



Cross stakeholder Data Governance for Energy Data Exchange D6.2

Authors:

Kalle Kukk (Elering),

Ferdinando Bosco (ENG)

Madalena Lacerda (E-REDES)

Vassilis Sakas (ED)

Apostolos Kapetanios (ED)

Konstantinos Kotsalos (ED)

Responsible Partner	Elering
Checked by WP leader	Vassilis Sakas (European Dynamics), 23.02.2023
Verified by the appointed Reviewers	Nermin Suljanović (EIMV), 10.03.2023 Nejc Petrovič (EG), 13.03.2023
Approved by Project Coordinator	Padraic McKeever (Fraunhofer), 29.03.2023

Dissemination Level	
PU	Public



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957739

Issue Record

Planned delivery date	31.03.2023
Actual date of delivery	29.03.2023
Status and version	V1.0

Version	Date	Author(s)	Notes
0.1	20.12.2022	Kalle Kukk (Elering), Kaja Trees (Elering)	Structure of the deliverable
0.2	23.01.2023	Kalle Kukk (Elering), Madalena Lacerda (E-REDES), Ferdinando Bosco (Engineering), Konstantinos Kotsalos (ED)	First full draft version, to be discussed in the task meeting
0.3	6.02.2023	All authors	The version containing all contributions from all authors
0.4	10.02.2023	Kalle Kukk (Elering)	The version for WP6 partners' and WP leader's review.
0.5	24.02.2023	Kalle Kukk (Elering)	The version for project reviewers.
0.6	20.03.2023	All authors	For coordinator's quality check.
0.7	28.03.2023	Kalle Kukk (Elering)	Addressing comments from quality check.
1.0	29.03.2023		Final version

Disclaimer:

All information provided reflects the status of the OneNet project at the time of writing and may be subject to change. All information reflects only the author's view and the Innovation and Networks Executive Agency (INEA) is not responsible for any use that may be made of the information contained in this deliverable.

About OneNet

The project OneNet (One Network for Europe) will provide a seamless integration of all the actors in the electricity network across Europe to create the conditions for a synergistic operation that optimizes the overall energy system while creating an open and fair market structure.

OneNet is funded through the EU's eighth Framework Programme Horizon 2020, "TSO – DSO Consumer: Large-scale demonstrations of innovative grid services through demand response, storage and small-scale (RES) generation" and responds to the call "Building a low-carbon, climate resilient future (LC)".

As the electrical grid moves from being a fully centralized to a highly decentralized system, grid operators have to adapt to this changing environment and adjust their current business model to accommodate faster reactions and adaptive flexibility. This is an unprecedented challenge requiring an unprecedented solution. The project brings together a consortium of over 70 partners, including key IT players, leading research institutions and the two most relevant associations for grid operators.

The key elements of the project are:

1. Definition of a common market design for Europe: this means standardized products and key parameters for grid services which aim at the coordination of all actors, from grid operators to customers;
2. Definition of a Common IT Architecture and Common IT Interfaces: this means not trying to create a single IT platform for all the products but enabling an open architecture of interactions among several platforms so that anybody can join any market across Europe; and
3. Large-scale demonstrators to implement and showcase the scalable solutions developed throughout the project. These demonstrators are organized in four clusters coming to include countries in every region of Europe and testing innovative use cases never validated before.

Table of Contents

1 Introduction	14
2 Data exchange initiatives, platforms and frameworks	16
2.1 Data Governance definitions and EU policy framework	16
2.2 Recommendations for data governance in literature	17
2.2.1 Barriers on the deployment of data exchange initiatives	19
2.2.2 Existing frameworks and standards on data exchange	19
2.2.3 Data Exchange Platforms and API development	20
2.2.4 Harmonised Role Models	21
2.2.5 Implementation at the national level	21
2.2.6 Sectoral involvement and integration	22
2.3 Review of selected data exchange frameworks	22
2.3.1 Flow of data	23
2.3.2 Data portability	24
2.3.3 Identification/registration mechanisms of the participants	25
2.3.4 Data ownership	25
2.3.5 Consent management	25
2.3.6 Logging	26
2.3.7 Licensing	26
2.3.8 Ownership and maintenance	27
2.3.9 Survey results analysis	27
3 Data governance related to OneNet architecture and middleware	29
3.1 Analysis of OneNet architecture and requirements (focus on data governance)	29
3.1.1 OneNet actors and roles	30
3.1.2 OneNet decentralised approach	31
3.1.3 OneNet and IDS	32
3.2 Analysis of other OneNet results related to Data Governance	33
3.2.1 Data quality	33
3.2.2 Data quality standards	34
3.2.3 Data Access Management	36
3.2.4 Data Security	37
3.3 OneNet Data Governance Framework	38
4 Reference Data Governance Model	42
4.1 Definition and scoping of data governance model	42

4.2	Elaboration of data governance requirements.....	44
4.2.1	Data governance business case	44
4.2.2	Orchestrated data governance	46
4.2.3	Rules and norms.....	47
4.2.4	Data ownership governance	49
4.2.5	Data access governance.....	49
4.2.6	Data security governance	50
4.2.7	Data vocabulary governance.....	51
4.2.8	Data platforms	53
4.2.9	Interfaces	56
4.2.10	Repositories.....	57
4.3	Results of data governance survey among OneNet partners	58
5	OneNet implementation and demonstration of cross-stakeholder Governance for Energy Data Exchange....	62
5.1	OneNet governance requirements identification.....	62
5.1.1	Governance Requirements Traceability Matrix	62
5.1.2	Governance Functional Requirements' mapping to Reference Data Governance Model	66
5.2	OneNet involvement in BRIDGE data exchange reference architecture implementation	68
5.3	Reference Data Governance Model elements in OneNet Data Governance Framework	70
6	Conclusion	71
	References	73
Appendix A	Survey responses from existing data exchange initiatives	79
A.1	Survey Responses - CoordiNet Platform	79
A.2	Survey Responses - ECCo SP	81
A.3	Survey Responses - IEGSA.....	82
A.4	Survey Responses - Estfeed	84
A.5	Survey Responses - Platone	85
A.6	Survey Responses - SYNERGY.....	87
A.7	Survey Responses – EUniversal.....	88
Appendix B	Data governance survey template	90
Appendix C	Appendix C: Governance Requirements Traceability Matrix (GRTM)	93

Table of Figures

Figure 1: Results from survey on the “Data access and storage” topic	23
Figure 2: Results from survey on the “Licensing” topic	27
Figure 3: OneNet Reference Architecture (OneNet D5.2, 2021 [47])	30
Figure 4: OneNet Decentralised Approach (OneNet D5.2, 2021 [47])	32
Figure 5: OneNet Data Access Policy Framework (OneNet D5.7, 2022 [49])	37
Figure 6: Application of the OneNet Data Governance Framework	40
Figure 7: Implementation of the data exchange process using the OneNet Data Governance Framework	41
Figure 8: Some already existing and still missing elements for smooth European data exchange	42
Figure 9: BRIDGE data exchange reference architecture DERA2.0 (BRIDGE, 2022 [9])	43
Figure 10: Data governance layers per SGAM interoperability layers	44
Figure 11: 4 most and 4 least relevant data governance requirements according to OneNet partners	59
Figure 12: 4 most and 4 least feasible data governance requirements according to OneNet partners	60
Figure 13: Top-10 data governance requirements implemented in OneNet	60
Figure 14: Illustrative data governance dimensions of OneNet reference architecture	66
Figure 15: OneNet connector as facilitator of data exchanges	69
Figure 16: OneNet Data Governance Framework mapping to SGAM based Data Governance Reference Model	70

Table of Tables

Table 1: Main recommendations on data governance based on the literature review	18
Table 2: Results from survey on the “Flow of data” topic	24
Table 3: OneNet cross-platform services categories (OneNet D5.3, 2021 [48])	35
Table 4: Data exchange governance elements per SGAM interoperability layers	43
Table 5: Relevance and feasibility of data exchange governance elements for OneNet partners.....	61
Table 6: Requirement traceability matrix (based on PM ² Alliance, 2020 [54])	63
Table 7: OneNet Governance Functional Requirements list	64
Table 8: OneNet Governance Functional Requirements reflected in Reference Data Governance Model	66

List of Abbreviations and Acronyms

Acronym	Meaning
ABAC	Attribute-Based Access Control
API	Application Programming Interface
B2B	Business-to-Business
BRP	Balance Responsible Party
CGMES	Common Grid Model Exchange Specification
CIM	Common Information Model
DAP	Data Access Policy
DB	Data Base
DBA	Data Bridge Alliance
DEP	Data Exchange Platform
DERA	Data Exchange Reference Architecture
DESAP	Digitalising the Energy System - EU Action Plan
DG	Data Governance
DLMS-COSEM	Device Language Message Specification – Companion Specification for Energy Metering
DSF	Demand Side Flexibility
DSO	Distribution System Operator
EC	European Commission
ECCo SP	ENTSO-E Communication & Connectivity Service Platform
ECP	Energy Communication Platform
EDA	Energy Data Exchange Austria
EDEF	Energy Data Exchange Framework in the Netherlands
EDX	ENTSO-E Data Exchange
EG	Expert Group
ENTSO-E	European Network of Transmission System Operators for Electricity
ESCO	Energy Service Company
ESMP	European Style Market Profile
EU	European Union
FAIR	Findability, Accessibility, Interoperability and Reusability
FR	Functional Requirement
FSP	Flexibility Service Provider
GAAP	Generally Accepted Information Principles
GAIP	Generally Accepted Information Principles

GDPR	General Data Protection Regulation
GFR	Governance Functional Requirement
GRTM	Governance Requirements Traceability Matrix
GUI	Graphical User Interface
HEMRM	Harmonised Electricity Market Role Model
HERM	Harmonised Energy Role Model
ICT	Information and Communication Technology
ID	Identity, Identifier
IDS	International Data Space
IDSA	International Data Space Association
IEC	International Electrotechnical Commission
IEGSA	Interoperable pan-European Grid Services Architecture
IoT	Internet of Things
ISO	International Organization for Standardization
IT	Information Technology
JSON	JavaScript Object Notation
JWT	JSON Web Tokens
KPI	Key Performance Indicator
LD	Linked Data
MADES	MArket Data EXchange Standard
MO	Market Operator
NGSI	Next Generation Service Interfaces
PDP	Policy Decision Point
PEP	Policy Enforcement Point
R&D	Research & Development
RAM	Reference Architecture Model
RBAC	Role-Based Access Control
RDGM	Reference Data Governance Model
SAREF	Smart Appliances REference (ontology)
SGAM	Smart Grid Architecture Model
SGTF	Smart Grids Task Force
SO	System Operator
SW	Software
TSO	Transmission System Operator
UC	Usage Control
UI	User Interface
UML	Unified Modelling Language

USEF	Universal Smart Energy Framework
VCE	Value Creation Ecosystem
WBS	Work Breakdown Structure
WP	Work Package
XML	eXtensible Markup Language

