all parties involved. Furthermore, governing bodies play a vital role in providing a framework for all business transactions within data spaces, including the reliable upkeep of underlying agreements. Therefore, OPEN-DEI includes in their governance building blocks the following related to interoperability, trust and administration:

Domain Data Standard: Provides the syntax and semantics for data exchange and data sharing on different levels

Unique Identifiers: Identification of legal entities, natural persons, or things in terms of a unique identifier and other information about an entity

Authorization Registries: Verification and validation of digital identities and their mapping to real-world objects

Trusted Parties: Provide neutral evidence on specified facts based on predefined criteria

Data Space Boards: Provide governance for data spaces in terms of decision-making, guidance, steering, and conflict resolution.

Overarching cooperation Agreements: Provide functional, technical, operational and legal agreements. While some agreements are reusable in a generic or sector-specific way (e. g. rule books), others are use-case specific.

Continuity Model: Describes the processes for the management of changes, versions, and releases for standards and agreements. This also includes the governance body for decision-making and conflict resolution.

Regulations: Laws or administrative rules, issued by an organisation, used to guide or prescribe the conduct of the members of that organisation or countries.

#### 2.2.4.4 Governance and Business Models

The paper emphasizes the importance of establishing data spaces with a harmonized approach to enable data sharing and exchange while ensuring data sovereignty and user control. The focus lies more on coordination and scaling rather than technological challenges. Data spaces refer to interoperable data-sharing applications in specific sectors, and the goal is to harmonize technical, operational, functional, and legal aspects to create a unified "soft infrastructure" for cross-sectoral data space interoperability.

The proposed Data Governance Act (DGA) aims to create a two-tier governance structure with a governance entity for each data space and an overall governance organization for common aspects of interoperability and data sovereignty. The act envisions a general authorization framework for data intermediaries like data marketplaces and brokers to ensure compliance with data sharing rules. The authors propose the establishment of a 'Data Exchange Board' (DEB) responsible for developing and maintaining the general authorization framework and soft infrastructure.

The DEB will work in coordination with data space governance entities to define the general authorization framework and specific data-sharing aspects for each use case. The process will leverage existing research and experience in data spaces to achieve a unified user experience across data spaces. Collaboration among EU stakeholders is emphasized, as well as leveraging existing governance structures to establish optimal governance for European data spaces.

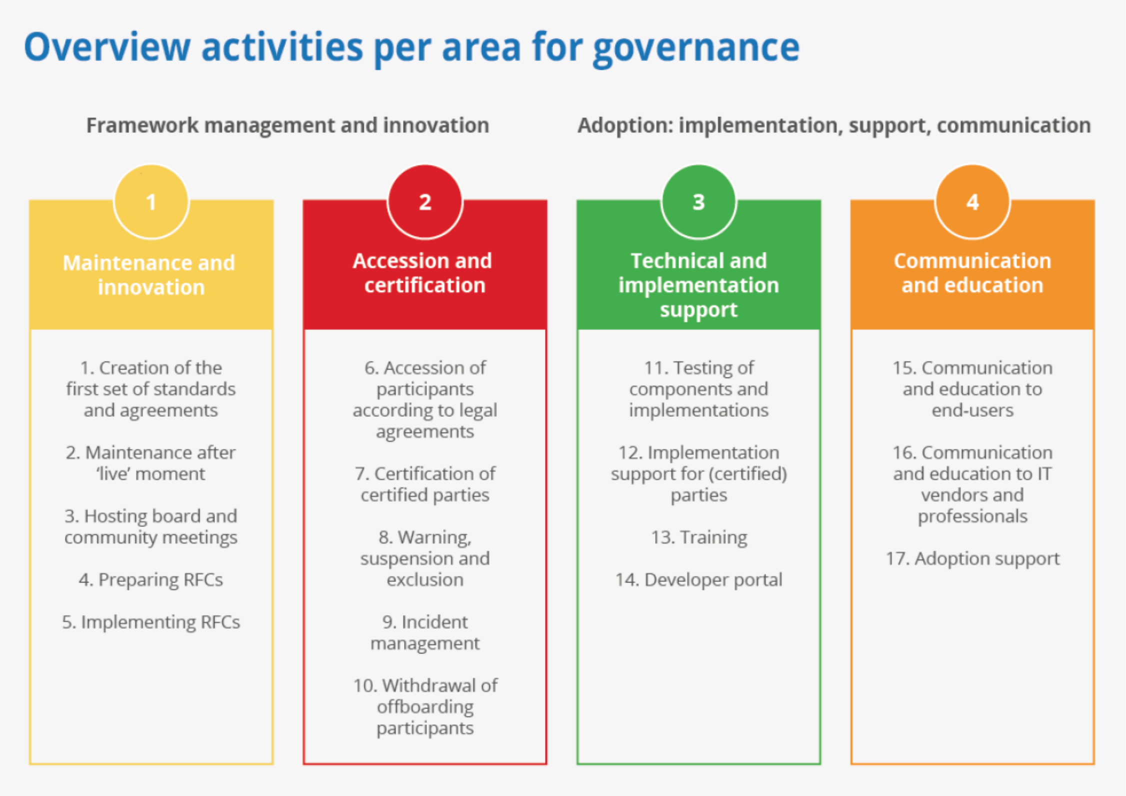
Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

OPEN-DEI has categorized topics of governance into four main areas, as can be seen in Figure 2-16:

Maintenance and further development of the set of agreements and standards defining the 'soft infrastructure' (i.e. of the authorisation framework);

Admission and certification of the members of the network (i.e. of all data intermediaries);

Communication and education, aiming both at end users and IT vendors/professionals.



Overview activities per area for governance

Framework management and innovation

Adoption: implementation, support, communication

1 Maintenance and innovation

1. Creation of the first set of standards and agreements

2. Maintenance after 'live' moment

3. Hosting board and community meetings

4. Preparing RFCs

5. Implementing RFCs

2 Accession and certification

6. Accession of participants according to legal agreements

7. Certification of certified parties

8. Warning, suspension and exclusion

9. Incident management

10. Withdrawal of offboarding participants

3 Technical and implementation support

11. Testing of components and implementations

12. Implementation support for (certified) parties

13. Training

14. Developer portal

4 Communication and education

15. Communication and education to end-users

16. Communication and education to IT vendors and professionals

17. Adoption support

Figure 2-16 – Activities in four areas of governance

### 2.2.5 OneNet

The OneNet European project has the ambition to create a fully replicable and scalable architecture that enables the whole European electrical system to operate as a single system, with a variety of markets that allow the participation of stakeholders regardless of their physical location – at any level, from small consumers to large producers. From a data governance perspective the OneNet System is a reference due to several pilots that are testing it in the ongoing project.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

One of the primary objectives during the design and development of the OneNet data exchange framework was to enable the availability and accessibility of data from various sources while ensuring security, trust, data ownership, and privacy. To achieve this, the OneNet architecture incorporates several key elements:

1. Data Providers and Data Consumers: The OneNet framework defines clear roles for data providers, who are the sources of data, and data consumers, who are the entities or applications that utilize the data. This distinction helps in managing data flows and interactions within the framework.
2. Fully Decentralized Data Exchange: OneNet implements a fully decentralized approach to data exchange, enabling direct peer-to-peer interactions between data providers and data consumers. This approach eliminates the need for intermediaries and promotes a more efficient and secure data exchange process.
3. Data Ownership and Consent Management: OneNet prioritizes data ownership and consent management to ensure that data is exchanged with the explicit consent of the data owners. It incorporates mechanisms and protocols to manage data ownership rights, permissions, and consent, maintaining privacy and compliance with relevant regulations.
4. Secure and Interoperable Cross-Platform Integration: The OneNet framework facilitates the seamless integration of data across different platforms, systems, and applications while ensuring security and interoperability. It employs standardized protocols and interfaces to enable efficient and secure data exchange, allowing diverse platforms to communicate and interact effectively.

The design process of the OneNet architecture combines bottom-up and top-down perspectives. The first involves designing the solution based on the use cases, requirements, and specifications gathered from the end-users, which, in this case, are the demonstration clusters of OneNet. This approach ensures that the architecture addresses the specific needs and challenges identified by the end-users. By collecting input from the users, their perspectives and requirements are taken into account, resulting in a more user-centric design. The top-down approach, on the other hand, takes into account the objectives and results already set and consolidated. It provides a high-level perspective and guides the design process based on pre-defined goals and outcomes. This approach ensures alignment with the overarching objectives of the OneNet project like the cross-border participation of stakeholders at all levels, platforms' integration and cooperation for cross-platform market and network operation services and make available and accessible data from different stakeholders in a secure and trusted way ensuring data ownership and privacy. These objectives are also aligned with the ENERSHARE goals.

In the Figure 2-17 is presented the OneNet architecture.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

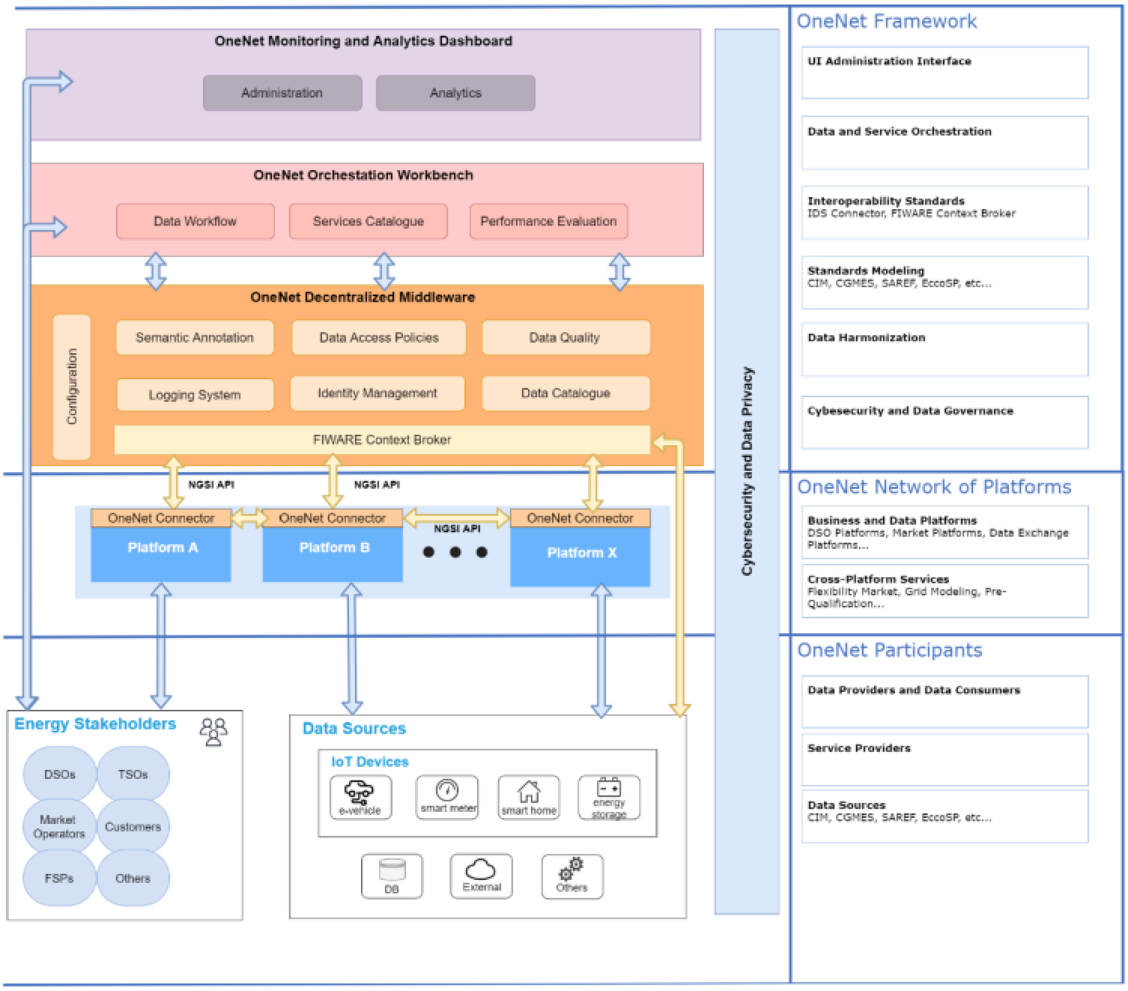


Figure 2-17 - OneNet architecture

The bottom layer of the OneNet System Architecture includes the different data sources and data and service providers/consumers. The middle layer enables the establishment of an OneNet Network of Platforms, encompassing all participating platforms engaged in data exchange and cross-platform service utilization. This layer introduces the initial component provided by OneNet, known as the OneNet connector. The top layer, known as the OneNet Framework, constitutes the central element of the OneNet Architecture. It encompasses all the components that will be implemented in the reference implementation along with the essential specifications for data harmonization, ontologies, data modelling, service orchestration, workflow monitoring, analytics, and more.

In the design of the OneNet system, data governance plays a crucial role due to the emphasis on making data available and accessible from different sources while ensuring data ownership, privacy, and trust. It is interesting to understand better how the OneNet architecture addresses:

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

- The Data providers and data consumers: the OneNet architecture comprises varius participants and components that enable data integration and exchange like: Data Sources that can be integrated, such as a database, IoT device, or file system; Data Providers that are the participants that provide data to the system, using the OneNet connector to ensure compliance; Data Consumer recipients of data from Data Providers, who can search for datasets using the OneNet Connector; Service Provider that are the participants offering data services or tools, registered in the OneNet framework for integration and utilization.
- The implementation of a fully decentralised data exchange platform: The OneNet architecture is characterized by its fully decentralized approach, implemented through the OneNet Decentralized Middleware and OneNet Connector. The Decentralized Middleware acts as a layer on top of the IT infrastructure, facilitating information exchange between assets and components within the OneNet Network of Platforms. It also provides centralized features like identity management and data discovery. The OneNet Connector, a specific instance of the Decentralized Middleware, is deployed in each participant's IT environment to enable easy integration, cooperation, and data ownership preservation. It ensures scalability for real-time data integration and supports multi-country and multi-stakeholder decision-making services. This decentralized infrastructure allows direct interaction between entities without the need for intermediaries, creating an interoperable network for Data Providers and Data Consumers.
- Cross-platform integration in a secure and interoperable way and definition of data ownership and consent management: The OneNet solution is implemented based on the International Data Space (IDS) concept, specifically its Reference Architecture Model (RAM) and the trusted data exchange framework. The alignment with IDS ensures interoperability and connectivity among participants while emphasizing data security, governance, and trust. The IDS components, such as the Data Management Interface, IDS connector, broker service, clearing house, and app provider, are integrated into the OneNet architecture. The IDS Data Governance Model, which defines the roles and decision-making framework for data usage, is also closely aligned with the Data Governance Model in OneNet.

The OneNet Architecture incorporates several key concepts from IDS:

- Data interoperability: OneNet focuses on efficient data exchange by enabling a common language, standardized interfaces (e.g., APIs), and shared data models. It also includes mechanisms for traceability, logging of data transactions, and data provenance.
- Data sovereignty and trust: OneNet ensures participants can trust each other and maintain control over their own data. This involves implementing identity management standards, verifying data truthfulness, and enforcing data access and usage control policies.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

- Data value creation: OneNet supports the creation of data markets where participants can derive value from data sharing, forming data value chains. This includes defining terms and conditions, such as pricing, for data usage and sharing, facilitating publication and discovery of data offerings, and managing permissions for data access and usage.

Other aspects related to the data governance are the data quality, data standards, data access management and data security.

The data quality assessment plays a crucial role due to the emphasis on data exchange. The assessment process involves identifying and addressing business and technical issues related to data, enabling data cleansing and enrichment using appropriate data quality tools. This ensures a high level of data quality and is performed for every data-related operation.

To achieve good data quality, OneNet establishes a Data Quality Framework and sets of Data Quality Requirements. The framework follows a 5-step process: Scope definition, Data exploration and profiling, data quality assessment, data quality improvement and lastly monitoring and control. The OneNet data quality assessment incorporates data quality requirements based on the ISO 25012 standard's Data Quality Dimensions (ISO2500, 2022). These dimensions include: Accuracy, Completeness, Consistency, Credibility, Currentness, Accessibility, Compliance, Confidentiality, Efficiency, Precision, Traceability, Understandability, Availability, Portability and Recoverability.

Data quality standards play a crucial role in ensuring compliance with data policies by providing an overarching framework. These standards encompass various aspects such as data modelling, naming conventions, metadata management, and more. This process commenced with the establishment of 10 categories of cross-platform services to classify and identify services to be supported in a harmonized manner within the OneNet system. For each harmonized cross-platform service, specific characteristics were defined, including:

- Unique ID and textual description
- Data process method (GET data or POST data)
- Actors involved (Data Providers and Consumers mapped to roles in the Harmonized Electricity Market Role Model)
- Exchanged Business Objects
- Data quality requirements
- Data format and standard data models

These results are incorporated into the OneNet implementation, particularly in the OneNet Middleware and OneNet Connector. They support standardized data exchange, including the use of standard data models based on the Common Information Model (CIM) and semantic validation.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

The OneNet system implements a comprehensive data access control and usage management framework, which goes beyond traditional access control methods such as Role-Based Access Control (RBAC) or Attribute-Based Access Control (ABAC). It incorporates the concept of Data Usage Control from the International Data Spaces (IDS) architecture guidelines [27].

Data usage control expands upon data access control by specifying and enforcing restrictions on how data should be processed, ensuring compliance with intellectual property protection, regulatory requirements, and digital rights management. In the IDS architecture, usage control is applied at the data level, governing the actions that can be performed on the data once access is granted.

In the OneNet system, the roles of Data Providers and Data Consumers are crucial. Data Providers define access and usage policies based on the IDS reference model, which encompass both access control and usage control. These policies are enforced through the OneNet Connector's Usage Control (UC) App, which is available to all participants in the OneNet ecosystem. This ensures that every platform connected to OneNet adheres to the defined policies during data exchanges.

The UC App within the OneNet Connector offers a range of pre-defined policies for the project's demonstrators and use cases, and it can be extended with new policies and classes as needed. The OneNet Data Access Policies (DAP) Framework, following the IDS reference model, provides a standardized approach to data access and usage control within the OneNet system, enhancing security and governance capabilities.

In what regards to the security data domain, the OneNet system prioritizes data security and cybersecurity to protect data from cyber threats, unauthorized access, and breaches. It ensures the confidentiality, integrity, and availability of data throughout its lifecycle. The system also addresses cybersecurity concerns, which focus on protecting the infrastructure of systems and networks. It follows industry standards and best practices for power systems and smart grids, requirements for power system management, security of industrial automation and control systems, information security management, and cybersecurity considerations specific to smart grids. The system incorporates specific cybersecurity measures, dedicated components, and a testing environment for secure service deployment.

Given the nature of smart grid networks that connect critical energy infrastructure with consumer-facing technologies and services, the privacy principles of the GDPR (General Data Protection Regulation) play a crucial role in compliant data processing, particularly when dealing with customer data and personally identifiable information. Data controllers must fulfil their obligations, and individuals' rights regarding data protection must be respected. Ethically, the collection and processing of personal data should be non-invasive. The OneNet system aligns with the EU's Data Protection Framework, Information Security Framework, Smart Grid Security (NISTIR 7628), and GDPR to ensure privacy and data protection.

To support all these aspects and ensure effective data governance, the OneNet project has designed and implemented a specific Data Governance Framework. This framework consists of five important dimensions:

1. Structure: It defines the organizational structure, roles, and responsibilities related to data governance within the OneNet ecosystem. The implementation of specific roles for data provisioning and consumption enables end-to-end data exchange processes in OneNet. The decentralized approach ensures that data exchanged during platform integration and cross-platform services remains stored within each participant's environment. The OneNet Middleware and Connector facilitate the use of metadata for defining data exchange processes while preserving the confidentiality of the actual data exchanged. The categorization of cross-platform services promotes data structuring, standardization, portability, and interoperability.
2. Access: It addresses policies and mechanisms for controlling access to data, ensuring that only authorized entities or applications can access and utilize the data. OneNet participants have the flexibility to assume the roles of Data Providers and/or Data Consumers and establish their own access policies for data exchange. The Identity Manager within the OneNet Middleware ensures the secure identification of participants, establishing a trusted data space for collaboration. A dedicated security layer guarantees authentication and authorization.
3. Usage: This dimension focuses on guidelines and rules for data usage, including restrictions, permissions, and compliance requirements, to ensure responsible and ethical data handling. OneNet goes beyond traditional access management by incorporating the IDS concept of usage control, which enables the specification and enforcement of data processing restrictions. This includes ensuring intellectual property protection, compliance with regulations, and digital rights management. Usage control, in conjunction with access management, is implemented within the OneNet Connector through a dedicated application called the Usage Control App. It focuses on governing data processing requirements rather than data access provisions.
4. Standardization: OneNet promotes the standardization of data formats, protocols, and interfaces to enable seamless integration and interoperability among different systems and platforms. The OneNet system encompasses over 60 diverse cross-platform services categorized into 10 distinct groups. Each service is accompanied by defined data formats and models, promoting integration and collaboration between platforms. This approach guarantees the portability, reusability, and interoperability of data across the OneNet ecosystem. Additionally, the system provides a data harmonization tool that maps commonly used CIM standards from XML to the JSON-LD schema, enabling support for the NGSI-LD (Next Generation Service Interfaces - Linked Data) standard.
5. Integrity: This dimension encompasses measures to maintain data integrity, including data quality assurance, validation, and verification processes. The OneNet Connector uses the FIWARE Context Broker and follows the NGSI-LD standard for data exchange.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

This ensures standardized verification of data quality and allows for the implementation of semantic tools and ontologies.

All the processes within the OneNet project rely on these five dimensions of the Data Governance Framework to ensure effective and responsible management of data throughout the data exchange ecosystem. In the Figure 2-18 is presented the implementation of the data exchange process using the OneNet Data Governance Framework.

The Cybersecurity Layer is essential for secure communication and data exchange in the OneNet system. It incorporates multiple mechanisms, including OAuth2.0 tokens for participant identification, secure interfaces for data access and usage control, monitoring of traffic and events, and AI-based detection of malicious network activities and cyber threat attacks.

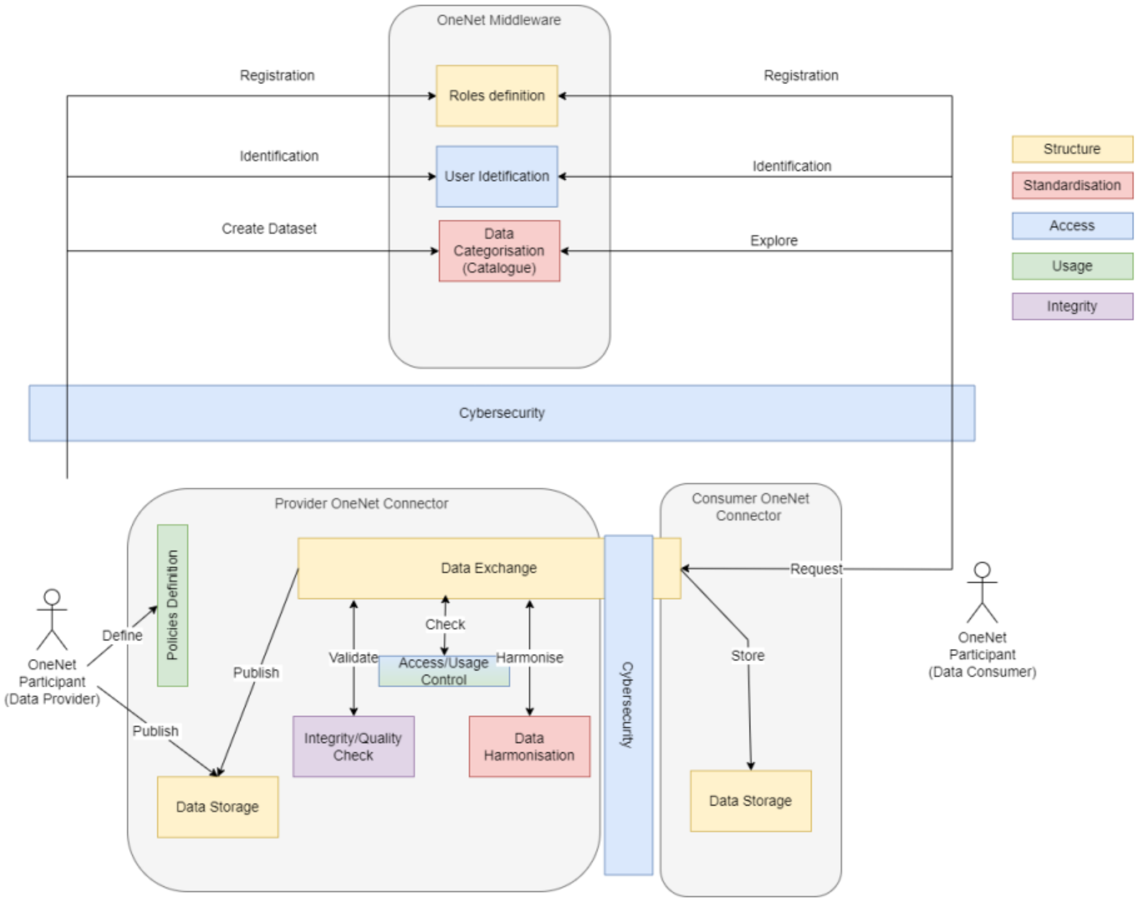


Figure 2-18 – OneNet data exchange process using Data Governance Framework

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

### 2.2.6 BD4NRG

BD4NRG aims to tackle emerging challenges in big data management for the energy sector through an innovative and comprehensive solution. Their approach involves an open, holistic framework that utilizes smart grid-tailored, near real-time, energy-specific, and AI-based open Big Data Analytics. The overarching vision is to provide holistic services for optimal management of Electric Power and Energy Systems throughout the value chain.

The services offered by BD4NRG cover a wide range of areas, including risk assessment for energy efficiency investment planning, optimized management of grid and non-grid assets, enhanced efficiency and reliability of electricity network operations, and the promotion of fair energy prices for consumers. Additionally, BD4NRG aims to lay the foundation for an EU-level energy-tailored data sharing economy.

As a big data platform, BD4NRG requires a data governance framework to ensure an appropriate management across the entire data value-chain. In summary, the BD4NRG Governance Layer is comprised of a FIWARE compliant-DLT/blockchain-based implementation for a decentralized data sovereignty and governance architecture for cross-entity data sharing. This architecture integrates IDSA and GAIA-X conceptual architectures and seamlessly integrates the FIWARE Context broker with hybrid IoT/blockchain off-chain data sharing solutions. The scalability of the infrastructure is achieved by utilizing the blockchain for hash storing, which uniquely refers to the information content managed off-chain in a decentralized way (e.g., IPFS). This approach provides the benefits of immutability, traceability, accountability, and notarization/time stamping offered by Distributed Ledgers and blockchain technologies while effectively managing the inherent difficulty of scaling up in DLT. The middleware acts as a mediator between data users (Applications and Tools) and data providers, allowing providers to decide case by case whether to disclose their data or not. State-of-the-art solutions are utilized to guarantee traceability, provenance tracking, and accountability. Figure 2-19 shows the BD4NRG Overall Data Architecture.

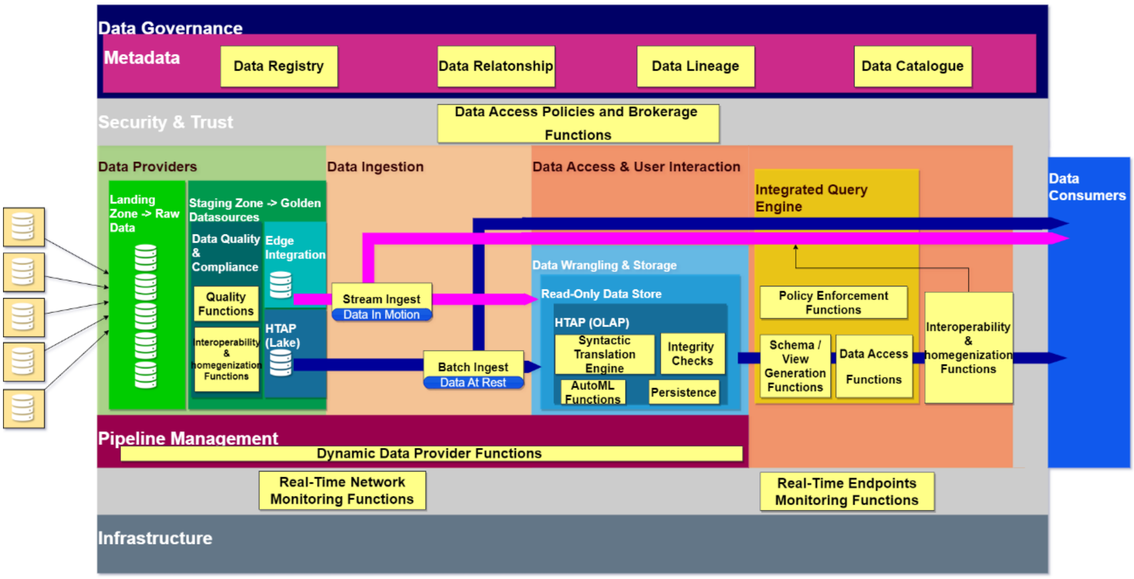


Figure 2-19 – Overall Data Architecture: BD4NRG Data System

The architecture of the BD4NRG system is structured into three vertical layers that focus on specific aspects of data processing, supported by two horizontal layers that address cross-cutting issues. These layers operate within a common infrastructure. It's important to note that the vertical layers do not strictly adhere to a layered architecture model, as data can be served to consumers or client applications without undergoing processing.

The purpose of each layer is as follows:

Data Providers: This layer introduces new data into the BD4NRG system for discovery, transformation, analysis, and access. Data can originate from various sources such as static files, social media, third-party services, and intelligent devices. Within this layer, raw data undergoes processing to create high-quality datasets, including metadata and adherence to interoperability standards.

Data Ingestion & Management: This layer is where data enters the BD4NRG system and is distributed for immediate use or storage. It encompasses two mechanisms: real-time streaming ingestion for data in motion and batch ingestion for data at rest. The choice of mechanism depends on the specific application use case.

Data Access & User Interaction: This layer enables access and navigation of the data, supporting the generation of different business views. It includes a high-performance real-time analytics database for interactive dashboards and analytics platforms. It also serves as a data warehouse and provides a query engine for presenting logical views of data to consumer applications.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

Data Governance: This layer ensures data stewardship, classification, transparency, discovery, ownership, and quality through data governance processes. It incorporates business and technical metadata to facilitate effective data management.

Security & Trust: Responsible for maintaining security and trust beyond anonymization and privacy measures. This layer defines and enforces data access policies and implements monitoring functions at the infrastructure level.

At the core of the BD4NRG system is the Infrastructure layer, which handles networking, computing, and storage requirements. It ensures the cost-efficient, secure, and scalable storage and transfer of large and diverse data formats. The infrastructure is designed to handle massive quantities of data, scale with organizational growth, and provide the necessary input/output operations per second (IOPS) to deliver data to applications.

The software components for ensuring the different aspects of data governance in the BD4NRG platform are the following:

- DLT & Smart contracts for B2B cross-stakeholder trusted off-chain data sharing and re-use.
- Data Access Policy Brokerage.
- Legal, Regulatory, Privacy and Cyber-security Management and Compliance Tools.
- Data Quality Compliance and Certification Tools.
- Interoperability and Homogenization.
- Seamless Elastic Distributed Data Management and HTAP (Heterogeneous Data Capture, Cleansing, Integration, Polyglot Persistence).
- Integrated Querying of Streaming Data and Data at Rest.
- Automated Parallelization of Data Streams and Intelligent Data Pipelining.

### 2.2.7 BRIDGE

BRIDGE is a European Commission initiative which unites Horizon 2020 and Horizon Europe Smart Grid, Energy Storage, Islands, and Digitalisation Projects. Its main goal is to systematically address common challenges that arise during the demonstration projects, potentially hindering innovation. The BRIDGE process encourages continuous collaboration and knowledge exchange among these projects that allow them to deliver conclusions and recommendations about the future exploitation of the project results, with a single voice, through four different Working Groups representing the main areas of interest:

- Data Management;
- Business Models;
- Regulations;
- Consumer and Citizen Engagement.

In the scope of the Data Management Working Group, the main work is focused on:

- Communication Infrastructure, which involves both technical and non-technical aspects of the communication infrastructure needed to exchange data and the related requirements, including challenges encountered by TSO and DSO;
- Cybersecurity and Data Privacy, entailing data integrity, customer privacy and protection;
- Data Handling, which involves establishing a structured framework for data exchange and related roles and responsibilities, addressing technical challenges to ensure secure and interoperable data exchange, and the data analytics techniques for data processing.

One of the key reports of the Data Management Working Group is the European (energy) data exchange reference architecture (DERA), which is produced yearly. The latest version of this report is version 2.0, which was published in June 2022. The objective of this report is to contribute to the discussions and take tangible actions to achieve truly interoperable and business process agnostic data exchange arrangements at a European level. This effort extends not only within the energy sector but also across various other domains, aiming to foster data exchange practices. The version 2.0 presents an improved DERA according to the survey, conducted within the scope of the first DERA report. Figure 2-20 shows the reference architecture from the DERA 2.0 report.

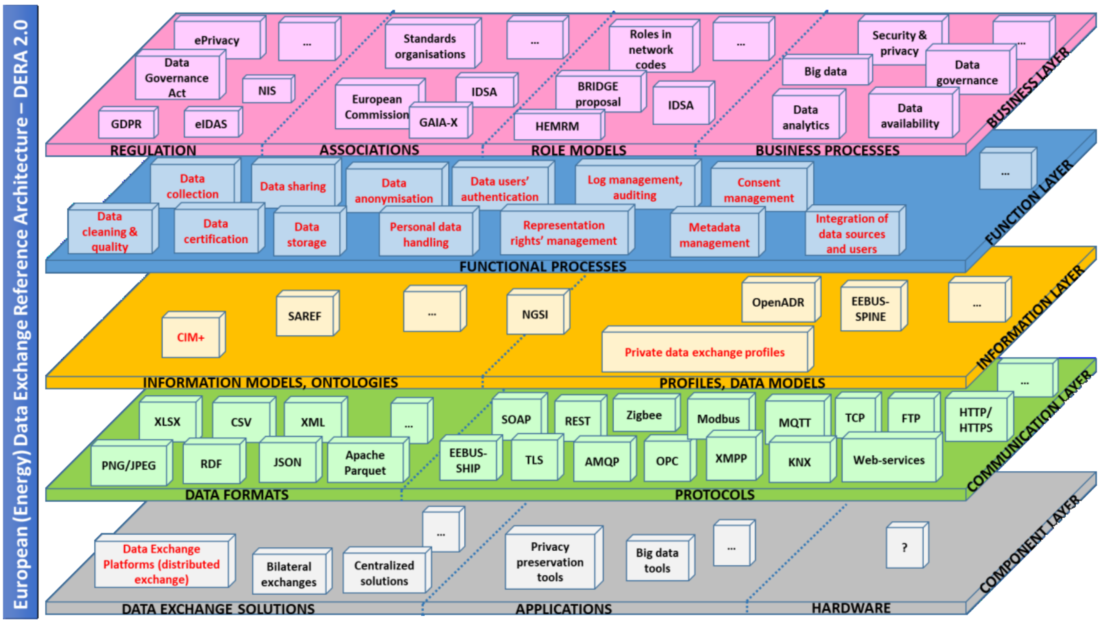


Figure 2-20 – European (energy) data exchange reference architecture from DERA 2.0 report (BRIDGE)

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

This architecture is based on the Smart Grid Architecture Model. It was proposed by CEN, CENELEC and ETSI Smart Grid Coordination Group in 2012 as the response for the issued mandate from European Commission to develop an interoperable framework for standardisation in the field of Smart Grids – Mandate M/490 [EC, 2011]. The SGAM Framework can be used for designing and assessing smart grid use cases and link these to standards, including identifying missing standards, in order to support interoperability on all layers of SGAM. However, the DERA 2.0 is not only about data exchanges between system operators (TSOs, DSOs), but addresses any data exchange involving any stakeholder (e.g. consumer, market operator, energy service provider, energy supplier, flexibility provider). This architecture contains five interoperability layers: Business, Function, Information, Communication and Component layers.

Business layer

The business layer represents, in principal, the business perspective on the information exchange. This layer is responsible for aligning regulatory and economic (market) structures and policies, business models, business portfolios (products & services) of involved market parties, as well as business capabilities and business processes [28]. It also can be divided in four sub-layers:

- Regulation sub-layer, which focuses on the proper implementation of not only the specifically electricity domain directives, such as Clean Energy Package, but also cross-sector interoperability GDPR, European Data Strategy, including Data Governance Act, regulations on electronic identification, authentication and trust services (eIDAS), directive on security of network and information systems (NIS) and others.
- Associations sub-layer, which focuses on different initiatives and associations for both electricity and cross-sector interoperability. These associations include ENSTO-E, EU DSO Entity, IDSA, European Standardisation Organisations (ESOs), and initiatives like GAIA-X.
- Role models sub-layer, which focuses on the business roles, which would enable unified understanding of the parties involved in a process. Along with the roles from the network codes and IDSA, the business roles for DERA 2.0 are also based on the Harmonised Electricity Market Role Model (HEMRM), which seems to be the most widely used role model, including Horizon2020 projects.
- Business processes sub-layer, which describes generic processes in electricity and cross-sector.

Function layer

The purpose of the function layer is to provide a conceptual and architectural overview of functions and services, along with their relationships and interactions. This involves deducing

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

existing or proposed functions by determining the functionalities of the use cases and physical implementations in applications, systems, and components. An analysis of the results reveals that many proposed data exchange platforms primarily serve as a common framework or middleware for applications, enabling access for relevant parties while disregarding the underlying data models and structures. Consequently, this approach allows for data management efforts and responsibilities without direct involvement.

In the context of the electricity sector, examples of functions include flexibility management, grid modelling, dispatching, capacity allocation, grid monitoring and operation, aggregation, grid maintenance, network planning, fraud detection, and energy management for smart houses, buildings, and industries. For cross-sector interoperability, various data-related functions need to be addressed, such as data collection, data sharing, consent management, authentication of data users, data log management, data analysis, integration of data sources and users with data platforms, and data visualization.