Executive Summary

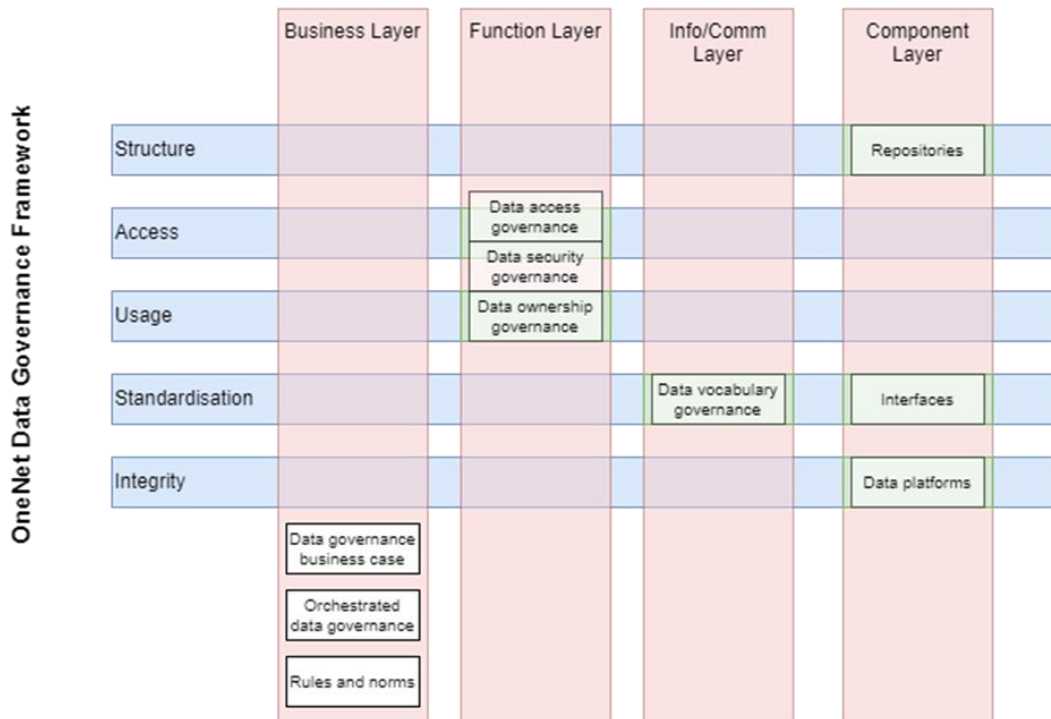
One can still often wonder why the (energy) data does not flow seamlessly across country borders and across sectors. This concerns specifically the ability to access and share the data which is generated and owned by end-customers. Definitely, there are many useful elements existing already and being developed for cross-border and cross-sector data exchange; however, a lot still needs to be done. A reference to a well-defined data governance framework could contribute to overcoming the remaining barriers.

This deliverable collected main recommendations on interoperability from literature and compared these with existing initiatives from European and independent projects. It was concluded that the majority of the recommendations are yet to be addressed, with the main work being done within the data portability topic, through application and creation of different standards, data models, data formats and ontologies. However, despite the recommendations are pointing more towards the open-source of data models and data architecture, the approach chosen by the initiatives is split between open-source and closed-source, possibly due to market competition reasons, therefore, greater efforts in this essential item need to be undertaken.

The deliverable analyses the OneNet system architecture and functional approach from a data governance perspective. One of the main goals during the design and definition of the OneNet data exchange framework was to make available and accessible data from different sources (actors) in a secure and trusted way ensuring data ownership and privacy. For this reason, it is useful to analyse how the OneNet architecture: defines the concepts of data providers and data consumers; implements the concept of fully decentralised data exchange; ensures the data ownership and consent management; and facilitates the cross-platform integration in a secure and interoperable way. These aspects are strictly connected with the Data Governance concept and for this reason a specific OneNet Data Governance Framework was designed and implemented. The framework consists of 5 important dimensions: Structure; Access; Usage; Standardisation; and Integrity. All the OneNet processes rely on these five dimensions.

The OneNet Data Governance Framework is aligned with the more generic and universal Reference Data Governance Model (RDGM) elaborated in this deliverable. RDGM consists of 10 elements and a set of requirements corresponding to each element. Data governance elements and their mapping to OneNet Data Governance Framework is depicted in the figure below.

Data Governance elements per SGAM Layers



The report proposes a set of data governance requirements:

1. Data governance business case

- 1.1. Define **business case** for data governance on relevant level [project / organisation / country / EU], e.g., by means of business model canvas or standardised IEC 62559-2 template.
- 1.2. Evaluate regularly the risks associated to the implementation of data governance programme using **risk assessment** methodologies.
- 1.3. Define and follow the **principles of data-as-an-asset**.
- 1.4. Define and monitor **KPIs** for data governance programme itself and for specific data exchanges.

2. Orchestrated data governance

- 2.1. Establish a **group to steer** the European Energy Data Space, open to European initiatives and stakeholders to participate, and ultimately leading to cooperation between energy and other sectors.
- 2.2. Define the **responsibilities and accountability** for European data exchange, including European Commission, Member states, data providers, data users, etc.

3. Rules and norms

- 3.1. Propose and promote **regulations and standards** facilitating improved data governance.
- 3.2. Understand regulatory and standards' **requirements** driving the need for proper data governance.

4. Data ownership governance

- 4.1. Ensure **consent management process** which is accessible to any party willing to provide or use any data and not limited to single country.

5. Data access governance

- 5.1. Ensure the availability of **one-stop-shop** providing information about and access guidance to different types of data.
- 5.2. Make available **single data access points** and ensure everyone's rights to access data.
- 5.3. Ensure legislative grounds for sub-meter and other **end-customer related data** governance.

6. Data security governance

- 6.1. Apply "**know-your-data-user**" **principle** by making data usage information available to data owners easily and free of charge.
- 6.2. Harmonise **authentication schemes** across Europe and sectors.

7. Data vocabulary governance

- 7.1. In data modelling, follow the generally recognised **reference models** for roles, information and processes.
- 7.2. Establish European arrangement for **coordinating reference models** and national mappings.

8. Data platforms

- 8.1. Make efforts and demonstrate the **interoperability of a data platform** with other European data platforms.
- 8.2. Call the common European (Energy) data space to keep the registry of and to issue **compliance labels** to interoperable data platforms.

9. Interfaces

- 9.1. Make available **interfaces** – Application Programming Interfaces and Graphical User Interfaces – of the data platform.
- 9.2. Provide unified European wide **guidance for integrating** with any of the European data platform for developers, data intermediaries, data providers and data users, regardless of their physical location and data type.

10. Repositories

- 10.1. Create common **European data repositories** at least for cross-sector data roles, data types (objects, profiles) and processes (use cases).
- 10.2. Make the common European data repositories available **free of charge**.

The deliverable creates the Governance Requirements Traceability Matrix (GRTM) and uses it for the assessment of OneNet project's governance functional requirements. These requirements are analysed vis-à-vis both RDGM and OneNet Data Governance Framework. The analysis indicated that there is an extended focus of OneNet developments on data access related functionalities. This is justified since OneNet adopts IDSA RAM



domain agnostic principles that enable participants to act as provider and/or consumer of data and to define their own access policies for any kind of data exchange assuming common authorisation and clearing services.

OneNet participation in the implementation of the Data Exchange Reference Architecture (DERA) of the BRIDGE Initiative was explored referring to the fact that OneNet connector can be the mediator to establish cross-demo and cross-sector secure and trusted information and data exchanges. BRIDGE DERA, given its alignment with DESAP (Digitalising the Energy System - EU Action Plan), will consider the OneNet data exchange framework, in particular the OneNet connector as a potential data space ecosystem.



1 Introduction

The BRIDGE report on TSO-DSO coordination revealed that there were few dedicated platforms for energy data exchanges existing or developing. Half of the projects investigated in the BRIDGE document demonstrated interoperability between platforms, while only few demonstrated cross-sector interoperability, whereby data could flow seamlessly across different economic sectors. This deliverable takes as its starting point the ‘landscape’ of existing and planned platforms used in different projects for different focal points of data exchange. In terms of governance, the OneNet solution should be built on data exchange platforms and frameworks such as Estfeed, ECCo SP, IEGSA and many others. Also, the deliverable follows recommendations given in literature and by initiatives like the European Smart Grids Task Force (SGTF) Expert Group 1 (2019 [30]; 2022 [31]) to facilitate interoperability by using available standards as a basis like IEC CIM (Common Information Model), by relying on role models like HEMRM (Harmonised Electricity Market Role Model) and by applying technology-neutral business requirements.

These recommendations are already followed by some ongoing projects. Chapter 2 addresses the main recommendations for increased interoperability gathered in literature and analysis existing initiatives from European projects and independent initiatives, to understand if those recommendations are being implemented.

Governance model elaborated in this deliverable is built on the use cases, data models, and trials demonstrated in Horizon2020 projects like EU-SysFlex, TDX-Assist and INTERRFACE. Chapter 3 analyses the OneNet system architecture and functional approach from the data governance perspective. It describes how the OneNet system addresses all the important aspects related to data governance designing a specific framework: the OneNet Data Governance Framework.

Based on the previous findings and OneNet analysis, this deliverable elaborates and proposes a generic Reference Data Governance Model (RDGM) in Chapter 4. The governance model should recognise the variety of different platforms and systems, fit to different market designs and business processes, enable cross-stakeholder, cross-border and cross-sector data exchanges, ensure easy access to data satisfying GDPR requirements, facilitate TSO-DSO coordination from customer perspective, ensure scalability through open-source principle and agreed rules.

The BRIDGE Initiative has proposed a sector-agnostic cross-border Data Exchange Reference Architecture – DERA2.0 (BRIDGE, 2022 [9]). The aim of DERA is to support cross-sector data interoperability. This deliverable attempts to make a step forward being more specific about the commonly agreed and to be taken administrative actions on European level to support the actualisation of Common Energy Data Space, and eventually the interoperability of sectoral data spaces. Such ‘administrative actions’ are the building blocks of data governance. Two levels of ‘building blocks’ are defined hereby. First, ten higher-level data governance elements are clustered

according to SGAM interoperability layers. Secondly, each element includes one or more specific governance requirements.

Chapter 5 identifies and presents the data governance developments of the OneNet reference architecture at its current status, including also specifications for future development during the lifecycle of OneNet project. The methodological approach applied is based on the following steps: 1) creation of the Governance Requirements Traceability Matrix (GRTM) for the specific functional requirements that are relevant to governance aspects; 2) reflection of specific functional requirements linking to the Reference Data Governance Model (described in Chapter 4); and 3) reference to the OneNet project participation in the BRIDGE DERA implementation focusing specifically on cross-sector stakeholder governance perspective.

2 Data exchange initiatives, platforms and frameworks

This chapter of the deliverable aims at addressing the main recommendations for increased interoperability and at analysing some existing initiatives, either from H2020 European projects, or from independent initiatives, to understand how these are tackling the main aspects within data governance itself, for instance, if the recommendations are being targeted or not. It is intended to serve as a guide, highlighting both the state of the art and best practices to provide support and information for adoption by decision makers, the ICT sector, end users (data intermediaries, service providers and users, data providers and users).

2.1 Data Governance definitions and EU policy framework

With the emergence of flexibility services, products and markets, the importance of data interoperability became even more clear for the energy sector, extending the need for harmonisation across sectors, namely Utility, Telecommunications and Home appliances sectors. This is highly relevant for demand side flexibility which requires clear integration between the IT infrastructure that connects Smart Meters, Consumer Energy Management Systems, Smart Appliances and Gateways between the home and external networks (E.DSO, 2020 [16]; 2022 [17]). Thus, a greater exchange and access of data does not only substantially improve efficiency gains in grid operation and planning, but also helps in lowering market access barriers, ensuring transparency in consumer usage and in the creation of new market opportunities (ENTSO-E, THEMA, 2017 [18]) and business models, which will require a well-established data governance framework.

There are multiple definitions of data governance, for instance Newman and Logan (2006 [45]) defined it as “the collection of decision rights, processes, standards, policies and technologies required to manage, maintain and exploit information as an enterprise resource”. SAP defines it as “the practice of organising and implementing policies, procedures and standards for the effective use of an organisation’s structured/unstructured information assets” [56]. Finally, the Data Governance Institute states that “Data Governance is a system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which describe who can take what actions with what information, and when, under what circumstances, using what methods” [14].

The European Data Strategy published by the European Commission (EC) aims at addressing issues like data availability, data interoperability, data governance, data infrastructure and the empowerment of individuals to exercise their rights. This should ensure that data can flow within the EU and across sectors, that data protection rules are fully respected, and that the rules of access to and use of data are fair, practical, and clear, with trustworthy data governance mechanisms in place (EC, 2020 [25]). More recently, the EC has published the communication on DESAP (Digitalising the energy system - EU action plan), that defines a strategic vision and concrete actions in different areas that are critical to the digitalisation of the energy sector, including actions for the promotion of connectivity, interoperability and seamless exchange of data between different actors, that

can also guarantee and respect the privacy and protection of the data (EC, COM(2022)552 [27]). Under the DESAP, one of the actions foreseen to be implemented by the EC, is the adoption and preparation of implementing acts on interoperability requirements and procedures, regarding the access to metering and consumption data, to data required for demand response, to customer switching data, and to data related to 'other services' (EC, COM(2022)552 [27]).

For certain strategic sectors and domains of public interest the creation of European Data Spaces is planned, including a Common European Energy Data Space, which aims at promoting stronger availability and cross-sector sharing of data, through a customer-centric, secure, and trustworthy approach, facilitating innovative solutions and supporting the decarbonisation of the energy system. The coordination of this data space is being led by the int:net project¹, that brings together relevant stakeholders from the European energy sector to jointly work on developing, testing and deploying interoperable energy services. The governance of this Common European Energy Data Space is to be established by the EC, as one of the actions foreseen within the DESAP, together with the support of its deployment through a Digital Europe Programme² call for proposals (EC, COM(2022)552 [27]).

Despite these developments at EU level to boost interoperability and allow for cross-sector exchange of data, there are still a lot of barriers to tackle. Fortunately, a significant effort has been put through by varied institutions and projects to map recommendations and solutions to solve these barriers, some of which are tackled in the following sub-chapter.

2.2 Recommendations for data governance in literature

This section will dive into the main recommendations retrieved from literature regarding Data Governance, but before that, an introduction and analysis to the main barriers identified so far will be done, around which the recommendations are then built.

The main recommendations mentioned within this chapter, and that were gathered from literature, are summarised in Table 1, and are further detailed in the following sub-chapters.

¹ <https://intnet-project.eu/>

² <https://digital-strategy.ec.europa.eu/en/activities/digital-programme>

Table 1: Main recommendations on data governance based on the literature review

#	Recommendation
1	Extend CIM standard with canonical data models from other sectors to allow for cross-sector data exchange, while also evaluating the benefits of using ontologies (BRIDGE, 2021 [8]).
2	Create a roadmap for interoperability that is closely monitored and accordingly adapted along the way (EU SGTF EG1, 2019 [30]; 2022 [31]).
3	Harmonised data models and architectures benefit interoperability, particularly under open-source licenses (BRIDGE, 2021 [8]).
4	Data quality should follow the principles: complete, timely, accessible, machine processable, non-discriminatory, non-proprietary and license free; and in similarity to these ones, data exchange should also comply with the FAIR (findability, accessibility, interoperability and reusability) principles (Tauberer, 2014 [60]).
5	Provide data portability through direct download and user-friendly APIs that need to be as close to real-time as possible (Hofheinz and Osimo, 2017 [35]).
6	Introduce well-established APIs at first but pending more demanding requirements with a revision of the sectoral legislation and GDPR (Ilves and Osimo, 2019 [40]).
7	Create a new mechanism for proposing new roles by BRIDGE Initiative to allow harmonisation of roles across electricity and other energy domains by developing a Harmonised Energy Role Model (HERM) (BRIDGE, 2021 [8]).
8	Look at other sectors to allow consistency outside the energy sector (BRIDGE, 2021 [8]).
9	An EU entity for interoperability could take the key role of organising the various innovation tools that are scattered across projects and stakeholders (BRIDGE, 2021 [8]).
10	Pursue a core model that adopts and allows for national specificities, while ensuring that it stays open for increased interoperability (EU SGTF EG1, 2019 [30]; 2022 [31]).
11	The enforcement responsibility should fall under the national regulator, ensuring that compliance is enforced and that regional differences are accommodated (ASSET, 2020 [4]).
12	The transparency at Member State level can be increased by making the role models, the data formats and all standards and non-standards procedures publicly available (ASSET, 2020 [4]).
13	To further promote the normalisation of data at the national level in Member States, the Governments should lead by example with the way they handle their own data and influence the public sector to adapt its current practices (Ilves and Osimo, 2019 [40]).
14	Organisations need to enable individuals to understand its privacy policies and how to manage them, certifying that they can be empowered to give, deny, or revoke consent to share data on a basis of why, how and for how long the data is to be stored and used (Hofheinz and Osimo, 2017 [35]).
15	The push for SGAM should be made and its extension to other sectors should be considered while developing cross-sector data models and profiles. The data format must follow an agnostic approach in cross-sector data exchange (BRIDGE, 2021 [8]).

2.2.1 Barriers on the deployment of data exchange initiatives

The BRIDGE Initiative has published a report on the European energy data exchange reference architecture aiming to contribute to the discussion and definition of practical steps towards truly interoperable and business process agnostic data exchange at EU level, both within the energy sector and across different sectors (BRIDGE, 2021 [8]). In that aim, and to collect the experience and know-how from ongoing EU R&D projects, a questionnaire was prepared and disseminated to projects participating in the BRIDGE Initiative, and within it, the main barriers limiting the deployment of data exchange initiatives in the electricity sector and, consequently, the accomplishment of a common European reference architecture were addressed. The main issues with impact on the development of interoperability functionalities were rated by the stakeholders in the following order of importance (from the most to least):

1. “the unwillingness among players to exchange private data and models due to privacy issues.
2. the limited standards and generally the need for updates.
3. the vulnerability to cyber-attacks.
4. the competition among vendors/tech procurers.” (BRIDGE, 2021 [8])

Apart from these, it is important to note that the national markets’ legal aspects can be a limiting factor in achieving full interoperability.

For the means of achieving interoperability, the introduction of more standards may not contribute to solving the problem but can in fact aggravate it. However, forcing and pressuring stakeholders to use or support standards requires a more in depth understanding to better maximise the resulting benefits.

2.2.2 Existing frameworks and standards on data exchange

The security layer of smart grid communication infrastructure and smart grid devices should have minimum requirements and standards (BRIDGE, 2019-1 [6]) and the adoption of currently available European standards should be the basis to improve on interoperability. One of the identified standards that could be among the solutions to improve TSO-DSO coordination is CIM (Common Information Model) (BRIDGE, 2019-2 [7]). The extension of this standard with canonical data models from other sectors should be considered to allow for cross-sector data exchange. However, at the same time, it is also important to evaluate the benefits of using ontologies (Recommendation #1) (BRIDGE, 2021 [8]). An example on the use of ontologies is the project InterConnect³, that is based on open standards, such as SAREF (Smart Appliances REference ontology), to guarantee the semantic interoperability between the equipment and systems from homes, buildings, and

³ <https://interconnectproject.eu/>

electricity networks. The need for further advancement of standards by the evolving flexibility products requires further incorporation of said products and other developments currently arriving at the market, so that it keeps up with innovation and new trends (BRIDGE, 2021 [8]). As for today, there are many frameworks and standards that are influencing the overall picture of energy data exchange architecture (BRIDGE, 2019-2 [7]), namely:

- Information models: CIM, IEC 61850, USEF, DLMS-COSEM (Device Language Message Specification – Companion Specification for Energy Metering), SAREF, UMEI (Universal Market Enabling Interface).
- Data exchange architectures: GAIA-X, IDS (International Data Spaces), EDA (Energy Data Exchange Austria), EDEF (Energy Data Exchange Framework in the Netherlands), OPEN DEI, FIWARE, Estfeed, Data Bridge Alliance.
- Guidelines: HEMRM, EC Communication on European Interoperability Framework; EC's annual Rolling Plan for ICT Standardisation.

However, to reach and maintain interoperability, a step-by-step approach needs to be adopted, requiring a roadmap that will be closely monitored and adapted accordingly along the way (Recommendation #2) (EU SGTF EG1, 2019 [30]; 2022 [31]). In addition, the business requirements should be in the central focus point in the pursuit of interoperability and remain technology-neutral (EU SGTF EG1, 2019 [30]; 2022 [31]). Finally, harmonised data models and architectures benefit interoperability, particularly under open-source licenses (Recommendation #3) (BRIDGE, 2021 [8]).

2.2.3 Data Exchange Platforms and API development

Data Exchange Platforms (DEPs) can be one of the tools to improve coordination and market functionality (ENTSO-E, THEMA, 2017 [18]). DEPs can be made interoperable by developing APIs that assure that data providers and data users can easily connect to any European DEP, and by doing so, ensure data exchange with any other stakeholder in Europe (BRIDGE, 2021 [8]). The exchange of data through APIs is becoming more and more recommended, as they can be product enablers, product components, or even products themselves. They give enterprises great potential, as they can manage APIs like a product and design them like a service. Like all products, APIs are tools to deliver value from producers to consumers, as a digital product they can offer immediacy, and as software interfaces, they can be easily automated, updated and composed (Fishman and McLarty, 2021 [32]).

Beyond the use of APIs, data quality should be also considered and should follow the original eight principles of open government data first established in 2007 by 30 open government advocates in California. These principles require the data to be complete, timely, accessible, machine processable, non-discriminatory, non-proprietary and license free. Similar to these principles, the European strategy for data (EC, 2020 [25]) supports the importance of the data exchanged to comply with the principles on Findability, Accessibility, Interoperability and Reusability (FAIR), that should certainly need to be taken into account (Recommendation #4) (Tauberer,

2014 [60]). A great focus should be made in providing data portability through direct download and user-friendly APIs that need to be as close to real-time as possible (Recommendation #5) (Hofheinz and Osimo, 2017 [35]).

A push for well-established APIs to achieve portability, as a set of soft recommendations at first but pending more demanding requirements with a revision of the sectoral legislation and the GDPR may also be considered (Recommendation #6) (Ilves and Osimo, 2019 [40]).