Information layer

The information layer provides a detailed analysis of the data utilized and shared among functions, services, and components. This contains informational objects and data models. The purpose of information objects and canonical data models is to establish a shared understanding of semantics for functions, enabling seamless and interoperable information exchange. To achieve this, the establishment of a well-defined semantic repository, such as semantic vocabulary and ontologies, becomes vitally significant. This layer can be divided in two sub-layers:

- Information models and ontologies sub-layer that contains the most common information models in electricity such as the Common Information Model (CIM), Companion Specification for Energy Metering (COSEM) and IEC 61850 protocol. For sector agnostic approach Smart Applications REFerence (SAREF) and NGSI-LD could be applied.
- Profiles and data models sub-layer that contains the new profiles covering the communication between new roles and system, but based on the existing profiles and complement the CIM libraries. These profiles include Common Grid Model Exchange Specification (CGMES) and European Style Market Profile (ESMP) for energy sector and different private data exchange profiles for cross-sector data models.

Communication layer

The objective of the communication layer is to describe the data formats, protocols, and mechanisms necessary for achieving interoperable information exchange between components within the context of the underlying use case, function, or service, along with the associated information objects or data models. The key to enabling communication among diverse systems lies in the adoption of standardized solutions. This layer can be divided in two sub-layers:

- Data formats sub-layer that contains the different commonly used formats in both energy and cross-sector data exchange like CSV, XML, JSON, etc.
- Protocols sub-layer that contains protocols like ICCP, Energy Flexibility Interface (EFI) for electricity sector only, web-services and XMPP (Extensible Messaging and Presence Protocol) are of common use, HDFS (Hadoop Distributed File System) layered on top of the TCP (Transmission Control Protocol) / IP (Internet Protocol) for smart grid projects and many other relevant protocols.

Component layer

The component layer involves the physical distribution of all the components that play a role in the data exchange platforms and other solutions. This includes system actors, devices and applications. It is of utmost importance for data platforms to incorporate all the essential modules required for their efficient functioning, in alignment with the established objectives. This layer can be divided in two sub-layers:

- Data exchange solutions sub-layer that contain different data exchange arrangements - centralised, distributed, bilateral, hybrid. The DERA 2.0 report mainly focuses on the data exchange platforms (DEPs), mostly associated with distributed data exchange.
- Applications sub-layer that contains different privacy preservation tools and big data tools such as Supervisory Control and Data Acquisition (SCADA) and Energy Management System (EMS).

Taking into account the detailed representation of the reference architecture in the DERA 2.0 report, it does not contain the Governance layer that is supposed to be added in the DERA 3.0 and the topic of the data governance is not addressed in the DERA 2.0 report.

### 2.2.8 Living Energy

Living Energy – Lab for designing tomorrow’s energy is a living lab held by SEL, this initiative is one of the inputs for the development of the use cases in the Portuguese Pilot, more detailed description of the use cases and the business-to-consumer aspects can be found in Deliverable D2.1. Living Energy (LE) consists of a network of living-buildings, monitored and with their users engaged, to better understand how people use energy and their preferences in real-life. LE approach to the residential sector counts with 60 residential buildings, representing 60 families in the Portuguese territory, reaching more than 120 energy users. For residential context, participants can see their global energy consumption, energy production, detailed energy consumption by time slot and type of appliance as well as records on the temperature and humidity in the household. All this information is made available through LE portal, where participants can access to their personal area and information. The portal also supports participant's engagement, by considering specific dashboards on activities to be proposed to the participants and that, by being part of it, can receive some benefits/incentives to participation.

Data categories

Energy consumption and production data is being monitored from all participants. This data can be divided into the following categories:

1- Participants characterization (demographics behavioral)
2- Aggregated energy consumption (data from the main meter)
3- Specific appliance consumption (data retrieved by smart-plugs and supplier's API's)
4- Energy production (data from the renewable production (PV))
5- Other data (temperature, humidity)

Roles & Actors

There are two basic types of roles that are users and providers.

All LE participants have the role of being the basic data providers. Nevertheless, the participants also have the role of data users, through the offered features and capacities of LE portal the participants have the opportunity to visualize and analyze their own data.

SEL is also both user and provider of data, meaning that SEL is using the gathered data to develop analysis about energy consumption habits and profiles at the same time that it is also providing treated data to other parties (data consumers).

Clients of LE are considered data users.

Rules and responsibilities

All LE participants have a contract with SEL stating the terms on which the data is provided, stored, managed and used. The participants have the right to leave and retrieve their data at any moment.

All gathered data is managed by SEL which has the role of data keeper. It is the responsibility of SEL to guarantee the GDPR compliance, security and anonymity of all data.

SEL is developing a framework to sell and share the LE data with external entities. This framework will define the:

- Security standards to which the external entities need to comply in order to start any interaction

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

- Format, type and extension of data access that is provided to external entities
- Layers of security that need to be verified for every data transaction
- Obligations regarding registration, conformity, marking, labelling and certification of data.
- Any tracking system needed to be implemented for security purposes.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

# 3 Requirements at national level – pilots

## 3.1 Collection of data governance requirements from pilots

The aim of this chapter is to prepare a questionnaire, which will bring pilots on a common level, providing the information for later detailed study on the data spaces governance models. The Deliverable D2.1 provides detailed information about the pilot, actors, software-applications and exchanged information for each pilot, but for these data governance models, a method on how to collect information from pilots is needed. The solution provided by the questionnaire originated from the data spaces definition and its governance, forming its initial version.

### 3.1.1 Pilots questionnaire template

The questionnaire is compiled for each type of the data or service, with the request for detailed description of them. It is important to mention that the questionnaire template was made in close collaboration with the remaining horizontal WPs that were requested to incorporate and review governance-related key aspects that are essential for the pilot's perspective. This collaborative effort aimed to ensure that the pilot's design and development align precisely with its specific needs and requirements.

The questionnaire, which is in on-going stage, consists of ten main points:

1. Definition of roles (data owner, provider, consumer, user) / Domain, plus description
2. Actors: regulated domain (TSOs / DSOs / Public sector companies) VS non-regulated domain (Retailers, Consumers / Prosumers / Energy Communities)
3. Flow of data (end-to-end, end-to-platform data space, data storage); Logs and tracking (logging)
4. Data portability, conversion, reusability, replicability
5. Compatibility and interoperability mechanism
6. Identification/registration mechanisms of the participants (data consumers& providers)
7. Consent management, clearing house, brokers
8. Legal agreements/licensing
9. Policy: UC data governance policy
10. SW solutions (App), App provider

The first section of the questions is related to the topic of the roles and actors in the Data Space. This question defines four main roles that can be identified for the Data Space:

- Data provider, who makes the data available in the DS;

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

- Data owner, who possesses the legal rights to their data, granting them full control over it (can be different entity from data provider in case if data owner does not participate in DS and provides the data under bilateral agreement to data provider)
- Data consumer, who retrieves the data from the DS
- Data user, who possesses the legal rights to use the data under access policy (can be different entity from data consumer in case if data user does not participate in DS and obtain the data under bilateral agreement from data consumer)

Also important information about the types of the parties is collected concerning their representation, either regulated domain or non-regulated domain.

The next set of the questions is related to the security, protection and sovereignty of the data. These questions tackle the topics of personalization of the data, possible anonymization and encryption techniques of the data, cybersecurity measures to protect the data from various threats. One topic includes all the policies for the entities who have access to the data, such as user registration, authorization, authentication, and certification measure used to ensure the security of the data.

Another set of questions is related to access and consent management. It includes the questions related to confidentiality levels of data and which data is needed to be confidential, specific rules for access the data, which can include different topics such as the definition of the type of the user, which can access the data, duration of use of the data, different possible topics of disposal, derivation, reproduction, distribution and re-context of the data. Particular attention is paid to the topics of access grant agreements between different participants of the Data Space, measures on how to use the data, requirements for clearing house and brokers.

Additionally, there is a set of questions is related to the flow of data, whose objective is to determine the communication approach of each initiative provided by the respondents. This involved identifying the starting and ending points of the data flow, if the data is followed to end-to-end approach, end-to-platform approach or both methods and what local storage infrastructures are used in order to keep the data.

Another important topic, which is addressed as well by a set of questions, is related to logging and tracking of the data, which is an important step in improving data traceability. It involves not only the questions about methods and strategies to track the data and where the logs are recorded, but also what information should be tracked.

The final set of the questions revolves around the topics of interoperability, portability and standardizations of the data. Although these topics are very broad, this set of questions focuses on details concerning data formats, conversion of the data in Data Space, readiness to use the data by other entities within Data Space and ensuring the quality of the data sharing mechanisms in order to be able to reuse them in other projects or initiatives.

The questionnaire is added to the Annex I.

# 4 Gap Analysis of requirements for data governance

The identification of gaps in data governance requirements is conducted through a gap analysis process that utilizes a questionnaire outlined in Section 3. The projects mentioned in Section 2 serve as the primary sources of information regarding the presence or absence of these requirements. In the next version of the Deliverable, the responses from the Pilots will be included to further complement the questionnaire. While the questionnaire focuses on specific functions and data sharing procedures described by each pilot, it also helps identify gaps in existing projects that need to be addressed within the Governance models developed in the ENERSHARE Project. It's important to note that although not all technical questions from Section 3 are covered in the gap analysis, the primary governance models and requirements are thoroughly analysed.

This gap analysis is divided into six main topics according to the questionnaire:

- Ownership of the data;
- Security, protection and sovereignty of the data;
- Access and consent of the data;
- Flow of the data;
- Logging and tracking of the data;
- Interoperability, portability and standardisation of the data.

These topics are described from existence of the specific requirements in the initiatives, platforms and projects point of view. If a particular topic is not addressed in any of these, it signifies a gap in the governance requirements. These gaps should be identified to ensure that the relevant topic is included in the governance models of the ENERSHARE project.

Ownership of the data

This section contains the analysis of existence of requirements for the different types of the Data Space participants, such as the Owner of the data, the Provider of the data to the Data Space (which may be different from the owner), Target Consumer of the data, who participates in the Data Space and retrieves the data from the Data Space and Target User, who utilizes the data (can be different from the Target Consumer). Additionally, the analysis is carried out whether there are discrepancies in the requirements based on roles within the regulated or non-regulated domain.

| Initiative, platform or project | Requirements for the **Owner** of the data | Requirements for the **Provider** of the data | Requirements for the **Target Consumer** of the data | Requirements for the **Target User** of the data |
|---|---|---|---|---|
| IDSA | Yes, the role is described, no specific distinction between regulated and non-regulated | Yes, the role is described, no specific distinction between regulated and non-regulated | Yes, the role is described, no specific distinction between regulated and non-regulated | Yes, the role is described, no specific distinction between regulated and non-regulated |
| GAIA-X | No, no distinction between Data Consumer or User | Yes, the role is described, no specific distinction between regulated and non-regulated | Yes, the role is described, no specific distinction between regulated and non-regulated | No, no distinction between Data Consumer or User |
| FIWARE | No, since the FIWARE Platform/Smart Data Models provide the possibility to share the data within the platform, no role apart from Data Provider and Data Consumer | Yes, the role is described, no specific distinction between regulated and non-regulated | Yes, the role is described, no specific distinction between regulated and non-regulated | No, since the FIWARE Platform/Smart Data Models provide the possibility to share the data within the platform, no role apart from Data Provider and Data Consumer |
| OPEN-DEI | Yes, Data Owner role is described, as well as it’s relationships to other roles. No specific distinction between regulated and non-regulated | Yes, Data Provider role is described, as well as it’s relationships to other roles. No specific distinction between regulated and non-regulated | Yes, Target Consumer role is described (as Data Processing Entity), as well as it’s relationships to other roles. No specific distinction between regulated and non-regulated | No, no distinction between Data Consumer or User |

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

| Initiative, platform or project | Requirements for the **Owner** of the data | Requirements for the **Provider** of the data | Requirements for the **Target Consumer** of the data | Requirements for the **Target User** of the data |
|---|---|---|---|---|
| OneNet | Yes, in OneNet is called **data source.** No specific distinction between regulated and non-regulated | Yes. No specific distinction between regulated and non-regulated | Yes, called **data consumers.** No specific distinction between regulated and non-regulated | Not considered in particularly. No specific distinction between regulated and non-regulated |
| BD4NRG | No, no distinction between Data Owner or Provider | Yes. No specific distinction between regulated and non-regulated | Yes. No specific distinction between regulated and non-regulated | No, no distinction between Data Consumer or User |
| BRIDGE (DERA 2.0) | No, Data Owner role is not described, no specific distinction between regulated and non-regulated | No, Data Provider role is not described, no specific distinction between regulated and non-regulated | No, Data Consumer role is not described, no specific distinction between regulated and non-regulated | No, Data User role is not described, no specific distinction between regulated and non-regulated |
| Health Data Space | Yes, distinction between several categories of owners and providers, and distinctions between regulated and non-regulated in a health context | Yes, distinction between several categories of owners and providers, and distinctions between regulated and non-regulated in a health context | Yes, distinction between several categories of owners and providers, and distinctions between regulated and non-regulated in a health context | Yes, distinction between several categories of owners and providers, and distinctions between regulated and non-regulated in a health context |

Security, protection and sovereignty of the data

This section contains the analysis of existence of requirements for the cybersecurity measures, such as anonymization of the data or specific software, registration and authentication of the users of the Data Space and utilization of the certificates.

| Initiative, platform or project | Requirements for **Cybersecurity** (measures, anonymization) | Requirements for user's **registration**, **identification**, **authentication** | Requirements for utilization of **certificates** |
|---|---|---|---|
| IDSA | Yes, under the Policy Execution Framework (PEF) | Yes, registration, identification and authentication are done at two levels:<br>- As legal identities, to identify and authenticate natural persons, organizations, or software components as legal entities<br>- As data space members, to administer and to continuously check that the identified and authenticated legal entities are actually registered as member of a specific data space, and as such adhere to the legal agreements as agreed upon within the data space | Yes, under certification policy by International Data Spaces Certification Body (IDS-CB), which manages and monitors the certification process and is in charge of certifying Evaluation Facilities |
| GAIA-X | Yes, under Policy Rules Document (Cybersecurity section) according to 3 levels of compliance (from low to high)<br>- All EU cybersecurity laws apply<br>- In the future, cyber certification schemes for cloud services might be added | Yes, under Identity and Access Management Federation Service | Yes, via compliance with established standards, certifications, and codes of conduct.<br>- additionally, verifiable credentials obtainable via the Gaia-X Labelling: "a set of automatable rules that enforce the same level of verified descriptive information for Participants and Service Offerings.<br>- through either Gaia-X compliant Identifier |

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

| Initiative, platform or project | Requirements for **Cybersecurity** (measures, anonymization) | Requirements for user's **registration**, **identification**, **authentication** | Requirements for utilization of **certificates** |
|---|---|---|---|
| | | | of the Participant or X509 certificate |
| FIWARE | Yes, through the additional security tokens (namely, Json Web Tokens - JWT) linked to users on behalf of which those notifications/requests have been issued | Yes, through the Identity Management building block and such technology as Keyrock, which supports OpenIDConnect, SAML 2.0 and OAuth2 standards | Yes, through the Certification Authority (CA) |
| OPEN-DEI | Yes, data spaces should be complaint with cybersecurity norms and be part of a Federated Security Management framework | Yes, as part of the technical building blocks, Identity Management (IM) block is mentioned, with some open source solutions for this given as examples | Yes, usage of unique identifiers (tax numbers, IDs, etc.), eIDAS qualified seals and neutral trusted parties. The Trusted Exchange technical building block ensures the certification of participants |
| OneNet | Yes, in OneNet are implemented mechanisms for the identification of the OneNet participants based on OAuth2.0 tokens; for the interfaces for secure data access and usage control; for monitoring of the source traffic, logs and events; for identification of malicious network activities and cyberthreat attacks based on AI and machine learning. The OneNet follows the specifications provided by the EU in the Data | Yes, the identification of the OneNet participants is completely ensured by the Identity Manager (every connector has to have a unique identifier and a valid certificate. Each connector must be able to verify the identity of other connectors) included in the OneNet Middleware. A specific security layer is included for ensuring authentication and authorisation for participating in the OneNet ecosystem. | OneNet system must be able to manage and certificate the identity of each OneNet Participant. Each OneNet Participant must be uniquely identified using certification |

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

| Initiative, platform or project | Requirements for **Cybersecurity** (measures, anonymization) | Requirements for user's **registration**, **identification**, **authentication** | Requirements for utilization of **certificates** |
|---|---|---|---|
| | Protection Framework and in the Information Security Framework, the Smart Grid Security (NISTIR 7628), Information security (CIA: Confidentiality, Integrity and Availability) and Data Privacy Protection (EU Data Protection Framework and GDPR) | | |
| BD4NRG | Yes, through the PRECYSE tools | Yes, using the Keyrock Identity Management | Yes, after future integrations, through the Certification Authority (CA) and Dynamic Attribute Provisioning Service (DAPS) (both IDS) and through FIWARE security components |
| BRIDGE (DERA 2.0) | Yes, in accordance with directive on security of network and information systems (NIS) | Yes, in accordance with regulation on electronic identification, authentication and trust services (eIDAS) | Yes, through the Data Certification Module |
| Health Data Space | Yes,<br>- in accordance with Security of Network and Information System Directive (NIS2) and Cyber Resilience Act;<br>- pre-approval by the European Commission Information Technology and Cybersecurity Board necessary; | Yes, in accordance with Regulation of the European Parliament and of the Council on the European Health Data Space, Article 9 "Identification management"<br>- interoperable, cross-border identification and authentication mechanism for natural and legal persons | Yes, , a combination of mandatory and voluntary self-certification and third-party certification schemes for specific applications, services, and operators of services according to data types and level of risk involved |

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

| Initiative, platform or project | Requirements for **Cybersecurity** (measures, anonymization) | Requirements for user's **registration**, **identification**, **authentication** | Requirements for utilization of **certificates** |
|---|---|---|---|
| | - use of anonymisation, pseudonymisation, generalisation, suppression and randomisation of personal data, in particular for secondary uses of data.<br>- role-based access to data | - role-based-access to data | |

Access and consent of the data

This section contains the analysis of existence of requirements for the access and consent of the data by Data Space participants, which includes the requirements for the confidentiality level of the data, specific rules for access of the data, such as user's type, duration of use, disposal, offline retention/retention via Data Space, derivation, reproduction, distribution, re-context and requirements for licensing the data and existence of agreements between participants of the Data Space.

| Initiative, platform or project | Requirements for **confidentiality** of the data | Requirements for specific **rules for access** | Requirements for **licensing**, **agreements** |
|---|---|---|---|
| IDSA | Yes, through two layers of security when using IDS Connector:<br>- point-to-point encryption (between Connectors), using an encrypted tunnel<br>- end-to-end authorization (authenticity and authorization based on actual communication endpoints; i.e., Data Apps) | Yes, through the Dynamic Trust Management (DTM) (former Security Operation Center) | Yes, IDS provides a technical framework for technically enforced agreements in addition to existing legally binding contracts |