2.2.4 Harmonised Role Models

At the European level, some initiatives and entities have also contributed to achieving full interoperability. A new mechanism for proposing new roles by BRIDGE Initiative would allow to harmonise data roles across electricity and other energy domains by developing a Harmonised Energy Role Model (HERM) (Recommendation #7) (BRIDGE, 2021 [8]). Other sectors should be looked at in other aspects to allow consistency outside of the energy sector (Recommendation #8) (BRIDGE, 2021 [8]).

Also, an EU entity for interoperability could take the key role of organising the various innovation tools that are scattered across projects and stakeholders (Recommendation #9) (BRIDGE, 2021 [8]). This could improve future approaches and steer a common course of action by identifying challenges and providing new solutions and mechanisms for different interoperability issues (BRIDGE, 2021 [8]). In this field, good development has already been achieved through the int:net project⁴, by bringing together different initiatives on interoperability, legal and regulatory bodies, to build a consensus on how European governance and industry can foster interoperability on all levels, with one of the goals being to have a follow-up legal entity on interoperability, in the form of an association or non-profit organisation.

2.2.5 Implementation at the national level

At the national level, the convergence of national practices and the potential achievement of full interoperability at EU level are key to exchanging and accessing data. As such, a core model that adopts and allows for national specificities ought to be pursued, while ensuring that it stays open for increased interoperability (Recommendation #10) (EU SGTF EG1, 2019 [30]; 2022 [31]). The enforcement responsibility should fall under the national regulator, ensuring that compliance is enforced and that regional differences are accommodated on the national level (Recommendation #11) (ASSET, 2020 [4]). Transparency at Member State level can be increased by making the role models, the data formats and all standards and non-standards procedures publicly available (Recommendation #12) (ASSET, 2020 [4]).

Data exchange platforms are a key tool to achieving interoperability and can be used in a cross-border approach by connecting the national data systems and translating the national specificities (E.DSO, 2020 [16]).

⁴ <https://intnet-project.eu/>

The involvement of all the stakeholders that have a direct impact must be guaranteed ensuring they are able to discuss and negotiate (EU SGTF EG1, 2019 [30]; 2022 [31]).

2.2.6 Sectoral involvement and integration

To further promote the normalisation of data at the national level in Member States, the Governments should lead by example with the way they handle their own data and influence the public sector to adapt its current practices, for example, to voluntarily comply with GDPR requirements on data access and reuse (currently exempted) and implement standardised APIs for their data (Recommendation #13) (Ilves and Osimo, 2019 [40]). Including a voluntary compliance with the GDPR (currently it has an exception for the public sector) and implementation of APIs for public data and non-public data restricted by right to access (Ilves and Osimo, 2019 [40]).

GDPR concerns should be on top of data interoperability priorities ensuring its compliance and in making sure that owners retain control over their data (BRIDGE, 2019-2 [7]). Hence, organisations need to enable individuals to understand their privacy policies and how to manage them, so that they can be empowered to give, deny, or revoke consent to share data on a basis of why, how and for how long the data is to be stored and used (Recommendation #14) (Hofheinz and Osimo, 2017 [35]).

The Smart Grid Architecture Model (SGAM) usage should also be promoted and its extension to other sectors should be considered while developing cross-sector data models and profiles. The data format must follow an agnostic approach in cross-sector data exchange (Recommendation #15) (BRIDGE, 2021 [8]).

Exchanged and stored data will grow past mere metering values to also include market data, like weather forecasts or spot prices, grid congestions, unavailability of assets or possibly even grid-planning data where this is relevant for other stakeholders besides system operators (ENTSO-E, THEMA, 2017 [18]).

2.3 Review of selected data exchange frameworks

To have an overview of the main approaches and characteristics of existing data exchange initiatives developed under the H2020 European projects that were analysed in deliverable D2.1 [46] and under other independent initiatives, a survey was conducted, in the beginning of 2022, and responded by representatives from all the different initiatives targeted, which were the following: CoordiNet, ECCo SP, IEGSA, Estfeed, Platone, SYNERGY and EUniversal. It is important to highlight that these initiatives were selected due to the presence of representatives within the OneNet consortium.

The topics addressed in the survey were: i) Data access and storage; ii) Flow of data; iii) Data portability; iv) Identification/registration mechanisms of the participants; v) Data ownership; vi) Consent management; vii) Logging; viii) Licensing; ix) Ownership and maintenance. These topics were chosen based on expert opinion from the task members while scoping these tasks.

The main conclusions and observations from the survey for each of the addressed topics are presented below. The responses gathered from the survey can be found in Appendix A.

It was identified how the exchange of data is handled in the different projects and initiatives, by asking if either a central/shared storage approach or a distributed/decentralised one that would enable a message-based integration is used. Three main types of responses were received: central/shared storage only, distributed/decentralised exchange only, and ones that would use both. From the seven respondents three used a central/shared approach (IEGSA, Platone, SYNERGY), two a distributed/decentralised approach (Estfeed, EUniversal) and the remaining two used both (CoordiNet, ECCo SP). Figure 1 summarises the given answers.

Data access and storage

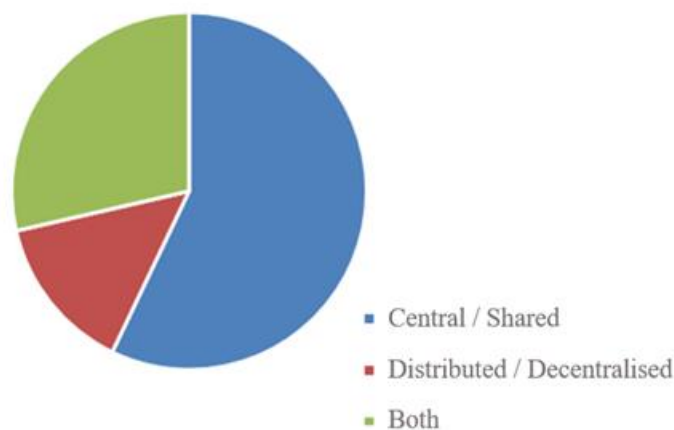


Figure 1: Results from survey on the “Data access and storage” topic

Although some push for a central approach can be noted, with some distributed data exchange platforms, like Estfeed, aiming to transition to a central/shared data exchange only, a clear trend for one approach cannot be inferred, as the number of answers for both are similar and a small sample size is considered. A close monitoring of the success of these platforms and initiatives can later shed some light on what approach becomes dominant in the energy sector.

2.3.1 Flow of data

For this section, the goal was to identify, for each initiative from the respondents, what is their approach to communication, namely if an end-to-end approach, or an end-to-platform, or even both approaches are followed. In case of an end-to-end approach, respondents should specify the entity pairs that exchange information and for the end-to-platform the connected entities to the platform should be provided.

Table 2 summarises the responses, where we see that the most chosen approach is end-to-platform, although some initiatives also consider end-to-end, having ability to guide the user in the entire process.

Table 2: Results from survey on the “Flow of data” topic

Solution/Initiative	End-to-End/End-to-Platform	Actors
CoordiNet	Both	DSO, TSO, FSP, MO, Market Platform, Regional DSO, sFSP, CoordiNet Platform
ECCo SP	End-to-Platform	ECP Endpoint, EDX toolbox
IEGSA	End-to-Platform	FSP, MO, TSO, DSO, Marketplace, IEGSA
Estfeed	Both	Energy Service Provider, Supplier, SO, Generator, BRP, Charging Station Operator
Platone	End-to-Platform	DSO, Aggregator, TSO, Market Platform
SYNERGY	-	-
EUniversal	End-to-End	DSO, FSP, Flexibility MO

2.3.2 Data portability

For this section, two points were assessed: how the data is being communicated between the interested parties or between them and the platforms/interfaces, and which compatibility and interoperability mechanisms are used in the transactions (standards, data models, data formats, ontologies).

The first question establishes APIs as a common and clear trend in how to communicate and connect, since almost all platforms and initiatives indicated using APIs in their approach to data portability. To reinforce this idea, the solution proposed by EUniversal project aims to deploy and implement a set of APIs for the procurement of market-based flexibility. The second most common approach, indicated by three of the seven respondents (CoordiNet, IEGSA, Estfeed), is using traditional UI (User Interfaces). A final remark for an outlier can be made for a Message Brokering technology with Apache Kafka being used in the Platone project.

This high utilisation of APIs from the analysed initiatives goes hand in hand with the recommendations stated previously, clearly pointing towards the potential use of APIs to achieve interoperability and ensure that the different stakeholders from the Europe can seamlessly connect to each other.

In relation to standards, the focus falls onto the Common Information Model (CIM) as three respondents (CoordiNet, ECCo SP, IEGSA) stated that some standard from CIM was used (IEC 61850, IEC 62325-351), while others developed internal models and practices.

The use of current available standards that are relevant goes accordingly with the vision described in the previous section, while creating new ones can move us backwards as more standards will create more entropy

in an already staked sector with different approaches being adopted throughout the European Member States, that need to harmonise communications between stakeholders in a simple and swift way.

2.3.3 Identification/registration mechanisms of the participants

In this part the goal was to know how user data is handled, considering participant registration and certification. From the inquired platforms where a distributed/decentralised approach was taken (Estfeed, EUniversal), a form of minimum guidelines was proposed for EUniversal. In the case of ECCo SP this responsibility was left open to manage by whoever made the service registration. For the remaining respondents, different procedures were implemented, such as, OAuth, Client Certification, API Keys, Secure Tokens, or a required national economic activity in the case of Estfeed. From this we can conclude that mainly three approaches were taken:

- Open implementation for whoever adopts its technology.
- Usage of well-known security protocols.
- Integration and adaptation of external registries.

2.3.4 Data ownership

For this topic, the main goal was to assess the individual data usage policies that data owners can use to exert their rights over the data they provide. Different approaches were taken by the respondents, with a role-based access control (RBAC) and attribute-based access control (ABAC) being used in two (CoordiNet, IEGSA) and one (SYNERGY) initiatives, respectively. Two of the respondents haven't defined an approach for controlling the access to the data, with Platone indicating that this approach was not yet defined and EUniversal mentioning that this concern goes out of scope as it consists of a distributed communication mechanism with each party making sure that the right procedures are followed. Consent-based access is granted by Estfeed to any legal or natural person. ECCo SP requests during registration the acceptance of GDPR rules to data access.

The initiatives recommended individuals to give, deny, or revoke consent to share their data, thus any mechanism for access control or others with the same intent of limiting information availability to others based on preferences established by the data owner are well received.

2.3.5 Consent management

For this category three main themes were assessed: portability of consents (sharing consents between countries), the reutilisation of data, and representation rights. The respondent from Platone stated that no consent management was implemented as of this moment and EUniversal, due to its distributed approach, marked this subject as not applicable. For ECCo SP, all consent management is conducted by the TSOs.

From the remaining four respondents, three indicated to have some kind of portability tool implemented, with Estfeed implementing a form of whitelist for suppliers but requiring an Estonian ID for other stakeholders, CoordiNet being dependent on RBAC, IEGSA implementing Estfeed's datahub consents, and SYNERGY stated that to their platform this was not applicable.

For data reutilisation, Estfeed highlighted concerns regarding implementation since the "reuse of private data seems to be complicated". SYNERGY considered this in the data sharing contracts signed for data sharing through the marketplace. The remaining two used some form of reutilisation either upon resource registration (IEGSA) or dependent on the roles attributed to the users (RBAC, CoordiNet).