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

| Initiative, platform or project | Requirements for **confidentiality** of the data | Requirements for specific **rules for access** | Requirements for **licensing**, **agreements** |
|---|---|---|---|
| GAIA-X | Yes, under Policy Rules Document (Cryptography and key management) | Yes, under Policy Rules Document, cybersecurity measures regarding authentication, and access control management (to limit access to information and information processing facilities)<br>- More specific rules applicable to data spaces are currently under development | Yes, under Policy Rules Document (master agreements, service level agreements, data protection agreements) |
| FIWARE | Not precisely, applicable if there are special agreements, defined access/usage control policies between data provider and data consumer | Yes, through the Access Management blocks by checking if a user has permission to access a resource and custom eXtensible Access Control Markup Language (XACML) policies | Yes, the set of the requirements for the Business, Operational and Organizational agreements |
| OPEN-DEI | Not explicitly | Yes, through the Access and Usage Policies technical building block | Yes, through Service Level Agreements (SLAs) and Smart Contracts |
| OneNet | Yes, OneNet follows the specifications provided by EU in the Information Security (CIA: Confidentiality, Integrity and Availability) and Data Privacy Protection (EU Data Protection | Yes, the identification of the OneNet participants is completely ensured by the Identity Manager included in the OneNet Middleware. A specific security layer is included for ensuring | Yes, framework that facilitates agreements on the use of data, such as allowing (or disallowing) the processing, linkage or analysis of data and allowing (or disallowing) third parties access to |

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

| Initiative, platform or project | Requirements for **confidentiality** of the data | Requirements for specific **rules for access** | Requirements for **licensing, agreements** |
|---|---|---|---|
| | Framework and GDPR). | authentication and authorisation for participating in the OneNet ecosystem. | data. Smart contracts can also be used to hard-code agreements between parties involving value and other types of asset transfer and allow them to be very transparent and run automatically based on predetermined rules, making it impossible for a party to back out |
| BD4NRG | Yes, through the Dynamic Local Metadata Catalog | Yes, through the Data Access Policy Brokerage | Yes, using Smart Contracts |
| BRIDGE (DERA 2.0) | Not precisely, applicable if there are special agreements, defined access/usage control policies | Yes, according to the requirements for The Harmonised Electricity Market Role Model (HEMRM) | No specific requirements for licensing and agreements |
| Health Data Space | Yes, in accordance with Regulation of the European Parliament and of the Council on the European Health Data Space, Articles 23 (Electronic health record “EHR" systems and wellness applications) and 33 (Secondary use of electronic health data) | Yes, for interoperable, cross-border identification and authentication mechanism for natural and legal persons<br>role-based-access to data (technical details still to be defined) | Yes, various categories of data access agreements, such as:<br>- data permits (administrative decisions defining the conditions for the access to the data) issued by health data access bodies or by data holders for secondary uses of data<br>- various types of agreements for international |

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

| Initiative, platform or project | Requirements for **confidentiality** of the data | Requirements for specific **rules for access** | Requirements for **licensing, agreements** |
|---|---|---|---|
| | | | access and transfer of non-personal electronic health data to non "health data access bodies"<br>- etc. |

Logging and tracking of the data

This section contains the analysis of existence of requirements for logging and tracking of the data, which includes specific requirements for the need to track the data and methods to track the data, and also requirements for identification of what data is needed to be tracked in the Data Space.

| Initiative, platform or project | Requirements for **dataflow tracking** |
|---|---|
| IDSA | Yes, through the Data Provenance tracking building block |
| GAIA-X | Yes, through Data Exchange Services (both logging and tracking of the data), defined by the Gaia-X Association AISBL |
| FIWARE | Yes, by using the Traffic router and such components as Canis Major, that ease recording of transaction logs into different Distributed Ledgers/Blockchains |
| OPEN-DEI | Yes, through the Data Provenance and Traceability technical building block |
| OneNet | The OneNet Connector has specific requirements of transaction logging (activate/deactivate, logging intensity and details etc.) |
| BD4NRG | Yes, using Distributed Ledgers and through the Dynamic Local Metadata Catalog |
| BRIDGE (DERA 2.0) | No specific requirements for dataflow tracking and logging |
| Health Data Space | Yes for EHR system to record identification of the health professional/individual, categories of data accessed, time and date of access, origin of the data<br>Yes, for various operational, reporting, monitoring, supervision tasks of responsible bodies for primary and secondary uses of data |

Interoperability, portability and standardization of the data

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

This section contains the analysis of existence of requirements for interoperability, portability and standardization of the data. Interoperability in this section includes such topics as needs for conversion of the data formats, existence of the requirements for the data formats to be used and the requirements for usage of the converters in the Data Space. Portability in this section includes existence of requirements for readiness to utilize the data by several entities and use cases. Standardization in this sections means the existence of the requirements for the replicability of the data, namely to ensure that the quality of the data is high to be replicable and reusable in other initiatives, platforms of projects.

| Initiative, platform or project | Requirements for **interoperability** (need for conversion of data formants) | Requirements for **portability** (readiness to use by several entities) | Requirements for **replicability** (need for quality of the data) |
|---|---|---|---|
| IDSA | Yes, by following the European Interoperability Framework, developed by the European Commission | No | No |
| GAIA-X | Yes, under Policy Rules Document to ensure on different levels (Infrastructure as a Service [IaaS], Platform as a Service [PaaS], Software as a Service [Saas], data resources, and others);<br>requirements to provide data in a structured, commonly used, and machine-readable format<br>including open standard formats if so requested | Yes, under Policy Rules Document (Portability section), which is in line with Art. 6 (1) Free Flow of Data Regulation (FFoDR)<br>- Additional cybersecurity requirements for portability of data in the cloud (access via other cloud services or IT systems of the cloud customers, access to stored data at the end of the contractual relationship; and requirement for the delition of data from the | No |

| Initiative, platform or project | Requirements for **interoperability** (need for conversion of data formants) | Requirements for **portability** (readiness to use by several entities) | Requirements for **replicability** (need for quality of the data) |
|---|---|---|---|
| | | cloud service provider)<br>- Pre-contractual requirement for the provision of detailed information about the data with a view to switching & porting | |
| FIWARE | Yes, by establishing a several formats (e.g. JSON/JSON-LD), compatible with NGSIv2/NGSI-LD APIs | Not precisely, only by using the established formats | No |
| OPEN-DEI | Yes, through the technical building blocks Data Models and Formats and Data Exchange APIs, and through the governance building block Domain Data Standard | Yes, considering that Data Spaces will incorporate the same soft infrastructure, which will follow EU guidelines and regulations | No |
| ONENET | Yes, OneNet system supports and facilitates more than 60 different cross-platform services grouped into 10 categories. For each of these services, specific data formats and models are defined to facilitate the integration and cooperation of platforms at any level, ensuring portability, reusability, and interoperability of data. OneNet system also offers specific data harmonisation tool for the mapping of most used CIM standards from XML into JSON-LD schema in order to support the NGSI-LD (Next Generation Service Interfaces – Linked Data) standard. | | |
| BD4NRG | Yes, with the Interoperability and Homogenization module | No | Yes, through the Data Quality Compliance and Certification Tools |
| BRIDGE (DERA 2.0) | Yes by establishing the list of data | No specific requirements for | No |

| Initiative, platform or project | Requirements for **interoperability** (need for conversion of data formants) | Requirements for **portability** (readiness to use by several entities) | Requirements for **replicability** (need for quality of the data) |
|---|---|---|---|
| | formats and communication protocols | portability of the data | |
| Health Data Space | Yes, in accordance with Regulation of the European Parliament and of the Council on the European Health Data Space<br>- semantic and technical standards,<br>- standards for certain categories of datasets<br>- standards for certain categories of data exchanges<br>- standards for descriptions of certain infrastructures<br>- set of essential requirements for specific core applications<br>- set of essential requirements for certain categories of (inter)connected systems | Yes, in accordance with Regulation of the European Parliament and of the Council on the European Health Data Space<br>- set of essential requirements for specific core applications<br>- broader definition of portability, going beyond what is allowed based on consent or contract as legal basis for the processing of personal data | Yes<br>- standards for certain categories of datasets<br>- voluntary self-declared data quality label (mandatory only for data holders with publicly funded datasets)<br>- requirements and technical specifications for the data quality and utility label; |

Identified gaps

By examining the aforementioned tables, it becomes apparent that certain aspects are lacking in the analysed initiatives, platforms, and projects when it comes to specifying the necessary requirements for the governance model. While it is possible that these areas are intentionally

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

excluded from these initiatives due to their unrelated nature, it would be beneficial to include them in order to comprehensively address all aspects of Data Space governance.

Regarding data ownership requirements, the majority of platforms do not have the distinction between data owners and data providers, as well as between data consumers and data users. This is because platforms typically disregard such distinctions outside of their Data Space. Nonetheless, it is important to establish requirements for data owners and data users, even if they do not directly participate in the Data Space. This ensures the preservation of data confidentiality and security. Furthermore, most of the observed initiatives, platforms, and projects neglect to differentiate between entity types. However, considering that EU regulations and local regulations vary for entities operating in regulated and non-regulated domains, it is important to establish separate regulatory frameworks for these distinct entity categories.

Regarding access and consent of the data, some initiatives neglect to include requirements of the confidentiality of the data, namely is the data confidential or public and what data is needed to be confidential (owner, provider, date, location, etc.). While from the Data Space perspective, this topic is needed to be discussed between data owner and data provider, it is important to establish the set of requirements for the confidentiality of the data. Additionally, the topic of access grant requirements, which involve licensing and agreements between various participants within the Data Space, should also be taken into consideration.

When it comes to logging and tracking data, the majority of initiatives, platforms, and projects include requirements for these functionalities. However, in the case of DERA 2.0 from BRIDGE, there is a notable absence of specific requirements for tracking of the data, the methods used to track the data, and the information that should be tracked. It is essential for future projects to establish clear requirements for data tracking in order to maintain control over the dataflow, particularly for security purposes.

In terms of interoperability, portability, and replicability of data, all the mentioned initiatives, platforms, and projects establish a set of requirements for interoperability, including data formats, communication protocols, and specific interoperability modules. However, the aspect of data portability, which pertains to the ability of data to be utilized by multiple entities and for different use cases, is only partially addressed within the context of data interoperability, and it lacks detailed requirements in most aforementioned initiatives and platforms. Along with the topic of replicability of the data, namely the requirements for the quality of the data to be replicable in other platforms and project, the topic of portability should be covered in detail in ENERSHARE's Data Governance model.

In addition to the identified gaps and recommendations based on the questionnaire structure, through the analysis of mentioned initiatives, platforms and projects, some general

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

recommendations could be highlighted. These recommendations include fostering collaboration among relevant platforms to enhance the effectiveness of cross-sector data management (portability), promoting standardized formats and communication protocols to facilitate seamless data exchange between platforms, particularly in cross-sector domains (interoperability), and establishing a shared understanding of the business roles associated with data ownership. These general recommendations aim to improve overall data management processes and facilitate efficient data sharing across different platforms.

# 5 Data sharing incentive and business models design for regulated and non-regulated domains

This section focuses on Task 7.3, which aims to create a set of incentive mechanisms for data sharing in the B2B domain. These mechanisms will cover both non-regulated and regulated (DSOs, TSOs, etc.) domains, and the main goal is to attract data consumers while increasing the revenue or benefits for data sellers. To achieve this, two main types of incentive mechanisms will be considered for each business model or use case:

- **Data-by-money (monetary incentive):** data owners accept to share their data because they are monetarily compensated if their data is relevant for solving analytics/optimization tasks and pay in case data from the others is relevant to their own tasks. ENERSHARE will depart from data auction solutions of past projects such as H2020 Smart4RES.
- **Data-by-data (non-monetary incentive):** barter trading, specifically a data-by-data exchange scheme for non-monetary compensations. There is no money involved and data owners agree to share and receive data with approximately the same value.
- **Data altruism:** individuals and companies giving their consent or permission to make available data that they generate – voluntarily and without reward – to be used in the public interest (not considered in ENERSHARE project yet).

In what follows, the original contributions of ENERSHARE, as well as the relevant previous related approaches, are presented for both non-regulated (Section 5.1) and regulated (Section 5.2) domains.

## 5.1 Non-regulated domain

For the non-regulated domain, a set of mathematical algorithms is introduced. In Section 5.1.1, our attention is directed towards the mechanisms of monetary incentives. Initially, an overview of the pertinent prior work is provided, followed by a discussion of the novel contributions proposed by the ENERSHARE project. Likewise, in Section 5.1.2, the expected advancements for the non-monetary incentive framework are outlined. Lastly, Section 5.1.3 highlights the specific use cases selected for evaluating and validating the developed algorithms.

### 5.1.1 Data monetization in regression / forecasting problems

Assume data are collected by $N$ data owners. The $n$-th data owner has a set of $|\Omega_n| \geq 1$ covariates, denoted by $\mathbf{X}_{\Omega_n}$, and wants to predict $\mathrm{Y}_\mathrm{n}$. A forecasting model $\mathcal{M}_\mathrm{n}(\mathbf{X}_{\Omega_n})$ can be obtained with local data, $\widehat{\mathrm{Y}}_\mathrm{n} = \mathcal{M}_\mathrm{n}(\mathbf{X}_{\Omega_n})$, and the main goal of the $n$-th data owner when entering the data market is: (i) to buy data that allows for a better model; and/or (ii) to be monetarily compensated if its data is relevant to improve the accuracy of its competitors' model.

#### 5.1.1.1 Zero-regret auction mechanism

To the best of our knowledge, the first work to describe an algorithmic solution for data markets that enable different power plant agents to sell data and buy forecasts was proposed in [29], as part of the H2020 Smart4RES project. Collaboration between data owners is done through a market operator who receives all data and prepares forecasts. This mechanism guarantees that (i) data sellers with similar information receive similar revenue, (ii) the market price depends on the data buyer's benefit, so the buyer pays only if there is an improvement in forecasting skill, (iii) buyers pay based on incremental gain, and (iv) buyers purchase forecasts, not features, and have no knowledge about the datasets used for forecasting. The mechanism assumes zero loss for sellers, meaning they have no-regret with data sharing and are content with the compensation provided by the data market operator.

In addition, in the H2020 Smart4RES, a prototype for the data market platform was developed by integrating distributed ledger technology with an extended version of this zero-regret auction mechanism. Subsequent improvements were made to enhance algorithm scalability and pricing strategy's robustness to abrupt oscillations. This prototype serves as a foundation for the forthcoming implementation of advanced algorithms in ENERSHARE. Therefore, an overview of the original and improved zero-regret auction mechanisms is provided next.

**Version 1.0:** Data owners provide their historical data to the market operator. Then, at a certain time $\mathrm{T}$, the $n$-th data owner wants to forecast the next $\mathrm{H}$ values of $\mathrm{Y}_\mathrm{n}$, i.e., $\mathrm{Y}_{\mathrm{n,T+1}}, \dots, \mathrm{Y}_{\mathrm{n,T+H}}$, and the following steps occur in sequence, as illustrated in Figure 5-1:

Step 1. The marketplace sets a market price $\mathrm{p}_\mathrm{n}$, before buyer $n$ arrives, for a unit increase in gain when forecasting $\mathrm{Y}_{\mathrm{n,T+1}}, \dots, \mathrm{Y}_{\mathrm{n,T+H}}$. The market price depends on the market configuration for the previous data buyer. If we assume data owners enter sequentially, and according to their identification indexes, then $\mathrm{p}_\mathrm{n} = \mathcal{PF}(\mathrm{b}_{\mathrm{n-1}}, \mathrm{p}_{\mathrm{n-1}}; \Theta_{\mathrm{n-1}})$, where $\mathcal{PF}$ is a market price update function, and $\Theta_{\mathrm{n-1}} = (\mathcal{M}_{\mathrm{n-1}}, \mathcal{G}_{\mathrm{n-1}})$ is the forecasting model and gain function for the $(n-1)$-th buyer.

Step 2. Data buyer $n$ enters the market and submits a bid $\mathrm{b}_\mathrm{n}$, data, desirable forecasting model $\mathcal{M}_n$ and gain function $\mathcal{G}_n$.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

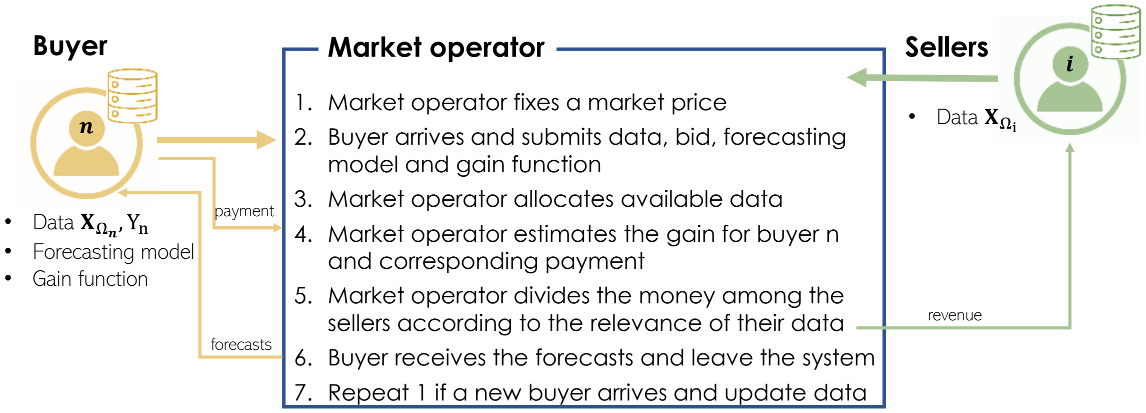
Step 3. The marketplace allocates available features according to the market and bid price, $\widetilde{\mathbf{X}} = \mathcal{AF}(\mathrm{p_n}, \mathrm{b_n}; \cup_{\mathrm{i=1}}^{\mathrm{N}} \mathbf{X}_{\Omega_\mathrm{i}})$, with $\mathcal{AF}$ representing the allocation function.

Step 4. The marketplace estimates the increase in gain when using the collaborative dataset ($\widetilde{\mathbf{X}}$), instead of local data ($\mathbf{X}_{\Omega_\mathrm{n}}$), to train the forecasting model $\mathcal{M}_\mathrm{n}$, and extracts revenue $r_n$ from buyer $n$ according to the estimated increase in gain, $\mathrm{r_n} = \mathcal{RF}(\mathrm{p_n}, \mathrm{b_n}; \Theta_\mathrm{n})$.

Step 5. Market divides $r_n$ among the $N-1$ data sellers using a payment division function $\mathcal{PD}$.

Step 6. Buyer $n$ receives $\hat{\mathrm{Y}}_{\mathrm{n,T+1}}, \hat{\mathrm{Y}}_{\mathrm{n,T+2}}, \ldots, \hat{\mathrm{Y}}_{\mathrm{n,T+H}}$ and leaves the market.

Step 7. If a new time step occurs, data sellers update their data and send it to the market operator.



1. Market operator fixes a market price
2. Buyer arrives and submits data, bid, forecasting model and gain function
3. Market operator allocates available data
4. Market operator estimates the gain for buyer n and corresponding payment
5. Market operator divides the money among the sellers according to the relevance of their data
6. Buyer receives the forecasts and leave the system
7. Repeat 1 if a new buyer arrives and update data

Figure 5-1 - Zero-regret auction mechanism proposed in [29] for H2020 Smart4RES.