Lastly, for matters concerning representational rights two answers stated that this was not applicable for solution (SYNERGY). As for the remaining two, representational rights can be given to Estonian residents in case of Estfeed and in IEGSA the legitimacy to represent resources was asked to the FSPs.

2.3.6 Logging

As an important step in data traceability, the logging mechanisms were also addressed in the questionnaire. Out of the seven, five respondents had some form of logging mechanism, with mixed approaches in their records extensivity and livelihood.

Regarding the duration of which records were kept, it motivated answers from seven days to indefinitely through a blockchain approach. As for the information stored it ranged from minimum requirements to all the information concerning transactions, with this being divided in three levels:

- Minimum – information on statistics of the system (e.g., number of transactions)
- Medium – information on communications (e.g., from who, to whom, when)
- Maximum – detailed record of communications (e.g., from who, to whom, when, how, what)

2.3.7 Licensing

This section aims to uncover if open-source licenses or closed source are in use by the platforms and initiatives from the seven respondents. A mixed response was given as three respondents stated that they use closed-source licenses (SYNERGY, Estfeed, ECCo SP) and other three use open-source (EUniversal, IEGSA, Platone). The respondents from CoordiNet were not able to provide an answer. Figure 2 summarises the given answers.

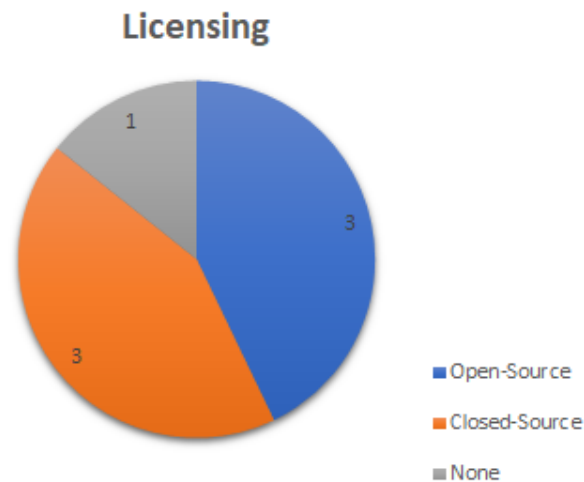


Figure 2: Results from survey on the “Licensing” topic

The recommendations were clear in stating that interoperability would benefit from open-source architectures and data models, therefore, greater efforts in this essential item need to be conducted.

2.3.8 Ownership and maintenance

Ownership and Maintenance responsibility was surveyed at this stage to identify if there is a responsible party for running and maintaining the solution. Three of the respondents answered that there is an entity responsible for Ownership and Maintenance (ECCo SP, Estfeed, Platone) where in one case the maintenance part is subcontracted. For the remaining four, half indicated that this action is still pending decision (SYNERGY, EUniversal) and the two others (CoordiNet, IEGSA) did not provide an answer.

2.3.9 Survey results analysis

Crossing the recommendations summarised in Table 1 with the results from the review of the existing data exchange initiatives, that resulted from a survey addressed to representatives of these initiatives, it is possible to conclude that the main work is being done within the data portability topic, through application and creation of different standards, data models, data formats and ontologies, meaning that there are still several areas to be tackled in future projects, in line with the recommendations from Table 1. In this topic, there is a clear inclination to the adoption of APIs, although solutions like UIs are also highly popular. Regarding standards, the CIM model is highly used, although there are some initiatives developing their own internal models and practices.

Licensing is another topic well regarded both within the recommendations and within the initiatives considered. However, despite the recommendations are pointing more towards the open-source of data models

and data architecture, the approach chosen by the initiatives is split between open-source and closed-source, possibly due to market competition reasons, therefore, greater efforts in this essential item need to be conducted.

Some other important aspects to highlight from the results of the survey to the existing initiatives are regarding the approach to data access and storage, with most initiatives having implemented a central/shared approach. Regarding the flow of data, the most chosen approach is End-to-Platform, although some initiatives also consider End-to-End, having ability to guide the user in the entire process. On data ownership, there is no “winner” approach, being split between RBAC, ABAC, consent-based and request upon registration for acceptance of GDPR rules. As for the identification/registration mechanisms of the participants, several approaches are adopted such as OAuth, Client Certification, API Keys, Secure Tokens, among others. Both portability tools (for consent management) and logging mechanisms are adopted by most of the respondents, and regarding ownership and maintenance, considering those that have the process defined, the majority has an entity responsible for this task.

However, it is important to highlight that these conclusions are related to the sample of seven initiatives that were chosen based on the presence of representatives within the OneNet consortium, therefore, it is not possible to infer any clear trend in each of the topics addressed. Hence, a close monitoring on the success of these initiatives can later shed some light on what approach becomes more dominant in the energy sector.

3 Data governance related to OneNet architecture and middleware

3.1 Analysis of OneNet architecture and requirements (focus on data governance)

The design process of the OneNet architecture and the definition of functional and non-functional requirements followed a hybrid analysis approach between bottom-up, in which the architecture of a software solution is designed starting from the use cases, requirements and specifications collected by the end-users (in this case the demonstration clusters of OneNet) and top-down, in which the objectives already set and the results already consolidated are the main reference.

In addition, this phase was also guided by three main pillars, as main goals to be implemented in the design and implementation of the OneNet solution:

- allows **cross-border participation of stakeholders at all levels**, from TSOs to DSOs, from small consumers to large producers;
- facilitates the **platforms' integration and cooperation for cross-platform market and network operation services**;
- makes **available and accessible data** from different sources (actors) in a **secure and trusted way ensuring data ownership and privacy**.

The result of this analysis is the OneNet Reference Architecture shown in Figure 3.

As reported in the OneNet D5.2 (2021 [46]), the OneNet Reference Architecture consists of three logical layers:

- The bottom layer includes data sources and energy stakeholders, the OneNet participants.
- The middle layer is the one that in the OneNet ecosystem allows the creation of a OneNet Network of Platforms and includes all the platforms that participate in data exchange and the use of cross-platform services. In this layer there is the first component provided by OneNet, the OneNet connector.
- The top layer is the one properly defined as OneNet Framework. This is the core of the OneNet Architecture. It includes all the components that will be implemented in the reference implementation in WP6, as well as all the necessary specifications for data harmonisation, ontologies, data modelling, service orchestration, workflow monitoring, analytics, etc.

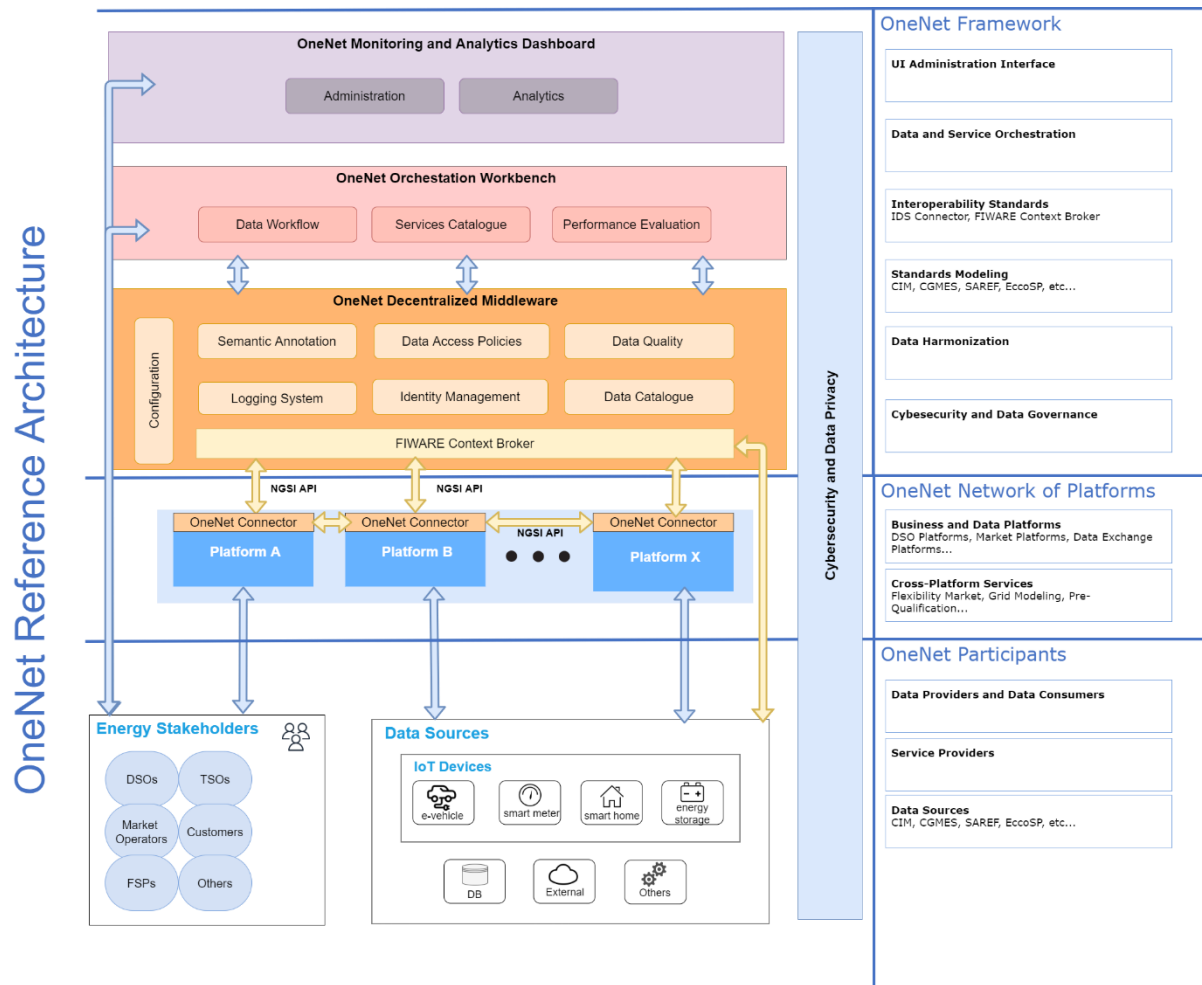


Figure 3: OneNet Reference Architecture (OneNet D5.2, 2021 [47])

It is important to emphasise how much important is the Data Governance aspect in the OneNet system design, since one of the main goals of the solution is to make available and accessible data from different sources (actors) in a secure and trusted way ensuring data ownership and privacy.

For this reason, it is useful to analyse how the OneNet architecture:

- defines the concepts of **data providers and data consumers**;
- implements the concept of **fully decentralised data exchange**;
- ensures the **data ownership and consent management**;
- facilitate the **cross-platform integration in a secure and interoperable way**.