For more details about the market price function ($\mathcal{PF}$), data allocation function ($\mathcal{AF}$), revenue function ($\mathcal{RF}$) and payment division function ($\mathcal{PD}$) please consult [29].

**Version 2.0:** The scalability of Version 1.0 was later improved with significant changes including:

1) **Data market sessions:** Instead of calculating the data price for each new buyer, a fixed price per session is proposed. This means that all buyers who enter the data market during a session will have the same price per 1% improvement in accuracy. The price will only update once the session ends, which means the order in which buyers enter the market no longer affects the data price set in the next session.
2) **Change in data pricing:** Data prices are no longer sampled from a distribution that assigns each price a probability of an increase in the gain function. Instead, they are now the average value of that distribution. This modification aims to avoid significant price oscillations that may occur when sampling extremes from the distribution, leading to abrupt price jumps that can make data buyers feel that they depend on luck.
3) **Maximum payment:** The data price is designed as the amount to pay for each 1% of improvement. However, there can be instances where the improvement is exceptionally high, and the final payment can be significant for the buyer. To avoid such surprises, buyers

are now required to submit the maximum amount they are willing to pay for a forecast. If the final price of the forecast is below the maximum, the data market proceeds as usual. Otherwise, if the final price is above the maximum, noise is added to the variables until the final price falls below the maximum.

The prototype for the data market platform built in H2020 Smart4RES combines distributed ledger technology, namely IOTA, with this Version 2.0 of the zero-regret auction mechanism. More details about the developed prototype are provided in Deliverable 5.1 of ENERSHARE.

#### 5.1.1.2 Social Welfare Maximization

Other approaches have been proposed to monetize data in regression problems. [30] proposed a time-adaptive configuration where the value of data is determined solely by buyers. On the other hand, [31] uses a LASSO-based algorithm to define data prices according to sellers' preferences. These solutions mark significant progress towards the development of a data market, but several challenges remain. For instance, the pricing strategy assumes unrealistic behaviour, such as data owners accepting any price to buy or sell their data.

With this in mind, INESC TEC's team formulated a new algorithm where linear collaborative forecasting models are estimated taking into account that data owners set their value function for such a model as well as the minimum amount of money they want to receive $\underline{\mathrm{p}}_{\mathrm{n}}$ (if their data are used to improve others' forecasting model), and the maximum value they are willing to pay $\overline{\mathrm{p}}_{\mathrm{n}}$ (if there are useful collaborative data for them). The developed algorithm aims to maximize the sum of all value functions (social welfare maximization) while ensuring the minimum and maximum acceptable prices, as depicted in Figure 5-2. The buyers' value function is related to the relative error improvement of such model when compared to a model fed with local data, while the sellers' value function is related to the model's coefficients (and the corresponding prices). In this way, while maximizing social welfare, the linear collaborative forecasting model (data allocation and coefficients) and data prices are optimized.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

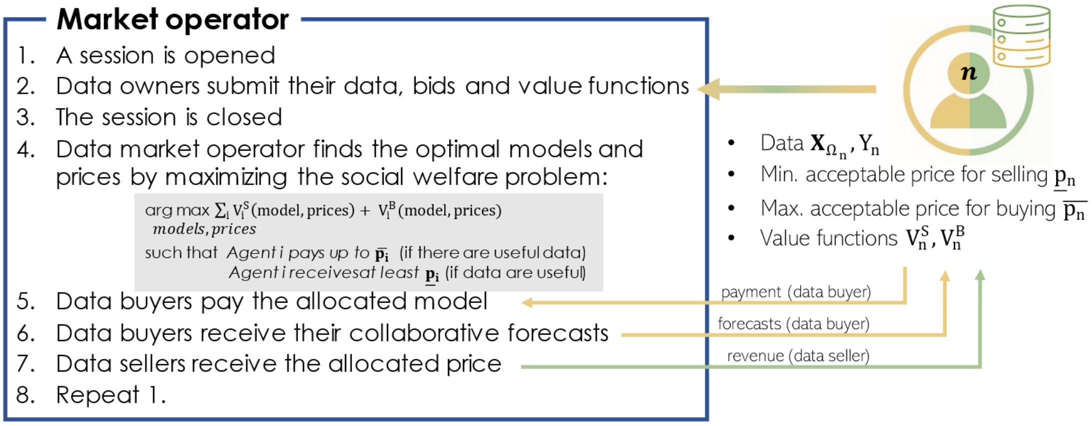

Market operator
1. A session is opened
2. Data owners submit their data, bids and value functions
3. The session is closed
4. Data market operator finds the optimal models and prices by maximizing the social welfare problem:
arg max $\sum_i V_i^S(\text{model, prices}) + V_i^B(\text{model, prices})$
$models, prices$
such that *Agent i pays up to* $\overline{\mathbf{p}_i}$ (if there are useful data)
*Agent i receivesat least* $\underline{\mathbf{p}_i}$ (if data are useful)
5. Data buyers pay the allocated model
6. Data buyers receive their collaborative forecasts
7. Data sellers receive the allocated price
8. Repeat 1.
$n$
Data $\mathbf{X}_{\Omega_n}, Y_n$
Min. acceptable price for selling $\underline{\mathbf{p}_n}$
Max. acceptable price for buying $\overline{\mathbf{p}_n}$
Value functions $V_n^S, V_n^B$
payment (data buyer)
forecasts (data buyer)
revenue (data seller)

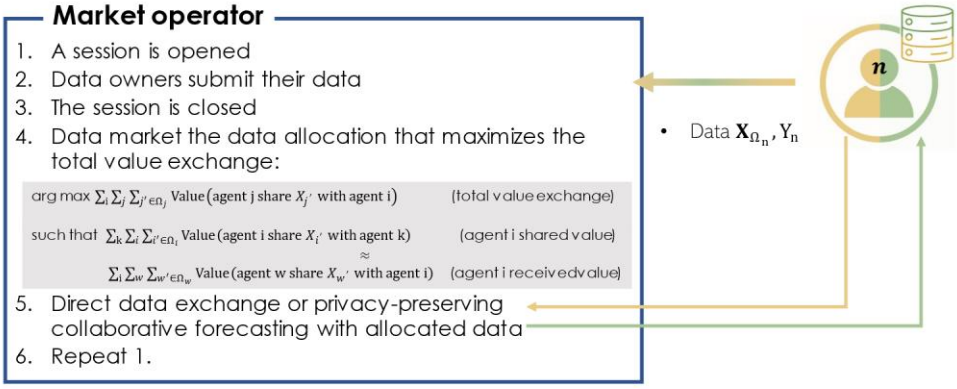
Figure 5-2 - Social welfare auction mechanism.

ENERSHARE presents an advancement in the existing social welfare auction mechanism by accommodating more complex collaborative regression forecasting models, such as neural networks or support vector regression. This extension poses additional challenges, as the seller is confronted with the obstacle of using neural network coefficients, which are considered black box models – the coefficients themselves offer no discernment of a variable's significance, and thus hinder the seller's ability to interpret the model. ENERSHARE will propose other ways to express these value functions, such as by using feature permutation importance to measure the relevance of a variable. Lastly, ENERSHARE will also accommodate classification problems, in which data value is potentially related with the improvement in classification accuracy.

The prototype mentioned in the previous sub-section (and described in detail in Deliverable 5.1 of ENERSHARE) is robust enough to incorporate these new algorithms without major changes.

### 5.1.2 Data-by-data exchange

ENERSHARE will also consider the case in which agents are interested in collaborating with their competitors but only if they provide and receive information with the approximately same value (non-monetary incentive mechanism). ENERSHARE propose a new algorithm to maximize the multilateral data exchange while ensuring each data owner provides and receives data with approximately the same value, as illustrated in Figure 5-3.



Market operator

1. A session is opened
2. Data owners submit their data
3. The session is closed
4. Data market the data allocation that maximizes the total value exchange:

$$\arg\max \textstyle\sum_{\mathrm{i}}\sum_j\sum_{j'\in\Omega_j} \text{Value}(\text{agent j share } X_{j'} \text{ with agent i}) \quad \text{(total value exchange)}$$

$$\text{such that } \textstyle\sum_{\mathrm{k}}\sum_i\sum_{i'\in\Omega_i} \text{Value}(\text{agent i share } X_{i'} \text{ with agent k}) \quad \text{(agent i shared value)}$$

$$\approx$$

$$\textstyle\sum_{\mathrm{i}}\sum_w\sum_{w'\in\Omega_w} \text{Value}(\text{agent w share } X_{w'} \text{ with agent i}) \quad \text{(agent i receivedvalue)}$$

5. Direct data exchange or privacy-preserving collaborative forecasting with allocated data
6. Repeat 1.

Figure 5-3 - Data-by-data exchange (ENERSHARE proposal).

Using the same notation as before, let assume data are collected by $N$ data owners, and the $n$-th data owner has a set of $|\Omega_n| \geq 1$ covariates, denoted by $\mathbf{X}_{\Omega_n}$, and wants to predict $\mathrm{Y}_n$. Let $\text{Value}(\mathrm{Y}, \mathrm{X}|\mathbf{Z})$ measure the value of acquiring the variable X when predicting Y, taking into consideration a pre-existing set of variables, denoted by $\mathbf{Z}$. Then, our proposal for the data-by-data incentive mechanism can be expressed with the following optimization problem:

$$\max_{z_{j'\to i}\in\{0,1\}} \overbrace{\textstyle\sum_i \underbrace{\textstyle\sum_{j\neq i} \sum_{j'\in\Omega_j} \text{Value}(\mathrm{Y_i}, \mathrm{X_{j'}}|\,\mathbf{X}_{\Omega_\mathrm{i}})\, z_{j'\to i}}_{\text{value received by agent i}}}^{\text{total value exchanged}}$$

$$s.t. \underbrace{\textstyle\sum_{i'\in\Omega_i}\sum_j \text{Value}(\mathrm{Y_j}, \mathrm{X_{i'}}|\mathbf{X}_{\Omega_j}) z_{i'\to j}}_{i-th\text{ data owner }\textbf{shared}\text{ value}} \approx \underbrace{\textstyle\sum_k \sum_{k'\in\Omega_k} \text{Value}(\mathrm{Y_i}, \mathrm{X_{k'}}|\mathbf{X}_{\Omega_i}) z_{k'\to i}}_{i-th\text{ data owner }\textbf{received}\text{ value}}, \forall i$$

$$\underbrace{\textstyle\sum_k\sum_{k'\in\Omega_k}\sum_j\sum_{j'\in\Omega_j} \text{Value}(\mathrm{Y_i}, \mathrm{X_{k'}}|\mathbf{X}_{\Omega_i}, \mathrm{X_{j'}}) > 0\,, \forall k', j' \colon z_{k'\to i} = z_{j'\to i} = 1}_{\text{(ensure non}-\text{redundant data allocation)}},$$

where $z_{j'\to i} = 1$ if the $j'$ variable of $j$-th data owner is allocated to $i$-th data owner, $z_{j'\to i} = 0$ otherwise. Two main challenges are identified for this data-by-data formulation: how to measure the value of the data and how to solve the optimization problem efficiently. ENERSHARE will assess the value of data through metrics based on correlation (e.g., conditional Pearson or Spearman correlation) or other information-theoretic alternatives (e.g., conditional entropy or mutual information), and investigate efficient ways to solve constrained allocation problems.

### 5.1.3 Analysis of WP2 use cases

The data sharing incentive mechanisms described in the previous subsections have a potential to be adapted and used to incentivize data sharing in multiple use cases described in WP2, in Deliverable D2.1 *“Use cases' descriptions and list of minimum Data Space building blocks required for Pilots”*. While the data monetization in Section 5.1.1 is use-case specific since a

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

loss/profit function from an explicit application is used to translate data value into a monetary compensation, the data-by-data mechanism is mainly centred in the data value (which can be only information content) that is more flexible for application in multiple use cases. It is also important to mention that a fundamental requirement in any use case is to have data distributed across different Data Owners (which can be sensors, edge devices, enterprises, consumers, producers, etc.) and has cross-stakeholder value (i.e., collaborative analytics bring value to at least one Data Consumer). Besides, these incentive mechanisms were mainly designed for a business-to-business (B2B) context. For business-to-client perspective, the reader is redirected to Deliverable D2.2 "Report on the data sharing incentive design for consumers and local communities". In the Table 5-1, we identify and discuss the WP2 use cases where these data sharing incentives can bring value within a Data Space paradigm.

Table 5-1 - WP2 use cases and potential for data sharing incentives.

| ID | Use Case (UC) | Potential for B2B Data Sharing Incentives |
|---|---|---|
| P1-ES | Wind farm integrated predictive maintenance and supply chain optimization | Wind power plants (WPPs) owners and wind turbine Original Equipment Manufacturers (OEMs) have access to the data collected from the wind turbines in operation and they are the only players that are presently extracting value out of data. Nevertheless, for emerging O&M service providers that bring machine learning expertise and other data sources (e.g., robotics inspection, satellite images), the access to real operational data or data simulated with a Digital Twin is very important to construct data-driven models to support different O&M actions. For instance, a service provider can build a model with data from WPP A and apply it to WPP B just with the model constructed with data from WPP A. This is a good case for 'Social Welfare Maximization' (see Section 5.1.1.2) that can be applied to both regression and classification problems (e.g., fault identification) and the data value would be related with the improvement in classification accuracy (and savings in the O&M actions). Moreover, a data-by-data mechanism might be considered as well if Data Consumers/Providers start to exchange data across the value chain, e.g., exchange data from WPP A by data from WPP B. |
| P2-PT-A | Leveraging on consumer-level load data to improve TSO's operational and planning procedures | This UC considers the case where the TSO acts as a Data Consumer and uses a data monetization incentive mechanism to promote data (i.e., real-time active power measurements) sharing from a group of Consumers connected to the same primary substation and improve the short-term load forecasting error. For the TSO, this means getting and adding more information (in addition to the aggregated substation load measurements) to the forecasting model, in particular recent measurements from Consumers that might have DER such as EV, storage, or smart appliances. This is an incentive mechanism with a single Data Consumer (Buyer) and multiple Data Providers (Sellers), and monetization is possible since the improvement in load forecasting error can be translated to a better grid operation (and lower operational costs). The incentive mechanisms (data monetization) from Section 5.1.1 will be |

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

| ID | Use Case (UC) | Potential for B2B Data Sharing Incentives |
|---|---|---|
| | | demonstrated in this use case. |
| P2-PT-B | Instantiation of energy communities and digital simulation of business models | In this UC, the idea is to optimize (planning phase) the sizing of local energy communities and their operation (e.g., estimate a reference price signal to study different business models) by combining data from different Consumers and Prosumers. The core approach is based on mathematical optimization, with a formalization of an optimization problem. The data from different Data Owners is relevant but is mainly used to calculate the benefits of belonging to the community and sharing assets. For the planning domain, and in this specific UC, the application of the data sharing incentive mechanisms from Section 5.1 is not straightforward. Here, the mechanisms should be based on SSH methodologies, such as the one described in Deliverable D2.2 “Report on the data sharing incentive design for consumers and local communities”. |
| P2-PT-C | Detect irregularities in energy consumption in households with seniors living alone | B2C use case. The mechanisms should be based on SSH methodologies, such as the one described in Deliverable D2.2 “Report on the data sharing incentive design for consumers and local communities”. |
| P2-PT-D | Suggest maintenance of appliances based on NILM data | B2C use case. The mechanisms should be based on SSH methodologies, such as the one described in Deliverable D2.2 “Report on the data sharing incentive design for consumers and local communities”. |
| P3-SI | Optimal multi-energy vector planning - electricity vs heat | This UC falls in the regulated data sharing domain since it requires close cooperation between all actors in each geographic area of district heating and the logical clusters of users involved, and it is related to multi-energy grids infrastructure planning (i.e., activities of multi-energy system/network operators). |
| P4-GR | Digital Twin for optimal data-driven Power-to-Gas planning | In this case, the integration of multiple data sources (potentially from different Data Owners) can improve the simulation accuracy of the Power-to-Gas (P2G) Digital Twin, which could lead to an optimization of the Levelized Cost of Electricity (LCOE) by the investor. In this case, the data monetization incentive mechanisms can be used to foster data sharing across the hydrogen supply chain, e.g., improve the accuracy of the natural gas demand forecast using the ‘Social Welfare Maximization’ (see Section 5.1.1.2). The data-by-data exchange is also possible since simulated Digital Twin data can be exchanged with other data upstream or downstream the supply chain. For instance, investors in RES may be interested in getting data about electrolysers operating profile. The data can be valorised according to its contribution to the LCOE improvement, but this means linking data value with optimization problems, which is outside the scope of ENERSHARE but is starting to be explored in the literature (Mieth et al., 2013). |
| P5-IT-A | Cross-sector flexibility | Partially falls in the regulated data sharing domain since it requires |

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

| ID | Use Case (UC) | Potential for B2B Data Sharing Incentives |
|---|---|---|
| | services for aggregators and DSO | cooperation between TSO and DSO. However, for aggregators access to data from non-energy sectors (e.g., water, data centres, electrical mobility) is very important to estimate their flexibility potential and design marketing and engagement strategies for consumers from those sectors. In this case, monetization of historical data (e.g., operation of water pumps, use of EV chargers) is a potential strategy to pay for rich databases and enable pre-assessment of cross-sector energy flexibility potential. In this case, 'Social Welfare Maximization' (see Section 5.1.1.2) might be a potential solution, but with a mathematical formulation adapted to valorise data according to its volume – similar to what is done in (Cao et al., 2017). |
| P5-IT-B | Services for e-mobility CPOs, EVs drivers and DSO | For this UC, increasing the predictability of charging points availability and EV charging needs is fundamental for an optimal planning of incentives for EV drives and estimation of flexibility for DSO. For this goal, it is necessary to create incentive mechanisms for having EV drivers charging their mobility patters with the Charging Point Operator and DSO. In this case, the improvement in the accuracy of forecasting chargers' availability or distribution network congestions due to this data owned by the EV drivers can be promoted with the 'Social Welfare Maximization' (see Section 5.1.1.2) mechanism. |
| P5-IT-C | Flexibility provision for electricity grid with water pumps and predictive maintenance of the pumps | Forecasting water demand might benefit from external data sources, and, in this case, the approach can be like the one described in P2-PT-A. |
| P7-LV | Cross-value chain services for energy-data driven green financing | A data-by-data mechanism might be considered if Data Consumers/Providers start to exchange data across different sectors, or if different players (e.g., Energy Services Companies, financing companies) start exchanging their data to build larger datasets for energy efficiency and res investments assessment. In fact, the data-by-data mechanism can be used for UC like this one, where the same variables are collected but there are only a few data examples (limiting the application of machine learning methods). But combining (via data sharing) small chunks of data it is possible to increase data volume and enable the application of advanced machine learning algorithms. |

## 5.2 Regulated domain

### 5.2.1 DSO

This section highlights data sharing schemes with energy and non-energy sector stakeholders from the distribution system operator's (DSO) perspective. On this stage, a closer look is given to the Slovenian DSO to show the incentives with an example of the DSO's requirements.

Slovenia, Electrical energy sector

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

The main legal frameworks related to the Slovenian electrical energy sector are:

- Energy Act [32]
- Act on Energy Efficiency [33]
- Act on the Promotion of the Use of Renewable Energy Sources [34]

Among the data, which are provided by the Slovenian Electricity Distribution Companies (EDC), Slovenian DSO mainly considers data that are recorded and gathered by smart meters. Thus, the focus to the metering data will be given.

With the aim of fostering competition in the electricity retail market, the DSO has been established in 2007. DSO merged the operation of the five EDC - operating the distribution power system in Slovenia. Ownership of the distribution networks remains with the EDCs, while the DSO must rent the network and services related to the infrastructure from all five EDCs-owners of the networks. EDCs perform contracted construction and maintenance tasks for/in the name of DSO on their own infrastructure, and in some rare cases also on the DSO infrastructure. The EDCs are the owners of the metering devices, in some cases the owners of the meters are the consumers.

Smart metering of electricity (also gas, district heating, and water) involves various service providers and services through the smart metering process. The services in the smart metering involve:

- Installation of the smart meter and other devices that are necessary for the data transfer from the smart meter to the metering centre (MC).
- Maintenance of the smart meters and all associated devices and equipment.
- Data reading from smart meters and other devices.
- Validation of the metering data.
- Processing and integration of data and their further use.

The concept of smart metering in Slovenia consists of a few main elements.

- Metering devices and associated devices on the consumer's premises.
- Communication and data processing infrastructure between the devices on the consumer premises and the back-end systems.
- Information systems at the metering operators' back-end that provide necessary energy and metering data to billing and invoicing systems of the suppliers and optionally to the consumer and as well as information systems required for the management of smart meters.

It can be identified several stakeholders, which can be either directly or indirectly affected by the roll-out of smart metering: EDC and DSO, consumer, supplier, and other.

In Slovenia, the following smart metering service model is present: DSO, actually the EDC, is responsible for data transfer from their meters to their metering data centres. Different communication technologies are used; PLC technology is the most used technology when it is about to collect the data from the smart meters connected to the LV households and small commercial users (from the perspective of electricity consumption and connection power). Industrial meters and, in very rare cases, also smart meters metering the consumption of small commercial or household customers, GSM communication is used. EDCs for these purposes, contract individually with the telecommunication services operators. GSM is also used in case of data transfer from the concentrators to the EDCs metering data centres. The metering service model is depicted in Figure 5-4, and it clarifies the physical layer of the model.

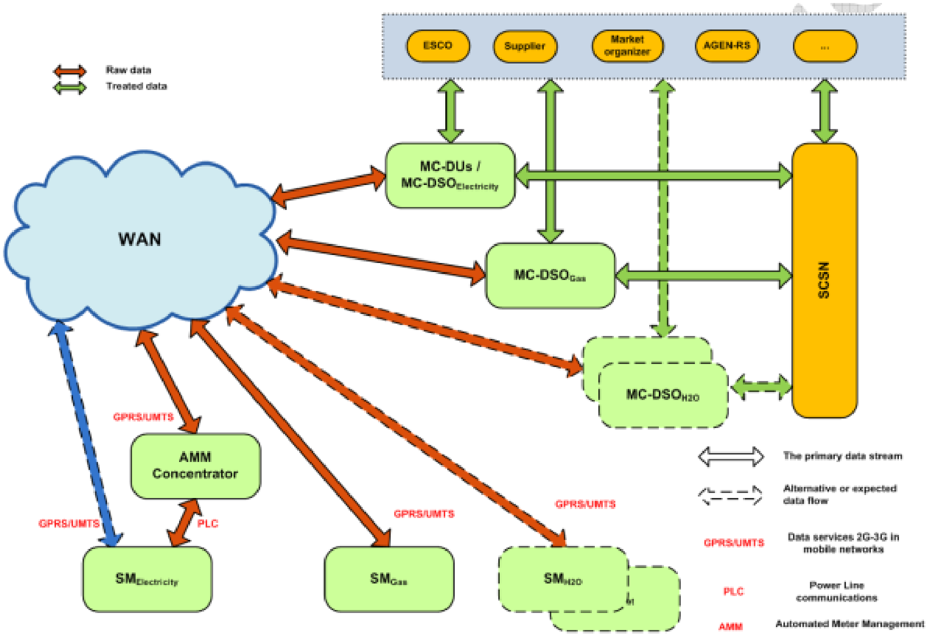


Figure 5-4 - Metering service model.

The current metering service model is depicted in Figure 5-5.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

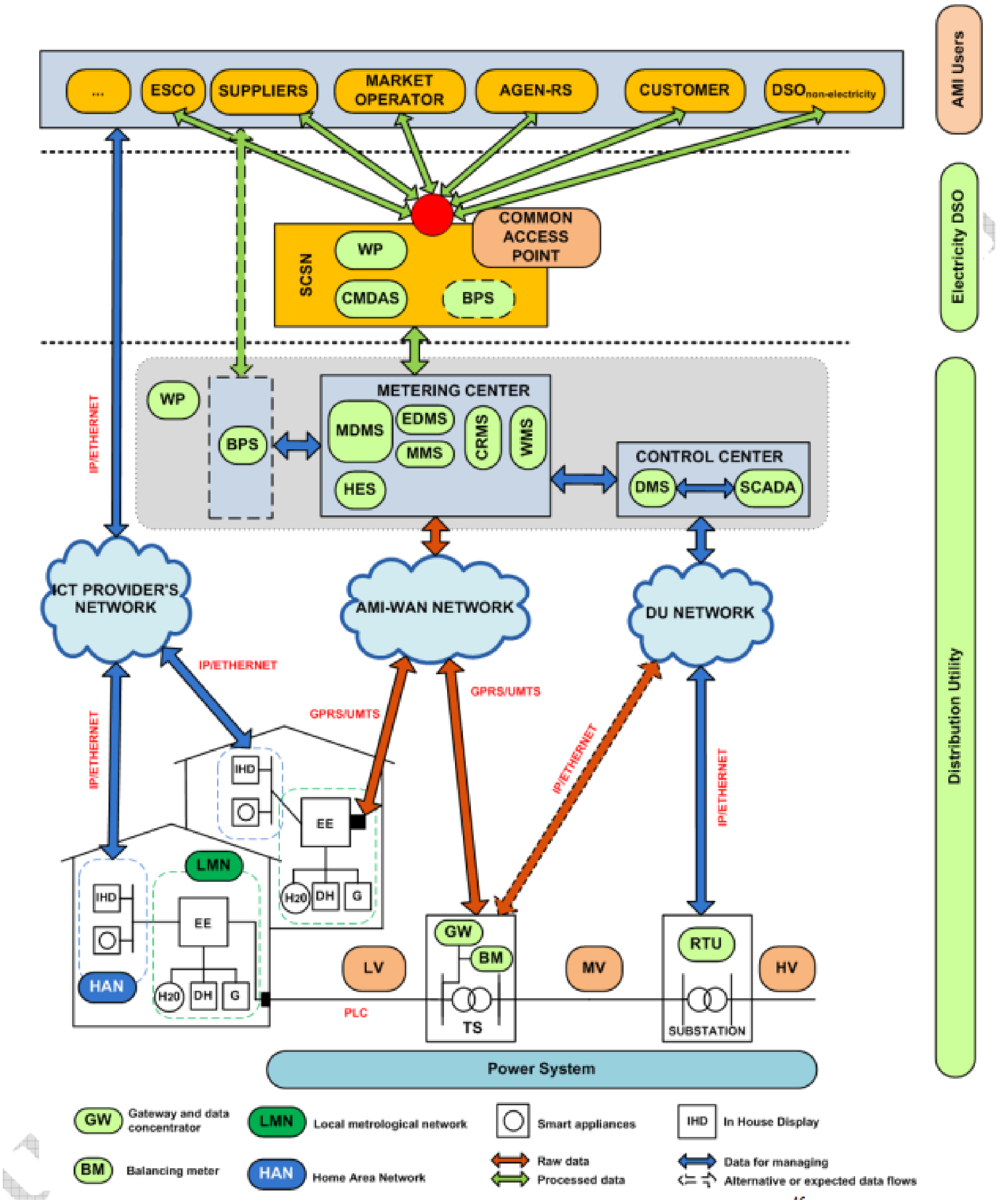


Figure 5-5 - Metering service model architecture.

In Figure 5-5, it is possible to see several smart infrastructure devices and software tools, together with the communications. The following section provides an explanation of the elements.

Smart meter

It represents a key element for measuring electricity. For providing data, there are several options:

Optical interface operates according to:

- IEC 62056-21 standard: Electricity metering: Data exchange for meter reading, tariff and load control.
- DLMS standard.

P1 interface is a one-way read-only communication interface and it is in compliance with DSMR V3.0 standard. Meter has one physical P1 port on which it is possible to connect more than one Other Service Module (OSM) devices via splitter. P1 interface support two different types of data depending on the choice of communication type. With IEC 62056-21 (IEC 1107) communication type the meter can send data predefined with objects: General local port readout (0-0:21.0.0), Consumer message text – Consumer information (0-0:96.13.0), Consumer message code – Meter display (0-0:96.13.1). If the device is connected to the P1 port, meter will send data configured in the General local port readout object every 10 seconds.

PLC stands for power-line communication over the low-voltage grid and the main advantage of this communication is the use of an existing infrastructure, which covers most parts of the inhabited areas. Each low-voltage grid has one substation, which transforms the voltage into 400 V and delivers it to the connected households via low-voltage lines. PLC consists of three major parts: E-meter with built-in Distribution Line Carrier (DLC) modem, Data concentrator, Head End System (HES).

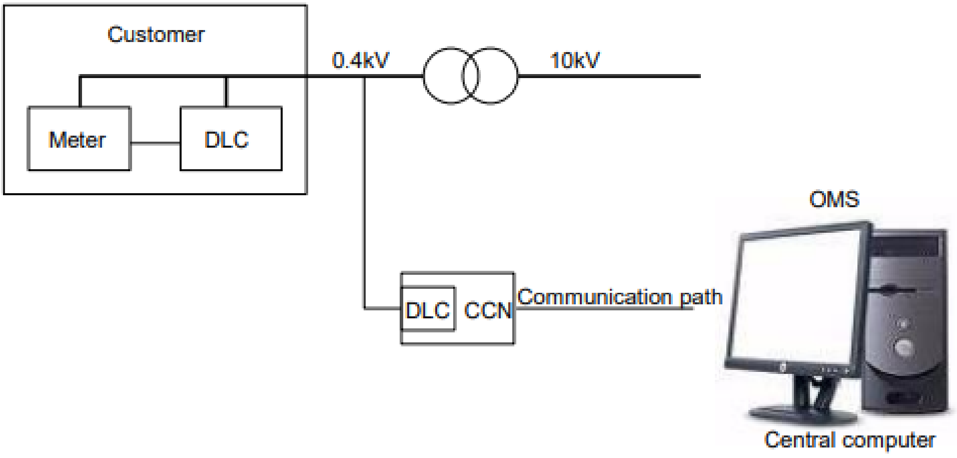


Figure 5-6 - Data acquisition from LV smart meters using PLC technology

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

Typical PLC configuration

Smart meter runs the Pull communications, from the central system (client) to the meter (server). On the contrary, in Push operation communication runs from the meter (server) to the central system (client), where the meter initiates the communication and pushes information to the central system without any request. Push process is implemented through the data notification process, which takes care of processing requested push object, checking for successful communication, and preparing data to build proper COSEM_APDU (Application Protocol Data Unit) message.

Smart meter, beside energy and power measurement and registration and instantaneous values measurement and registration (power, voltage, current, power factor, frequency), enables: power quality measurements (partly according to EN 50160*), power quality measurements data available as instantaneous or average data, voltage sags and swells, under voltages, over voltages, measurement of minimum, maximum - daily voltage, measurement of instantaneous power factor; per phase, three-phase registers, measurement of last average power factor, registration of three phase and phase power-downs and the power-down duration (long and short).

Balancing meters, also called "Sum meters", are installed in most low-middle voltage substations. EDC uses these data to compare the values with the amounts of consumed electricity measured by the LV smart meters. The difference should be not significant higher than the estimated technical losses. In this way, EDC discovers electricity theft.

Information systems and data exchange

HES is responsible for collection of metering data transferred to the EDC, through the communication infrastructure. It comprises: data interface for communication with smart meter gateway (directly in case of GSM) or via concentrator- communicator (in case of PLC), acquisition of smart meter data, plausibility and preparation of the data, providing access to data for upstream level information systems, data encryption, load balancing, sending requests to smart meters, initialization of specific data queries.

- Metering management system (MMS) manages monitors and administers the installed smart meters, provides status of the equipment and data exchange with smart meters/gateways.
- Meter data Management System (MDMS) is responsible for data validation, post processing, storage and assuring the validated metering data on a long term use. This component is a core one of Advanced Metering Infrastructure (AMI).
- Energy Data Management System (EDMS) provides services of storage, validation and management of energy consumption and production data for the market participants.

This system also provides services for the conventional meters replacement management, during the roll out of smart meters.

- Customer relationship management (CRM) System, processes and manages contractual and customer data. It supports customer services through different communication channels (call center, e-mail, web portal).
- WMS stands for Work Force Management system, with this system human resources work on the metering infrastructure in optimal organized.

Maintenance of the metering infrastructure

The latest legal data in English are unfortunately available only for 2021, for 2022 there is not yet available the Annual report in English. Therefore, in this part information relevant for 2021 will be given. It is necessary to consider, that in 2022, there was definitely again present an important improvement: from technical and also statistical perspective- share of smart meters and remote data read out increased.

Through the accelerated introduction of the advanced metering system (AMS) and coordinated tasks management, the costs of manual readings are significantly cut, while enabling network end users to switch to the billing of electricity according to actual consumption and other AMS functionalities.

The shortage of metering devices on the market and the resulting backlog of deliveries prevented us from achieving the plan to equip metering points with AMS in 2021. The opportunity to supply and install over 10,000 advanced measuring devices, which would have improved the situation significantly under normal circumstances, was lost.

The remote-control system already includes more than 261,001 metering points, or 75% of all metering devices in the area covered by Elektro Ljubljana. Of that number, 253,606 metering points are included in the AMS, meaning 74% of the total. The goal until the end of 2025 is to include the majority of metering points in the AMS (where possible).

As a result, annual manual and monthly readings are reduced by 19% and 59% respectively in 2021.

With the introduction of a special team to resolve power-line communication (PLC) issues, we are improving the reliability of data capture at end-customers in the LV network, where PLC, which employs the low-voltage network as a transmission path, is used as the communication protocol. Specialised knowledge and tools, which are already showing positive effects, are used due to different network disruptions that normally originate from end-customers' devices and require a comprehensive approach to identification and elimination. The achievement of this objective, which is very ambitious, is still a long way off, but results are improving. The reliability of data capture at end-customers in the LV network has thus improved. During the most

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

unfavourable network conditions, remote readings failures reached around 1.13% of installed devices, compared with the target of 0.8%.

Digitalisation of Electrical Energy Sector

Electricity Supply Act [35] defines as obligatory, that EDC must ensure data to suppliers, market operator and grid users. Thus, all Slovenian EDCs collaborate in a common project, to establish a central platform, through which grid users and other eligible entities could access to their data-smart meters collected data, the historical ones and also to the close to real time. The main driver was the current period of exponential growth in acquired and machine-captured data, the introduction of mechanisms and systems for capturing, storing, and managing data from various data subsystems. All beforementioned facts are essential for a systematic digitalisation of the EDC's. Through the appropriate authorisation, EDCs facilitated access to common analytical solutions and standardized reports via the company's central portal.

The joint project, System for uniform access to metering data (SSAMd), which is in the scope of the single entry point of the National Data Hub (SEP-NDH), includes a web portal for *Moj Elektro* end-users, the Central Electricity Portal of Slovenia for electricity suppliers, SODO, Borzen, the Employers' Association of Slovenia and the Energy Agency, ensures mass (B2B) data services, the exchange of data and the provision of data to ELES regarding all production sources in Slovenia in real-time via the ECCo SP plugin. The number of times detailed 15-minute data from metering points was accessed by electricity suppliers via 46,000 end-customers through calls to Elektro Ljubljana's metering centre using SEP-NDH services exceeded 12 million in December 2021 alone.

TSO-DSO collaboration

Under the agreement between ELES, SODO and electricity distribution companies, the transmission system operator data regarding key production sources (in excess of 100 kW) in near real-time for the previous 15-minute interval at 518 metering points throughout Slovenia is provided. With the upgrading of the SEP-NDH environment, all electricity distribution companies provided all data required by ELES via the common and single ECCo SP mechanism as part of the SEP-NDH. In addition to near real-time data, daily 15-minute aggregated values by individual DTS area for all production sources are also provided.

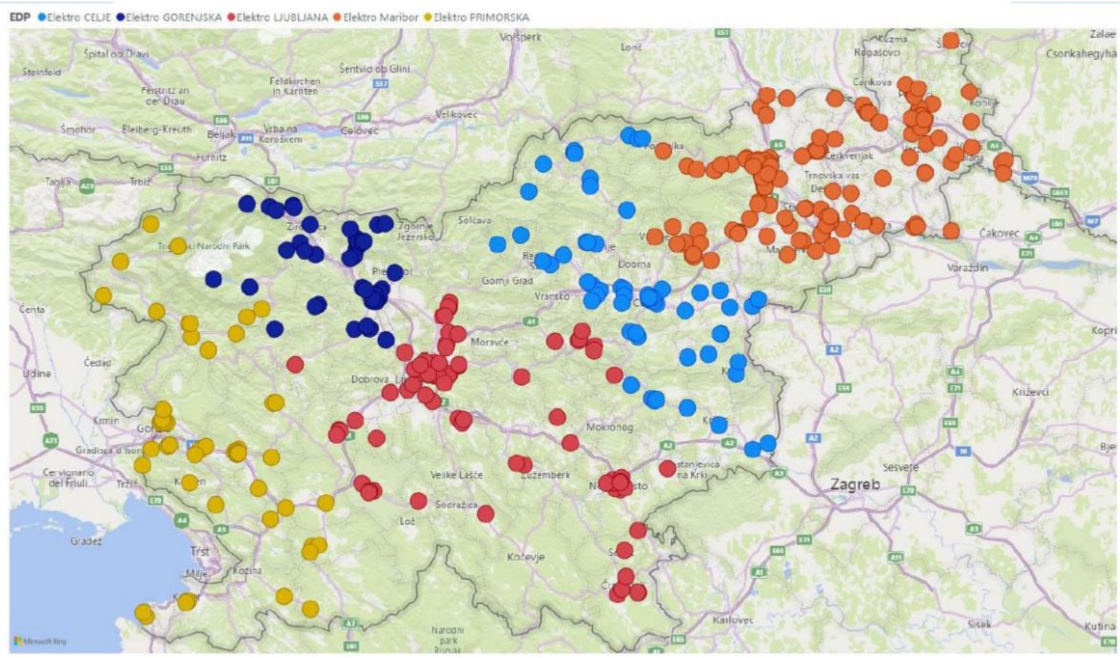


Figure 5-7 - Metering point locations in Slovenia where data is transmitted in near real-time.

Heat distribution sector

The main legal frameworks related to the Slovenian heat distribution sector are:

- Energy Act - EZ [32]
- Act on Energy Efficiency - ZURE [33]
- Act on the Promotion of the Use of Renewable Energy Sources - ZSROVE [34]
- Act on the supply of heat from distribution systems - ZOTDS [36]
- Act on heat supply pricing methodology [36]

In addition to the above legislation, heat distribution activity in our geographical area is additionally regulated by the document System operating instructions for the heat distribution system for the geographical area of the Municipality of Velenje and the Municipality of Šoštanj, which is confirmed by the Slovenian energy market regulator the Energy Agency.