3.1.1 OneNet actors and roles

The main actor of the OneNet ecosystem is the OneNet participant. More in detail, an OneNet participant can be identified as:

- **Data Source** – a more generic source of data that could be integrated within OneNet system. It could be represented by a Data Provider (see below), a single database, an IoT device, a file system etc.
- **Data Provider** – a specific OneNet participant that provides data to the system. To submit metadata to a broker, or exchange data with a Data Consumer, the Data Provider uses software components (OneNet connector) that are compliant with OneNet System.
- **Data Consumer** – receives data from a Data Provider. From a business process perspective, the Data Consumer is the mirror entity of the Data Provider; the activities performed by the Data Consumer are therefore like the activities performed by the Data Provider. Before the connection to a Data Provider can be established, the Data Consumer can search for existing datasets by making an inquiry through the OneNet Connector. The OneNet Connector then provides the required metadata for the Data Consumer to connect to a Data Provider.
- **Service Provider** – a specific OneNet participant that provides (mostly) data services or tools. The Service Provider registers its services in the OneNet Framework to be used, integrated and tested within any cross-platform integration or orchestration process.

3.1.2 OneNet decentralised approach

The main characteristic of the OneNet architecture is its fully decentralised approach, implemented in the OneNet Decentralised Middleware and the OneNet Connector.

The OneNet Decentralised Middleware is used as a layer on top of the common IT infrastructure enabling the exchange of information between all assets and other various components that will be integrated in OneNet Network of Platforms. It also adds further centralised features to the OneNet system, needed for implementing some important features (identity management, data discovery) for supporting the decentralised data exchange approach. In addition, the OneNet Decentralised Middleware enables the connection of the OneNet Network of Platforms to the OneNet Dashboard and Orchestration Workbench.

The OneNet Connector is a specific instance of the OneNet Decentralised Middleware, deployed in each OneNet participant IT environment allowing an easy integration and cooperation among the platforms, maintaining the data ownership, and preserving access to the data sources. The OneNet Connector is essential for connecting and integrating a platform within the OneNet ecosystem.

The OneNet Connector is completely developed following a decentralised approach, ensuring the necessary scalability for the near real-time data integration and management enabling multi-country and multi-stakeholder near real-time decision-making services.

In such an infrastructure, two entities can interact directly with each other, without intermediation by a third party. Figure 4 presents the concept of OneNet fully decentralised architecture, where the OneNet Connector opens a channel to an interoperable network for Data Providers and Data Consumers.

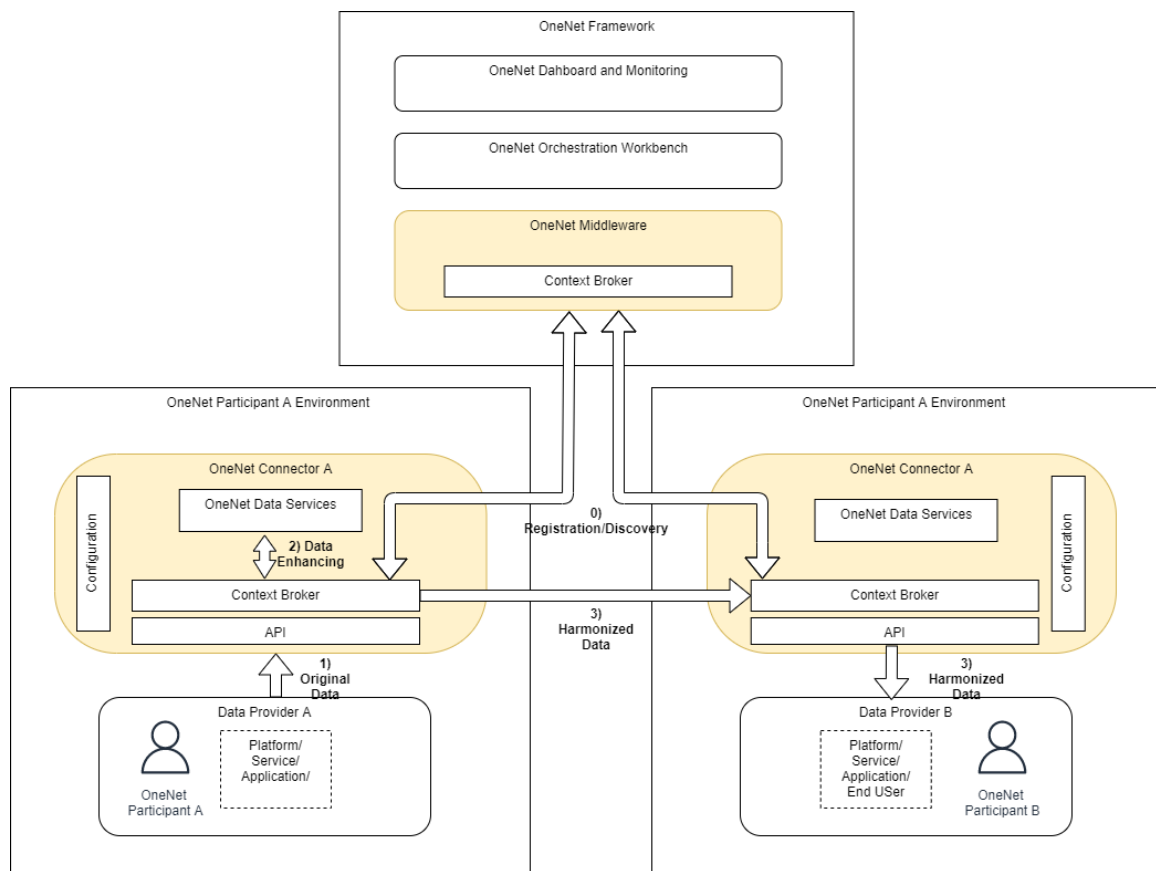


Figure 4: OneNet Decentralised Approach (OneNet D5.2, 2021 [47])

3.1.3 OneNet and IDS

The OneNet solution bases its main implementation (the OneNet Connector) on the International Data Space (IDS) concept of Data Space and in particular on its Reference Architecture Model (RAM) (Otto et al., 2019 [52]) and the definition of trusted data exchange.

The alignment of the OneNet project with IDS is obviously useful for interoperability and connectivity between various participants as a focus. At the same time the IDS reference model architecture has a strong focus in data security, governance, and trust. For this reason, the IDS model and components are working parts in the OneNet architecture, specifically the Data Management Interface, where the IDS connector - the central technical component of IDS, and other components such as the broker service, clearing house and app provider are envisioned to be part of.

IDS model also defines the roles of the participants in the data space in the IDS Data Governance Model (IDSA, 2022 [39]), which outlines a decision-making framework regarding the definition, creation, processing, and use of data for the participants. The concept of Data Governance Model in the OneNet definition is strictly aligned with the IDS one.

The following concepts of IDS are also considered in the OneNet Architecture (Ahle et al., 2022 [1]):

- **Data interoperability.** Data Spaces should provide a framework for an efficient data exchange among data space participants, supporting decoupling of data providers and consumers. This requires the adoption of a common language between users, the adoption of standardised interfaces (e.g., APIs), and the definition of common data models. Furthermore, mechanisms for traceability and logging of data exchange transactions and data provenance, are also required.
- **Data sovereignty and trust.** Data Spaces should verify that participants in a Data Space can trust each other and control the sovereignty of their own data. This requires the adoption of standards identity management, the verification of their truthfulness and the enforcement of policies agreed upon data access and usage control.
- **Data value creation.** Data Spaces should provide support for the creation of data markets where participants can generate value out of sharing data (i.e., creating data value chains). This requires the adoption of common mechanisms enabling the definition of terms and conditions (including pricing) for the usage and sharing of the data offering, the publication and discovery of such offerings and the management of all the necessary steps supporting the permission to access and use data.

3.2 Analysis of other OneNet results related to Data Governance

In the context of OneNet system design, other aspects are strictly related to the data governance such as Data Quality, Data (Quality) Standards, Data Access Management and Data Security.

3.2.1 Data quality

In the context of OneNet, the Data quality assessment takes on even more importance, as data exchange is the core of the system. The data quality assessment is the process of finding and exposing all the business and technical issues related to data so that data cleansing and data enrichment processes can be executed across the organisational data using appropriate data quality tools. This process ensures a high data quality level and is maintained for each operation related to the data.

To achieve good data quality, it is necessary to determine, in a structured way, exactly what ‘good data’ means to them, as well as finding a way to ensure that the quality of the data remains ‘good’. In order to make this, OneNet defines a Data Quality Framework and a set of Data Quality Requirements.

The OneNet Data Quality Framework is a 5-steps process for ensuring the data quality management. More in detail, it consists of:

1. Definition of the Scope
2. Data Exploration and Profiling
3. Data quality assessment

4. Data quality improvement
5. Monitoring and control

The OneNet data quality assessment also provided a list of data quality requirements, leveraging on the Data Quality Dimensions defined by ISO 25012 standard (ISO2500, 2022 [41]):

- Accuracy
- Completeness
- Consistency
- Credibility
- Currentness
- Accessibility
- Compliance
- Confidentiality
- Efficiency
- Precision
- Traceability
- Understandability
- Availability
- Portability
- Recoverability

In OneNet D5.3 (2021 [48]) the OneNet Data Quality Framework is described more in detail and the mapping between these data quality dimensions and the Business Objects of the OneNet cross-platform services is reported.

3.2.2 Data quality standards

Data quality standards define the overall approach for ensuring conformance to the data policy. Examples of data quality standards include data modelling standards, naming and abbreviation standards, metadata management, etc.

OneNet followed an important process for the harmonisation of the data processing. As described in OneNet D5.3 (2021 [48]), the process started with the definition of 10 categories of cross-platform services for the categorisation and identification of a list of services to be enabled and supported in a harmonised way by the OneNet system.

Table 3 reports the description of the 10 categories and the number of services identified.

Table 3: OneNet cross-platform services categories (OneNet D5.3, 2021 [48])

No	Category Name	Description
1	Authentication & Authorisation	Activities related to cross-platform authentication and authorisation. This category is different from the other categories of cross-platform services, since it specifies cross-domain services for authentication and data access policies.
2	Measurements & Monitoring	Exchanging measurements or other data related to monitoring, e.g., state estimation results
3	Forecasts	Exchanging forecast of any kind
4	Reports & invoices	Activities related to reporting or invoicing of system or other services, incl. reporting energy/flexibility settlement
5	(Flexibility) Market participation	Activities related to participation in market, e.g., sending bids, market clearing etc.
6	Grid models	Exchange of grid models, for example for grid reconfiguration
7	Simulation results	Exchange of simulation results, for example power flow results
8	Resource (pre-) qualification	Activities related to the (pre-) qualification of resources, incl. qualification of product's/ service's technical parameters
9	System service activation	Asking system operator to activate/ start certain system service
10	Resource control	Sending set points to assets/ flexibility sources etc.

After the identification of the harmonised cross-platform services (namely a specific service that involve two or more platforms exchanging data for satisfying business processes), for each of them the following characteristics were defined:

- **Unique ID** with textual description
- **Method** of the data process (GET data or POST data)
- **Actors involved** (Data Providers and Consumers as mapped to the roles in Harmonised Electricity Market Role Model)
- **Business Objects** exchanged
- **Data quality Requirements**
- **Data format and standard data models**

All these results are included in the OneNet implementation and in particular in the OneNet Middleware and in the OneNet Connector for supporting a standardised data exchange, including standard data models (based on CIM – Common Information Model) and semantic validation.

3.2.3 Data Access Management

The OneNet system implements a well-structured management of access control and use of data, during any data exchange, that extend the classic data access control, which therefore only provides control on the data access by the consumers, based on Role-Based Access Control (RBAC), or on Attribute-Based Access Control (ABAC), with IDS concept of Data Usage Control (IDSA, 2021 [38]).