- System operating instructions for the heat distribution system for the geographical area of the Municipality of Velenje and the Municipality of Šoštanj [37]

Within the framework of the above legislation, heat distribution systems are obliged to report to the Energy Agency and other state authorities. Reporting is carried out on an annual or monthly level and includes aggregated data, while the provision of real-time data to customers or other institutions in the field of heat distribution is currently not yet legally required.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

Main incentives for data sharing data between customers and regulated entities, electricity distribution system operators domain

As part of the measures implemented in line with its competencies aimed at unifying the most important data exchange processes at the national and regional levels, the Slovenian Energy Agency has been establishing an efficient data exchange between market participants, steering the participants towards the use of open standards and the reuse of generic models of the European forum for energy Business Information eXchange (ebIX®) and ENTSO-E models to the greatest extent possible [38]. The new regulatory framework and the vision for the evolution of energy networks by 2050 envisage the full integration of energy networks (electricity, gas and heat) and the consumers' complete engagement (development of a flexibility market). The harmonisation of data exchange processes using open standards in energy markets is thus becoming even more important and a crucial action to eliminate certain barriers to entry for new market participants and to reduce entry costs. Data exchange has been becoming more and more complex and is usually required in near real-time or real-time.

Due to the development of new business models and energy services, based on access to detailed metering data, there is a distinctive need in the retail markets as well to harmonise access to and the exchange of data on consumption or production, as access to this data must be ensured centrally or locally (on a metering device) for users eligible to access data (aggregators, suppliers, energy service providers, etc.), subject to the customer's authorisation. To support the green transformation, regulatory frameworks must ensure a sufficient level of data protection and privacy, tools for empowerment and the promotion of active consumption, a non-discriminatory environment and a level playing field for all stakeholders, a technologically neutral regulatory framework, and recognise the new roles of traditional actors. Besides the requirements regarding efficient and safe data exchange, Directive (EU) 2019/944 also defines the context for ensuring interoperability for the first time.

The implementation of data exchange between the participants in the Slovene electricity market is predominantly carried out in compliance with the relevant reference models (e.g. the ENTSO-E/ebiX/EFET harmonised model of roles in the electricity market, etc.). In 2021, the processes of the updated market model were intensely adapted to the concept of split supply, which is based on the introduction of a metering point and will eliminate incompatibilities with the reference model at the national level and provide the optimum possibilities for the development of energy services. The on-line data portal mojelektro.si is designed to ensure the compatibility of the centralised data access with the draft implementing act on access to the data on consumption (business-to-client segment).

The areas with the most incompatibilities are as follows: ensuring interoperability at the level of local access to data (I1 interface on the smart meter); implementation in the field of flexibility where planned deviations from reference models can be identified, and starting with unsuitable definitions of roles and responsibilities. As this is a developing area, the Slovenian Energy Agency assumes those incompatibilities are of a transitional nature. The Act on the identification of entities in the data exchange among participants in the electricity and natural gas markets requires market participants to use standardised identifiers of key data entities in the electronic exchange of data in the market. In accordance with the Energy Agency's general act, all key data entities in an electronic data exchange have to be determined with standardised identifiers.

The Energy Agency has been implementing its harmonisation strategy through public consultations, bilateral cooperation and participation in professional platforms, such as the IPET Section and ebIX®. In 2021, the following key issues were considered in the framework of the IPET Section:

- The project of a single entry point of the national data hub, data quality and new functionality;
- Setting up a catalogue of data that is exchanged in the electricity market;
- Development of the EU regulation on cybersecurity in the energy sector and consideration of the draft framework of the network rules in the energy sector;
- Preparations for the inclusion of consumers with an installed capacity of 43 kW or lower in the metered diagram;
- Consideration of the draft amendments to the System operating instructions for the electricity distribution system (SONDSEE);
- Proposal of a method for substituting of the missing measurements in the customer's profiles.

In the framework of ebIX, the focus was on modelling the processes in the area of flexibility and on an active contribution to the emerging EU framework for ensuring interoperability

The Government Decree on measures and procedures for the introduction and interoperability of advanced electric power metering systems (hereinafter the Decree) and the Plan for the introduction of an advanced metering system in the Slovenian electricity distribution system (hereinafter the Plan) define, among other things, the advanced metering system architecture, roles and responsibilities, its minimum functionalities, and some aspects of the implementation of data exchange based on relevant standards (CIM, etc.) The Decree requires the DSO to establish a single access point for accessing data in the advanced metering system. Based on the Plan mentioned above, the system is implemented as a central system for accessing metering data (national data warehouse), which is managed by the DSO and provides data exchange services among business entities and network users in the B2B and B2C domains, with a plan to further extend the area of exchange to the B2G segment. The development was carried out within an initiative by distribution companies, united under the Electricity Distribution Economic Interest Grouping, with the participation of the DSO. The single entry point of the

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

national data hub (EVT/Portal CEEPS) is a hub ensuring the exchange of data among distributors and suppliers of electricity, final consumers and their authorised representatives (e.g. aggregators, ancillary services providers) and at the same time the central data hub for the exchange of data in the electricity market.

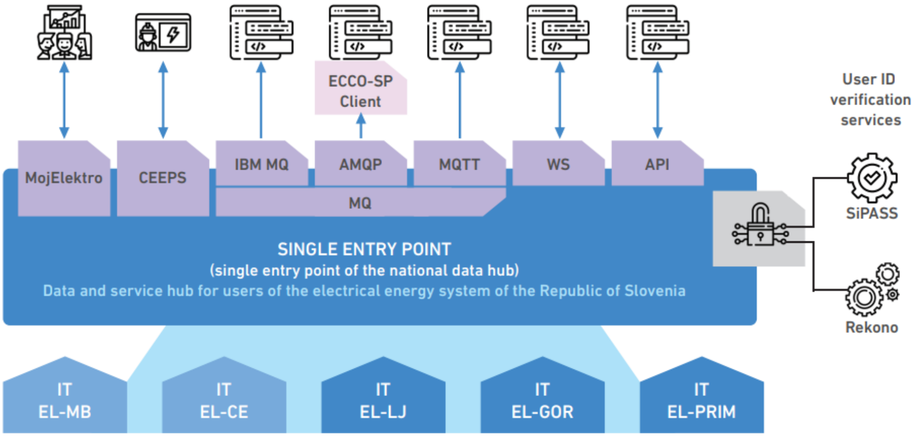


Figure 5-8 - HIGH-LEVEL ARCHITECTURE OF THE EVT NATIONAL DATA HUB.

The EVT provides a safe (two-step verification of a user's electronic identity) and unified registration and authentication with the Rekono application, as well as autonomous management of authorisations and user rights. It consists of the following building blocks:

- The MojElektro Portal – the online user portal intended for all end consumers and their authorised representatives who can access all the metering points and metering and accounting data that they are entitled to, regardless of their supplier or distribution area. It enables an overview and export of all available 15-minute data by metering points (received and delivered active/reactive power, possibility of aggregation by hour, day, month, etc.), monitoring consumption and production above the self-supply metering points, submission of a new tax ID number for a metering point, the submission and entry of the meter reading at a metering point;
- CEEPS Portal – for users eligible to access data, it fully replaces the PERUN in terms of functionality54. All electricity suppliers, Borzen, the Centre for RES/CHP support, the closed distribution systems and the distribution network operator are registered on the portal. It enables centralised imbalance settlement, access to and export of 15-minute data based on balance sheet eligibility, the submission and entry of meter readings on behalf of the final consumers, carrying out the supplier switching process in line with the SONDSEE requirements, access to accounting data (the so-called Annex A), management of all the changes on the metering points, etc.;
- Massive data exchange - B2B MQ services, continuous daily massive data exchange for the individual eligible user, daily transmission of the available 15-minute metering data

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

for the previous day, the addition of new measuring points to the daily transmission and specific inquiries for the available 15-minute metering data.

From the perspective of Slovenia state level, Slovenian Ministry of the Economy, Tourism and Sport published as one of the on-going projects (Jun2022-Dec2024), actually is in the preparation status: Ministry intends to implement the European Common Data Infrastructure and Services (IPCEI-CIS) project as part of the National Recovery and Resilience Plan, more specifically under the Digital Economy Transformation component.

The aim of the initiative is to ensure competitive, fair, secure and sustainable access to cloud capacity from anywhere in the EU. To achieve this, activities will be carried out to design, pilot, test and upgrade the use of cloud capacity in EU Member States.

The initiative aims to:

- create a common and multifunctional pan-European interconnected and secure data processing infrastructure,

- develop capabilities that can meet the real-time needs of users close to the sources where the data is generated,

- create secure and interoperable platforms for sectoral applications, allowing the exchange and sharing of data from common European data spaces.

No action plan or any detailed document is available, yet.

Beside before motioned project, same Ministry announced also another project, where the point is a hub for European Infrastructure for Blockchain Services (EBSI) hub. With this hub, an appropriate test infrastructure for blockchains will be put in place, contributing to more reliable cross-border, national and local services.

The EBSI project will support the upgrade of nodes and the addition of new nodes to the network. This will allow the inclusion of new target groups, the development of additional services, which will be further supported by Early Adopters initiatives. This will also ensure complementarity with the Digital Europe programme. Together with this, it will support the knowledge and skills transfer environment addressed by the establishment of a Blockchain Competence Centre in Slovenia as a complementary measure to the Digital Europe programme.

Building on the EBSI project and upgrading national infrastructures, the national blockchain infrastructures of at least three EU Member States and link national infrastructures with EBSI to services in the field of digital identities and other areas will be connected and integrated.

Slovenian Blockchain Partnership

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

The Slovenian Blockchain Partnership is being formed to implement the EBSI project as a cross-border and multi-country project and to build on it to ensure consistency with the Digital Europe Programme.

In the next version of this Deliverable (D7.2), data sharing incentives and business models from the DSO side will be updated with closer look to the EU incentives, focusing on the differences in the sections described above.

### 5.2.2 TSO

This section highlights data sharing schemes with energy and non-energy sector stakeholders from the transmission system operator's (TSO) perspective. The types of data that TSO needs to share with stakeholders, including generation and consumption data, network topology and status, market data is addressed in this section.

The data, shared by the TSO, can be divided in several parts:

- Open data that is provided in the real-time domain;
- Open data that is provided periodically;
- Confidential data that is provided to other energy and non-energy sector stakeholders.

The examples of the real-time open data are ENTSO-e e Transparency Platform and different data hubs that are present due to country's regulatory requirements.

ENTSO-e Transparency Platform is a centralized database that provides information on the European electricity market, including data on the availability and use of transmission capacity, generation and consumption data, and electricity prices. The requirement for TSOs to provide information to the ENTSO-E Transparency Platform is established by the European Union's Third Energy Package, which includes several regulations and directives aimed at promoting market transparency at the European level, facilitating cross-border cooperation, encouraging data harmonization and standardization among TSOs and improving energy security. The main regulation that establishes the requirement for TSOs to provide information to the ENTSO-E Transparency Platform is Regulation (EC) No 714/2009 of the European Parliament and of the Council of 13 July 2009 on conditions for access to the network for cross-border exchanges in electricity. This regulation requires TSOs to provide information on cross-border capacity, balancing markets, and other aspects of the electricity market to the ENTSO-E Transparency Platform. In addition, the European Union's Regulation (EU) 2019/943 on the internal market for electricity and Directive (EU) 2019/944 on common rules for the internal market for electricity also establish requirements for TSOs to provide data and information to the ENTSO-E Transparency Platform and to ensure transparency in the electricity market.

Along with the ENTSO-e Transparency Platform, every TSO need to provide the real-time data to the local data hubs. As an example, Portuguese TSO is obliged to provide the data to Portuguese TSO DataHub and Portuguese TSO Market Hub.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

Portuguese TSO DataHub is a platform that provides access to both real-time information on the status of the Portuguese electricity transmission system, including information on electricity generation, consumption, and interconnections with other countries and information about the network topology (not in real-time). All the real-time information is updated every 15 minutes. Portuguese TSO is obliged to provide this information according to the Decreto-Lei n.º 15/2022, de 14 de Janeiro and "Código da Rede de Transporte" (Transmission Grid Code), which defines the rules for the Portuguese TSO and aims at ensuring the data accessibility to stakeholders and promoting collaboration and knowledge sharing among stakeholders.

Portuguese TSO Market Hub is providing access to market data and analysis, including information on electricity prices, demand, and supply, as well as market reports and other relevant data. All the real-time information is updated every hour. Portuguese TSO is obliged to provide this information according to the Decreto-Lei n.º 15/2022, de 14 de Janeiro and "Regulamento do Mercado de Eletricidade" (Regulation of the Electricity Market) e do "Mercado de Derivados da Eletricidade" (Electricity Derivatives Market) and aims at promoting market transparency.

In addition to the real-time data, ENTSO-e is obliged to publish specific data periodically, which is obtained from the TSO's in a certain timeframe. As an example, ENTSO-e is obliged to publish Ten-Year Network Development Plan (TYNDP), Grid Connection Network Codes and Operational Reports.

Ten-Year Network Development Plan is a comprehensive planning document that outlines the development scenarios and investment needs of the European electricity transmission network for the next ten years. It is published in accordance with the requirements of the European Union's Regulation (EC) No 714/2009. It serves as a roadmap for the future development and expansion of the European transmission system. The main purpose of the TYNDP is to assess the future needs of the electricity transmission network, identify potential bottlenecks, and propose infrastructure projects to ensure the reliable and efficient operation of the European electricity system. It takes into account various factors such as electricity demand, generation mix, renewable energy integration, and cross-border exchanges. The TYNDP provides an overview of the infrastructure projects that are considered necessary to address the challenges and meet the evolving requirements of the European electricity market. It includes detailed analysis, forecasts, and recommendations for the development of the transmission system, taking into account different scenarios and potential future developments.

Grid Connection Network Codes, published periodically by ENTSO-E, are a set of technical requirements, guidelines, and procedures that define the rules for connecting new electricity generation and consumption facilities to the electricity grid. These codes establish standardized and harmonized rules across the European Union to ensure a consistent and efficient process for grid connections. They aim to facilitate the integration of renewable energy sources, promote fair and non-discriminatory access to the grid, and maintain grid stability and security.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

They are published in accordance with the requirements of different regulations, such as the European Union's Regulation (EU) 2019/943 and Commission Regulation (EU) 2016/631.

ENTSO-e's Operational Reports provide detailed information and insights on the operation and performance of the European electricity transmission system. These reports offer a comprehensive overview of various aspects related to grid operation, electricity flows, system adequacy, and security. ENTSO-E is required to publish operational reports in accordance with the European Union's Regulation (EU) 2017/1485 on establishing a guideline on electricity transmission system operation (SO GL). Under the SO GL, ENTSO-E is responsible for developing and implementing common rules and methodologies for the operation of the European electricity transmission system. These rules aim to ensure the secure, efficient, and coordinated operation of the transmission system across Europe.

Along with the data, published by ENTSO-e, every TSO needs to publish the data in accordance with the local regulations. For Portugal, Portuguese TSO is required to publish periodically the list of various reports, among which are:

- PRIDT – Plano de Desenvolvimento e Investimento da Rede Nacional de Transporte (Grid Development Plan);
- Relatório Anual (Annual Report);
- CRNT – Caracterização da Rede Nacional de Transporte (Characterisation of the National Transmission Network for purposes of Network Access);
- CINT – Caracterização das Interligações (Interconnections Characterisation);
- RQS – Relatório da Qualidade de Serviço da RNT (Quality of Service Report);
- RMSA - Relatório de Monitorização da Segurança de Abastecimento (Supply Adequacy Monitoring Report);
- Environmental, Social, and corporate Governance reports.

PDIRT is a strategic planning document that outlines the Portuguese TSO vision and plans for the development and operation of the national electricity transmission grid. It is updated every two years and serves as a roadmap for the Portuguese TSO to ensure the safe, reliable, and efficient operation of the grid. It identifies key challenges, such as the integration of renewable energy sources, the implementation of new technologies, and the reinforcement of the grid's interconnections with other European countries. PDIRT is an important tool for stakeholders, including energy producers, distributors, and consumers, as it provides a transparent and comprehensive overview of the Portuguese TSO's priorities and plans for the future development of the electricity transmission grid. It also helps to ensure that the grid development is aligned with the country's energy policies and goals, including the promotion of renewable energy and the reduction of greenhouse gas emissions.

Annual Report of the Portuguese TSO is a document that provides a comprehensive overview of the TSO's activities, operations, and financial performance in a given year. The report is published annually and serves as a valuable tool for stakeholders to evaluate the TSO's

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

performance and track its progress. The report includes information on the TSO's activities, key performance indicators, investments, regulatory environment, and environmental and social performance. It offers transparency and accountability, ensuring alignment with goals and responsibilities.

CRNT is a data report published by the Portuguese TSO that provides a comprehensive overview of the national transmission network, including its infrastructure, capacity and operational characteristics. The incentives to share this data include promoting transparency and market understanding, facilitating efficient grid planning and operation, enabling stakeholders to make informed decisions regarding network utilization and investments, and promoting fair competition and market integration. Sharing the CRNT data helps ensure a reliable and robust transmission network, supporting the sustainable development of the energy sector in Portugal.

CINT is a data published by the Portuguese TSO, which provides detailed information about the interconnections between the Portuguese electricity transmission system and Spanish electricity transmission system. The aim to share this data is to enhance transparency and promote market integration, enabling stakeholders to assess cross-border electricity flows, support efficient grid planning and operation, and facilitate cooperation and coordination with Spanish TSO.

RQS is published in accordance with the Quality of Service Regulation of the Electric Sector, which establishes the technical and commercial requirements of the services provided in the National Electric System. The Quality of Service Report contains detailed information on the quality of service provided by the National Transmission System, namely information about service continuity, voltage quality, availability of the network and quality of electricity supply. Although the publication of this report is mandatory, it also intends to provide a better understanding of the different aspects related with the quality of service of a transmission network.

RMSA is a data report published by DGEG (General Directorate for Energy and Geology) that provides information on the monitoring of supply security in the energy sector, including the needs of the system (in the electricity sector, in the natural gas sector and in the oil and petroleum products sector) in the medium and long term. Although this report is shared by DGEG, the sections related to the electricity sector are completed by the Portuguese TSO. Sharing this data promotes transparency, supports risk assessment and mitigation measures and ensures the reliable and secure supply of energy to consumers.

ESG reports are data reports provided by the Portuguese TSO, which contain information on the Portuguese TSO's environmental impact, social responsibility initiatives, and corporate governance practices. They are provided to comply with the set of company standards that socially responsible investors use to validate potential investments and must be incorporated into an organization's strategy. Sharing this data enhances transparency, demonstrates commitment to sustainability and stakeholder engagement and supports accountability.

In addition to the open data, Portuguese TSO shares the confidential data in real-time, using the ICCP (Inter-control Center Communications Protocol), mainly with Spanish TSO and Portuguese DSO. In addition, Portuguese TSO is obliged to provide the confidential data to ERSE (Energy Services Regulatory Authority) and DGEG, which are the regulatory authorities that have the responsibility to ensure the proper functioning and regulation of the energy sector in Portugal. Based on the data, these authorities publish various reports in order to ensure transparency, facilitate regulatory oversight and support market monitoring.

### 5.2.3 Multi-utility

The provision of real-time data to customers or other institutions in the field of distribution heat is currently not yet legally required. One of the main reasons for this is that the current introduction of smart metering for end users does not yet make sense, as the technology does not yet provide an affordable method of data transmission. The data on heat energy consumption by the end user is either on a monthly basis (multi-apartment buildings, industrial consumption) or on a semi-annual level (broad consumption - single-apartment buildings).

This consumption data is available to users in the user web portal, where users can also electronically process payments, submit applications and forms, etc.

On the other hand, there more detailed data (temperature, pressures, flow, energy consumption) in real time (daily, hourly or minute level) for the operator of the distribution system for:

- Heat production source (heat intake point)
- Major hubs of the distribution system
- Larger heat substations
- Weather forecast and real data for two locations

This technological data is available for sharing with energy and non-energy sector stakeholders and can be easily transmitted in real time with appropriate technology.

In the regulated multi-energy domain, the incentive mechanism should be created for stimulating data-sharing among different parties. For example:

- Access agreements between energy companies and energy and non-energy stakeholders should be established. Companies that proactively participate in such agreements may receive incentives, such as simplified regulatory procedures or preferential treatment in other areas.

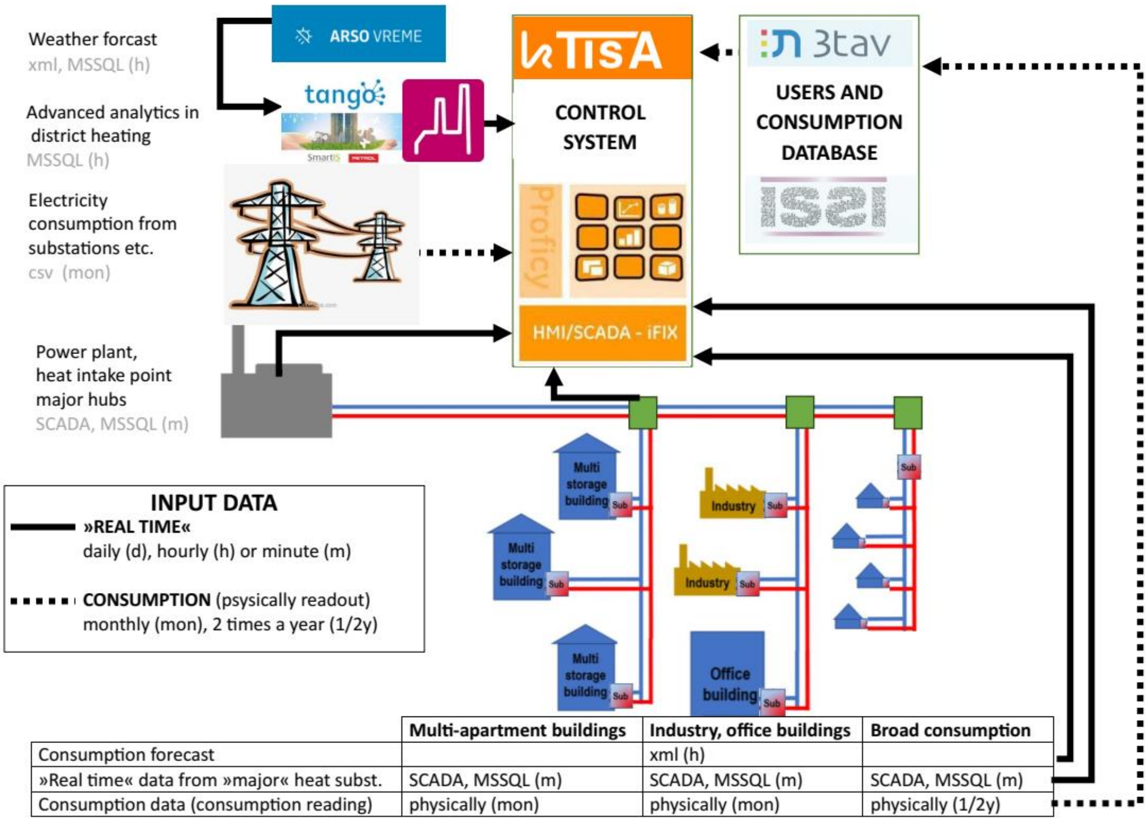
- Financial incentives to energy companies that voluntarily share their data. Incentives should be designed to offset the costs associated with data submission and sharing so that it makes more economic sense for companies to participate.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

- Energy companies may hesitate to share data because of concerns about data breaches or unauthorized access. Establishing robust security protocols and privacy policies can build trust, encouraging data sharing among stakeholders.

- Offering added value services to the companies that share the data. By demonstrating the added value of shared data, utilities may become interested in participating.

In the Figure 5-9 and Figure 5-10 the heat distribution system data input and output are presented respectively, describing the process of the collecting, storing and using the data for multi-utility data sharing.


Weather forcast
xml, MSSQL (h)
Advanced analytics in district heating
MSSQL (h)
Electricity consumption from substations etc.
csv (mon)
Power plant, heat intake point major hubs
SCADA, MSSQL (m)
ARSO VREME
tango
TISA
CONTROL SYSTEM
Proficy
HMI/SCADA - iFIX
3tav
USERS AND CONSUMPTION DATABASE
ISSI
Multi storage building
Sub
Industry
Office building
INPUT DATA
»REAL TIME«
daily (d), hourly (h) or minute (m)
CONSUMPTION (psysically readout)
monthly (mon), 2 times a year (1/2y)

| | Multi-apartment buildings | Industry, office buildings | Broad consumption |
|---|---|---|---|
| Consumption forecast | | xml (h) | |
| »Real time« data from »major« heat subst. | SCADA, MSSQL (m) | SCADA, MSSQL (m) | SCADA, MSSQL (m) |
| Consumption data (consumption reading) | physically (mon) | physically (mon) | physically (1/2y) |

Figure 5-9 - Heat distribution system data input

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

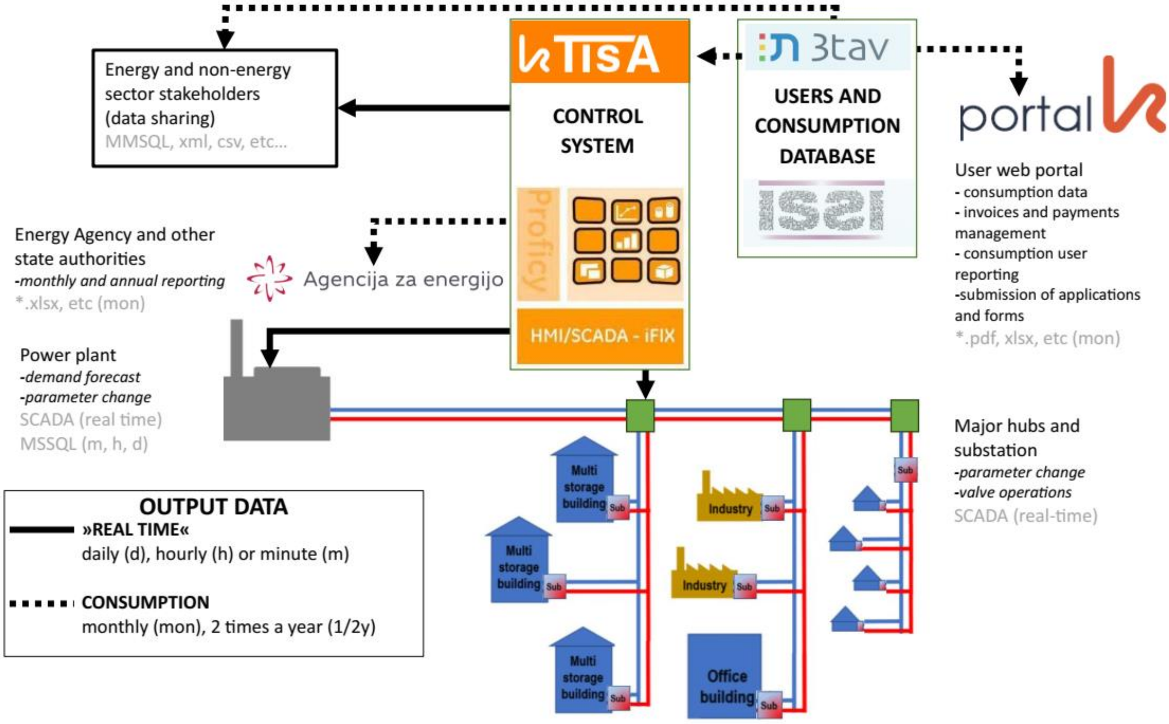


Figure 5-10 - Heat distribution system output data

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

# 6 Conclusion

This deliverable contains a detailed description of the data governance for Energy Data Spaces, covering such important aspect as data management, enterprise information management and data architecture. Different governance layers are identified from IDSA, which cover most of the reference architecture model layers. In addition to this, particular attention was paid to the differences for regulated and non-regulated domains and different Data Space Authority types. All these types were analysed in order to find advantages and disadvantages of different approaches in such aspects as ownership and sovereignty of the data, trust, privacy and security, value, quality and provenance of the data.

To ensure that the Data Governance Models in the scope of ENERSHARE project will be compliant with the European requirements and applicable to different operational context across Europe, the European Union regulations are analysed, namely:

- General Data Protection Regulation;
- Data Governance Act;
- Requirements for access to electricity metering and consumption data;
- Digital Services Act;
- Upcoming new EU legislation, EU laws, energy sector specific EU legislation;
- European Health Data Space.

All these acts and regulations were analysed from three main topics:

- Categories and uses of data;
- Roles and Actors in the Data Space;
- Rules and responsibilities of the data.

In addition to EU regulation, different initiatives, platforms and projects were analysed, which focuses on data exchange and there are specific requirements concerning data governance, namely:

- International Data Spaces Association;
- GAIA-X Association;
- FIWARE Foundation;
- OPEN-DEI Project;
- OneNet Project;
- BD4NRG Project;
- BRIDGE Initiative;
- Living Energy Lab.

Most of them were analysed from the reference architecture models point of view, focusing on the data governance methodologies.

To ensure that the Data Governance Models encompass all essential aspects and comply with national requirements, a questionnaire has been prepared for the pilots. This questionnaire aims to gain a clearer view of the data sharing mechanisms that will be utilized within the ENERSHARE project, facilitating the design of more detailed Data Governance Models that comprehensively cover all relevant topics. To cover most of the topics, the questions were grouped into five aspects:

- Data Ownership;
- Security, protection and sovereignty of the data;
- Access and consent management;
- Flow of the data;
- Logging and tracking of the data;
- Interoperability, portability and standardization of the data.

Although some of the aspect are broad, different sets of the questions were created in order to gather information about data sharing from the pilots. The goal is to ensure greater precision in developing the Data Governance Models by obtaining detailed insights from the pilots. In addition, the development of this questionnaire template involved close collaboration with the other horizontal WPs.

Taking into account the questionnaire, the list of initiatives, platforms and projects was analysed based on the questions, in order to identify existing gaps in them from data governance perspective and to be the starting point of the development of the Data Governance Models. The analysis showed that in some of the topics there was a lack of requirements in some of the projects, initiatives and platforms, for example:

- Some initiatives and platforms do not differentiate the roles “data owner” and “data provider”, “data user” and “data consumer”;
- Most of the observed initiatives, platforms, and projects neglect to differentiate between entity types (regulated or non-regulated);
- Some initiatives neglect to include requirements of the confidentiality of the data;
- DERA 2.0 from BRIDGE does not have specific requirements for tracking of the data, the methods used to track the data, and the information that should be tracked;
- Data portability is only partially covered within the context of data interoperability. In most of the initiatives and platforms, there is a lack of detailed requirements regarding data portability.

Most of the possible gaps were identified and a number of recommendations was made.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

In addition, the data sharing incentive and business models design was analysed, focusing on the differences in non-regulated and regulated domain. For the non-regulated domain, the mathematical algorithms were introduced, that are directed towards the mechanisms of monetary incentives, as well as expected advancements for the non-monetary incentive framework. The topics of data monetization addresses the topics of zero-regret auction mechanism that enable different power plant agents to sell data and buy forecasts and social welfare maximization, where the value of data is determined solely by buyers. The topic of non-monetary incentives is also analysed and ENERSHARE project propose a novel algorithm designed to optimize multilateral data exchange, ensuring equitable value exchange for each data owner involved in providing and receiving data. Additionally, the use cases were analysed from potential for B2B data sharing incentives perspective. Regarding the regulated domain, three big regulated roles were analysed, such as DSO, TSO and Multi-utility. The analysis was done in the topics of data exchange between different entities and the incentives to exchange the data.

# 7 References

[1] John Ladley, “How to Design, Deploy, and Sustain an Effective Data Governance Program Second ed.,” *Data Governance, Elsevier,* 2019.

[2] Earley Susan Deborah Henderson and Data Management Association, “Dama-Dmbok : Data Management Body of Knowledge Second ed,” *Bradley Beach New Jersey: Technics Publications.,* 2017.

[3] Curry, E., Scerri, S., Tuikka, T., “Data Spaces: Design, Deployment, and Future Directions,” 2022.

[4] IDSA, IDSA Rule Book – version2, 2023.

[5] IDSA, “IDSA Position Paper Governance for Data Space Instances Aspects and Roles for IDS Stakeholders,” 2021.

[6] Edward Curry, “Real-time Linked Dataspaces - Enabling Data Ecosystems for Intelligent Systems,” SpringerOpen, 2020.

[7] European Comission, “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”.

[8] European Comission, “Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance”.

[9] European Comission, “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”.

[10] European Comission, “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”.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

[11] European Comission, “Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services”.

[12] European Comission, “Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT)”.

[13] European Comission, “Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data”.

[14] European Comission, “Data Act – Questions and Answers,” 2023.

[15] European Comission, “Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements”.

[16] European Comission, “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”.

[17] European Comission, “COMMISSION STAFF WORKING DOCUMENT Accompanying the document COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Digitalising the energy system”.

[18] European Comission, “Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Health Data Space”.

[19] European Comission, “Feedback on the membership criteria and internal working rules of GAIA-X”.

[20] GAIA-X, “FAQs on the GAIA-X project”.

[21] GAIA-X, “GAIA-X Framework”.

[22] GAIA-X, “GAIA-X Data Spaces”.

[23] GAIA-X, “GAIA-X: A Federated Data Infrastructure for Europe”.

[24] GAIA-X, “Policy Rules Document”.

[25] GAIA-X, “Gaia-X: Compliance as Code,” 2022.

[26] OPEN-DEI, “Position paper: Design principles for Data Spaces,” April 2021. [Online]. Available: https://h2020-demeter.eu/wp-content/uploads/2021/05/Position-paper-design-principles-for-data-spaces.pdf.

[27] IDSA, “Reference Architecture Model,” April 2019. [Online]. Available: https://internationaldataspaces.org/wp-content/uploads/IDS-Reference-Architecture-Model-3.0-2019.pdf.

[28] CEN-CENELEC-ETSI Smart Grid Coordination Group, “Smart Grid Reference Architecture,” November 2012. [Online]. Available: https://www.cencenelec.eu/media/CEN-CENELEC/AreasOfWork/CEN-CENELEC_Topics/Smart%20Grids%20and%20Meters/Smart%20Grids/reference_architecture_smartgrids.pdf.

[29] Goncalves, Carla and Pinson, Pierre and Bessa, Ricardo J, “Towards data markets in renewable energy forecasting,” vol. 12, no. 1, 2021.

[30] Pinson, Pierre and Han, Liyang and Kazempour, Jalal, “Regression markets and application to energy forecasting,” *TOP,* 2022.

[31] Han, Liyang and Pinson, Pierre and Kazempour, Jalal, “Trading data for wind power forecasting: A regression market with lasso regularization,” *Electric Power Systems Research,* 2022.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

[32] “Official Gazette of the Republic of Slovenia, Article 60/19,” 8 10 2019. [Online]. Available: https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2019-01-2673/energetski-zakon-uradno-precisceno-besedilo-ez-1-upb2.

[33] “Official Gazette of the Republic of Slovenia, Article 158/20,” 2 11 2020. [Online]. Available: https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2020-01-2762/zakon-o-ucinkoviti-rabi-energije-zure.

[34] “Official Gazette of the Republic of Slovenia, Article 121/21,” 23 7 2021. [Online].

[35] “Official Gazette of the Republic of Slovenia, Article 172/21,” 29 10 2021. [Online]. Available: https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2021-01-3349/zakon-o-oskrbi-z-elektricno-energijo-zoee.

[36] “Official Gazette of the Republic of Slovenia, Article 44/22,” 29 3 2022. [Online]. Available: https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2022-01-0874/zakon-o-oskrbi-s-toploto-iz-distribucijskih-sistemov-zotds.

[37] “Official Gazette of the Republic of Slovenia, Article 88/16,” 30 12 2016. [Online]. Available: https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2016-01-3935/sistemska-obratovalna-navodila-za-distribucijski-sistem-toplote-za-geografsko-obmocje-mestne-obcine-velenje-in-obcine-sostanj.

[38] Agensija za energijo, “Report on the Energy Situation in Slovenia,” 2021.

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831

# Annex I – Questionnaire Template

| | | | | | | |
|---|---|---|---|---|---|---|
| **Data description within UC** | Is data or service? | Data/Service description | | | | |
| **Ownership** | **Owner**<br>Entity & type of party (regulated or non-regulated) | **Provider**<br>Entity & type of party (regulated or non-regulated) | **Target Consumer**<br>Entity & type of party (regulated or non-regulated) | **Target User**<br>Entity & type of party (regulated or non-regulated) | | |
| **Security, protection and sovereignty** | **Non-personal data** (anonymized, confidential) | **Cybersecurity measures** | **User' registration (Yes/No)** | **Users' authentication (yes/no)** | **Levels of authentication** | **Certificates** |
| **Access / Consent** | **Confidentiality level of data** (Public / case-defined confidential / confidential) | **Confidentiality level of meta-data** (owner, provider, date, location, other) | **Specific rules for access** (users' type, duration of use, maintenance?, disposal, offline retention/only via DS, derivation, reproduction, distribution, re-context) | **Access grants requirements**<br>Licensing, Agreements (NDA, MSA, SOW and SLA), GDPR | **Data rights**<br>Pair function (read, write, manage) + Agent (who) | |
| **Flow of data** | **Data starting point?** (Party/Role) | **Data final destination?** (Party/Role) | **Access is bidirectional?** | **Planning to use Data Space?** (end-to-end, end-to-platform) | **Are local storage infrastructures used?** | |
| **Logging & tracking** | **Need for dataflow tracking?** | **Methods/strategies for dataflow tracking.** | **Information needed to be tracked.** (internal control, billing, conflicts solving) | | | |
| **Interoperability, portability and standardization** | **Need for conversion of data formats (interoperability)?** | **Use converters from DS?** | **Needed conversions?** | **Are data ready to used by several entities** (portability/anonymization)? | **Are data ready to be reused in several UCs** (reusability)? | **Needs for quality of data?** Replicability, reusability |

Enershare has received funding from European Union's Horizon Europe Research and Innovation programme under the Grant Agreement No 101069831