Data usage control is an extension to traditional data access control. It is about the specification and enforcement of restrictions regulating what must (not) happen to data. Thus, usage control is concerned with requirements that pertain to data processing (obligations), rather than data access (provisions). Usage control is relevant in the context of intellectual property protection, compliance with regulations, and digital rights management.

In addition to data access control, where only the access to specific resources is managed, the IDS architecture supports data-centric usage control. In general, the overall goal is to enforce usage restrictions for data after access has been granted. Therefore, the purpose of usage control is to bind policies to data being exchanged and to continuously control the way how messages may be processed, aggregated, or forwarded to other endpoints.

OneNet system considers as crucial the roles of the Data Provider and the Data Consumer. In OneNet data access management, Data Providers can define access and usage policies based on the classes suggested by the IDS reference model and these policies can include both the access and usage control.

From the technological point of view, as shown in Figure 5 the OneNet Data Access Policies (DAP) Framework, following the IDS reference model, includes a specific Usage Control (UC) App within the OneNet Connector and therefore available to every OneNet participant. This ensures that every platform connected to the OneNet system uses the UC App and that the policies defined by the data provider are applied to every data exchange.

The UC App included within the OneNet Connector gives the possibility to create at least a series of policies defined as basic for the project and for the various demonstrators and use cases and is extensible with new policies and new classes.

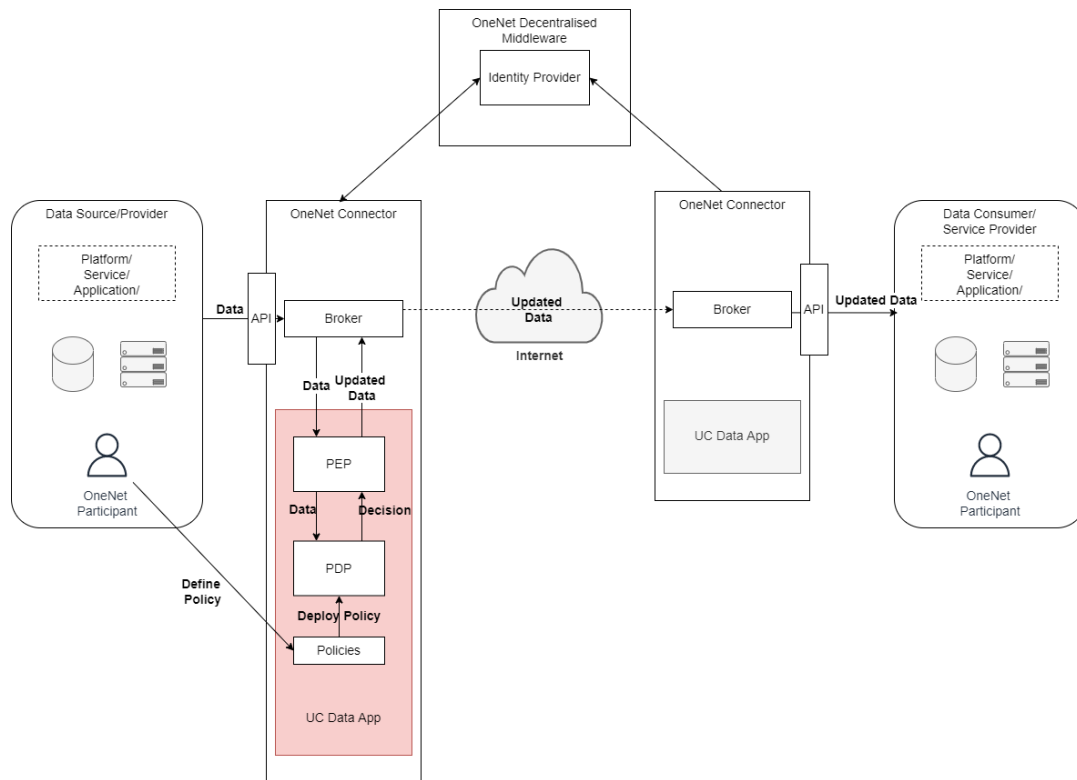


Figure 5: OneNet Data Access Policy Framework (OneNet D5.7, 2022 [49])

3.2.4 Data Security

Data security refers to safeguarding data throughout its lifecycle. Data security should implement the process for ensuring data is safe from cyber-attacks, unauthorised access, data breaches, and theft. It should also establish a clear plan of action to respond to all potential threats.

The OneNet system takes into high considerations both the data security aspects (relating to the protection of data in terms of confidentiality, integrity and availability) and cybersecurity aspects (relating to the protection of the systems and networks infrastructure), although they overlap in many instances. More details in the technical implementation aspects are provided in Chapter 3.3.

In particular relevant standards, principles, regulatory frameworks, and best practices in EU and globally in terms of power industry (smart grids) and related cybersecurity requirements were identified and assessed. These include requirements for power system management, industrial automation and control systems' security, information security management and cybersecurity (both in terms of smart grids and considering the proposed OneNet architecture).

Due to the nature of smart grid network which connects critical energy infrastructure components with consumer facing technology and services, the privacy principles of GDPR⁵ should be seen as the guiding principles of regulation on compliant processing, especially so when dealing with customer data and other personally identifiable information. Also, data controller obligations and data subject's rights in terms of GDPR must be considered. From ethics perspective, collection and processing of personal data should be non-invasive.

As described in OneNet D5.8 (2021 [50]), it becomes of fundamental importance to follow the specifications provided by the EU in the Data 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).

From a technical and implementation point of view, OneNet system provides specially tailored cybersecurity requirements, specific components for the management of cybersecurity aspects and a testing environment in order to test new services (and platform integration) before their production rollout.

3.3 OneNet Data Governance Framework

As described in sub-chapter 3.2, the OneNet solution addresses many aspects of the data governance, both from the point of view of processes as well as technologies. All these aspects should be linked and actuated for implementing a data governance programme in the OneNet ecosystem. This data governance programme could be executed defining a Data Governance Framework.

A Data Governance Framework creates a set of rules and processes for collecting, storing, and using data. By doing so, the framework makes it easier to streamline and scale core governance processes, enabling to maintain all the important aspects related to data processing: data quality; data ownership and access; quality of IT platform used for data processing.

In order to define a consistent OneNet Data Governance Framework, it's important to rely on 5 dimensions:

- Structure – defines how data will be organised, retrieved, and stored
- Access – defines how the data can be accessed, the policy and the security
- Usage – establishes parameters and restrictions on use of the data
- Standardisation – ensures conformance of the data, as well as the portability, reusability, and interoperability
- Integrity – establishes characteristics to ensure the quality of the data (accuracy, validity, and reliability)

⁵ https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr_en

Structure

The definition of specific roles for data provisioning and consuming allows to implement end-to-end processes for the data exchange. OneNet's decentralised approach ensures that all the data exchanged during the platform integration and cross-platform services execution are stored in the OneNet participants' environments. The fully decentralised ecosystem implemented using the OneNet Middleware and the OneNet Connector allows to define data exchange processes using only metadata that are stored in the central environment of the middleware, while the real data exchanged is never passed outside the end-to-end communication between two OneNet participants. In addition, the categorisation of cross-platform services supports the data structuring, standardisation, portability, and interoperability.

Access

The OneNet participants can act as Data Providers and/or Data Consumers and define their own access policies for any kind of data exchange. The identification of the OneNet participants is completely ensured by the Identity Manager included in the OneNet Middleware, creating a trusted data space where the OneNet participants can cooperate with each other. A specific security layer is included for ensuring authentication and authorisation for participating in the OneNet ecosystem.

Usage

OneNet extends the standard access management (based on roles or specific authorisations) with the IDS concept of usage control, that allows the specification and enforcement of restrictions regulating what must (not) happen to data). Usage control is relevant in the context of intellectual property protection, compliance with regulations, and digital rights management. The usage control, together with the access management, is implemented in automatic way at OneNet Connector level in a specific application: the Usage Control App is concerned with requirements that pertain to data processing (usage), rather than data access (provisioning).

Standardisation

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.

Integrity

All the data exchanged through the OneNet Connector are formatted and processed using FIWARE Context Broker and NGSI-LD standard, ensuring the possibility to verify the correctness and quality of the data in a standardised way, as well as adding the possibility to implement specific semantic tool, thanks to the implementation of Linked Data and NGSI ontologies.

Figure 6 and Figure 7 respectively represent how OneNet Data Governance Framework is applied to the OneNet system and how the implementation side exploiting the decentralised approach.

The Cybersecurity Layer plays a key role in both the central communication with the OneNet Middleware and the end-to-end data exchange among OneNet Connectors. It implements several 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.

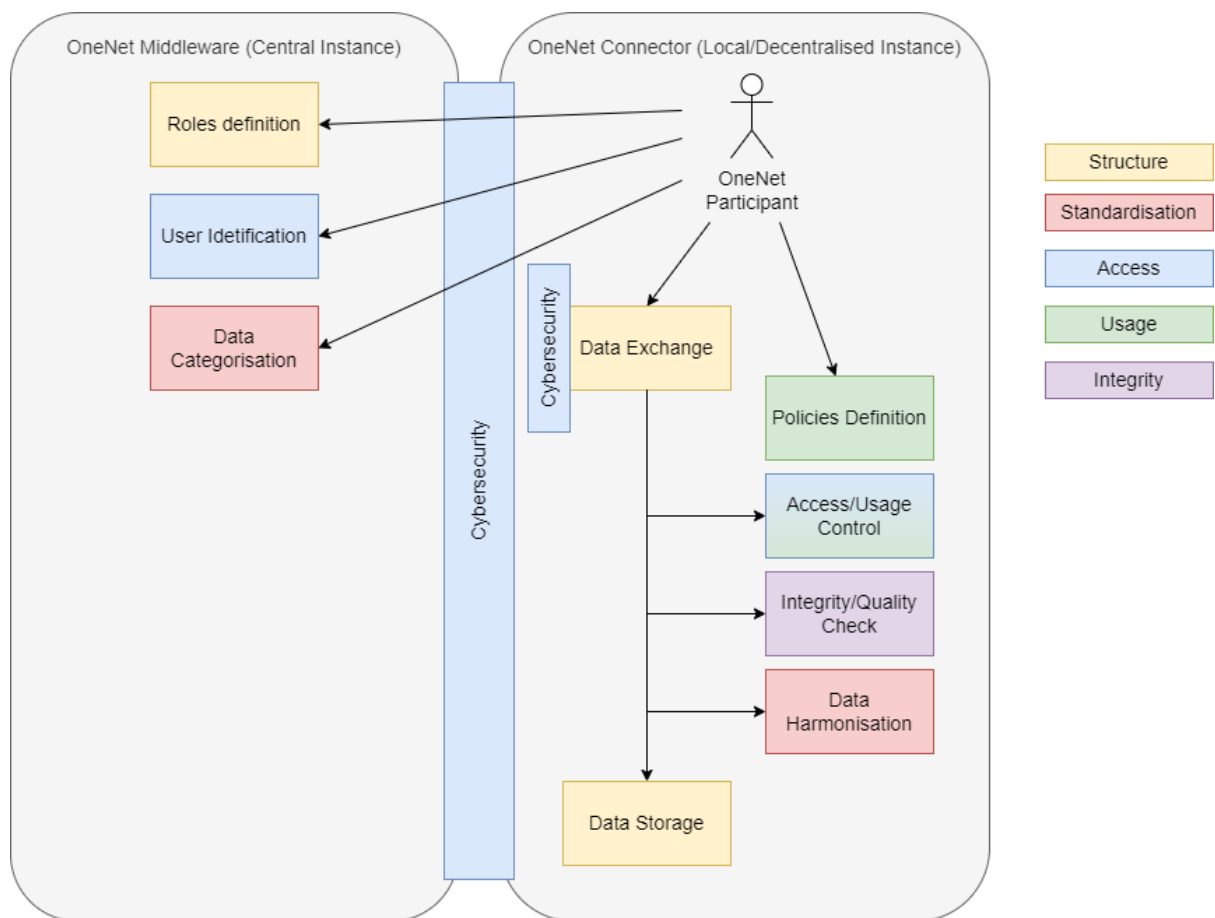


Figure 6: Application of the OneNet Data Governance Framework

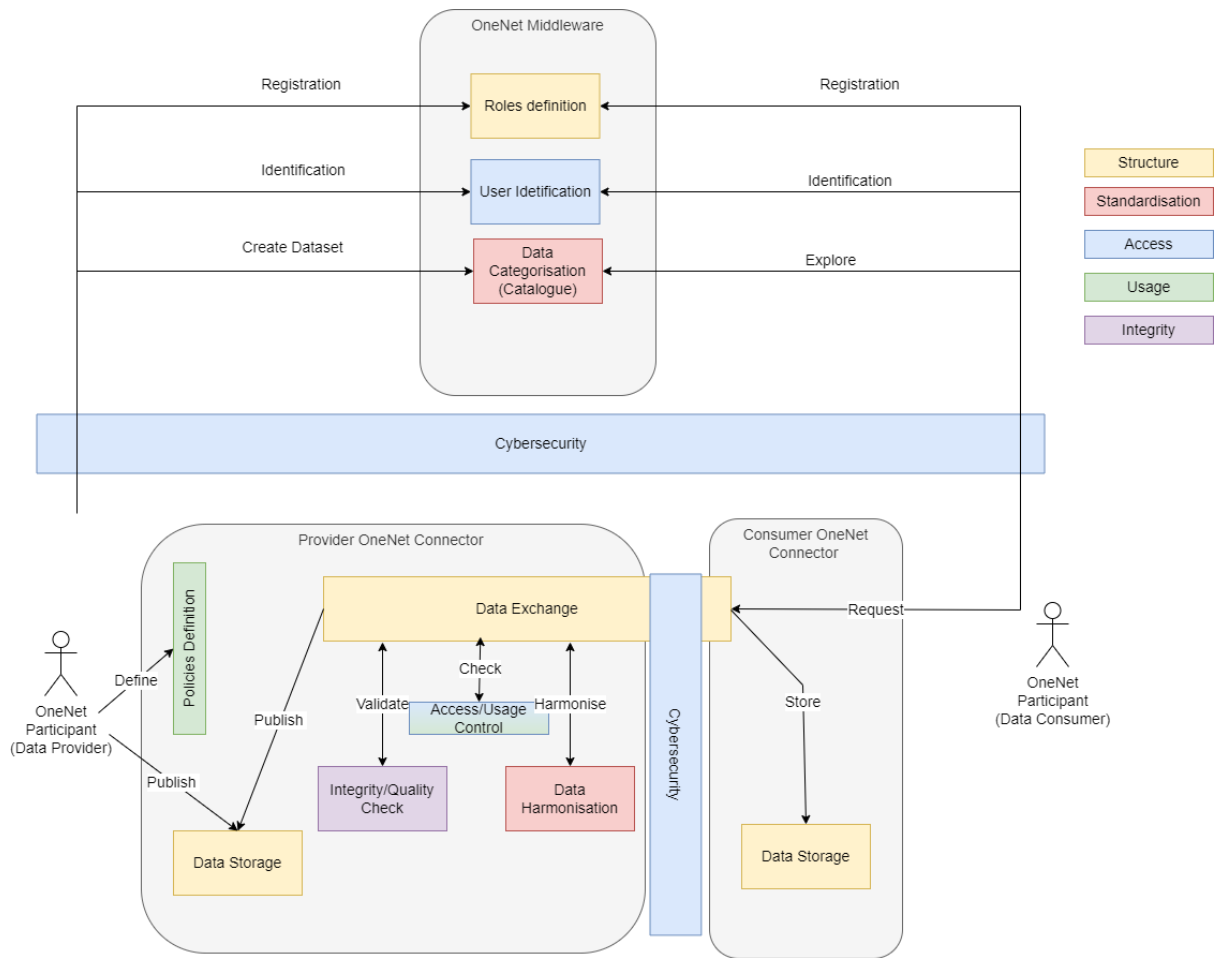


Figure 7: Implementation of the data exchange process using the OneNet Data Governance Framework

4 Reference Data Governance Model

4.1 Definition and scoping of data governance model

One can still often wonder why the (energy) data does not flow seamlessly across country borders and across sectors. This concerns specifically the ability to access and share the data which is generated and owned by end-customers: “My Data”. Why can I not easily access My Data (meter data, sub-meter data, market data), including access to My Data in other countries? Why are there no single data access points for different types of data from different sources? Why are there no convenient possibilities to provide My Data to any party across Europe, incl. across sectors?

There are definitely many useful elements existing already and being developed for cross-border and cross-sector data exchange, however, a lot still needs to be done (Figure 8). A reference to a well-defined data governance framework could contribute to overcoming the remaining barriers. This Chapter elaborates and proposes a Reference Data Governance Model (RDGM) consisting of governance requirements on different data interoperability layers.

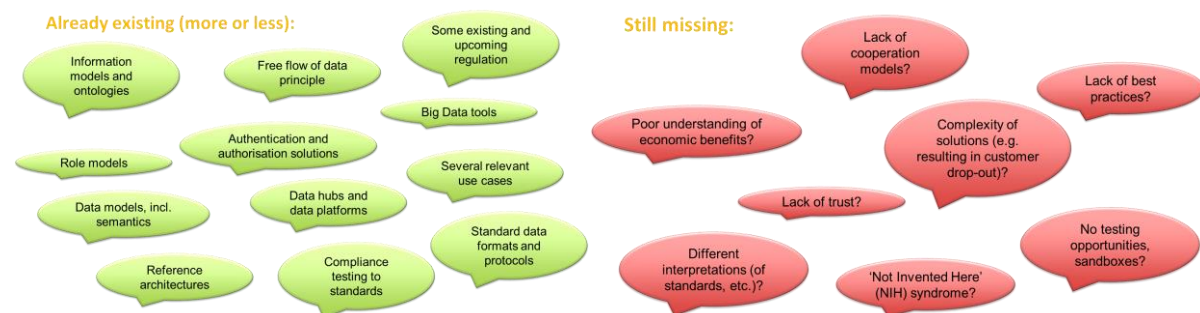


Figure 8: Some already existing and still missing elements for smooth European data exchange

The BRIDGE Initiative (2022 [9]) has proposed a sector-agnostic cross-border Data Exchange Reference Architecture – DERA2.0. Based on the input of many Horizon2020 projects, DERA describes the data exchange elements related to all five SGAM interoperability layers – Business, Function, Information, Communication and Component (Figure 9). These elements are certainly relevant for electricity sector – because proposed by electricity projects – but only the ones were picked which are reusable in other sectors. This includes other energy sectors like gas and heat as well as beyond-energy sectors like mobility, water, health, etc.

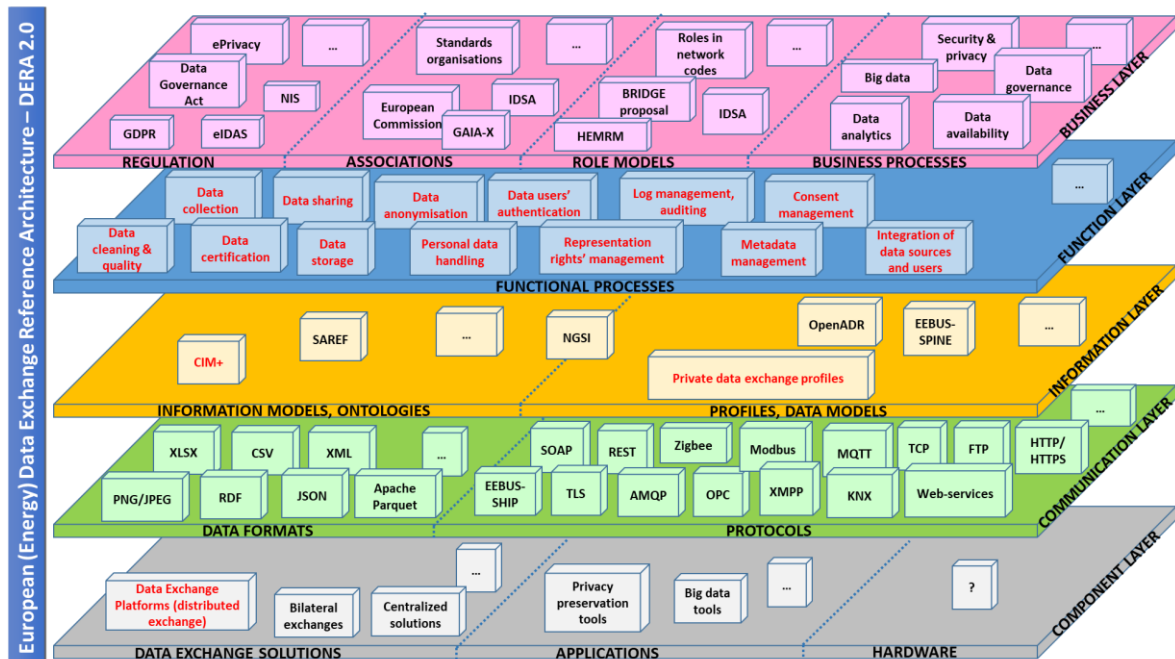


Figure 9: BRIDGE data exchange reference architecture DERA2.0 (BRIDGE, 2022 [9])

The aim of DERA is to support cross-sector data interoperability. It describes what needs to be implemented in moving towards this aim. It also gives some recommendations about how to make the implementation happen. However, this deliverable attempts to make a step forward being more specific about the commonly agreed and to be taken administrative actions on European level to support the actualisation of Common Energy Data Space, and eventually the interoperability of sectoral data spaces.

Such ‘administrative actions’ are the building blocks of data governance. Two levels of ‘building blocks’ are defined hereby, largely based on relevant literature review and OneNet project findings. First, ten higher-level data governance elements are clustered according to SGAM interoperability layers (Table 4). Secondly, each element includes one or more specific governance requirements. These requirements are visualised in Figure 10 and explained in detail in next section.

Table 4: Data exchange governance elements per SGAM interoperability layers

Business layer	Function layer	Information and Communication layer	Component layer
1. Data governance business case	4. Data ownership governance	7. Data vocabulary governance	8. Data platforms
2. Orchestrated data governance	5. Data access governance		9. Interfaces
3. Rules and norms	6. Data security governance		10. Repositories

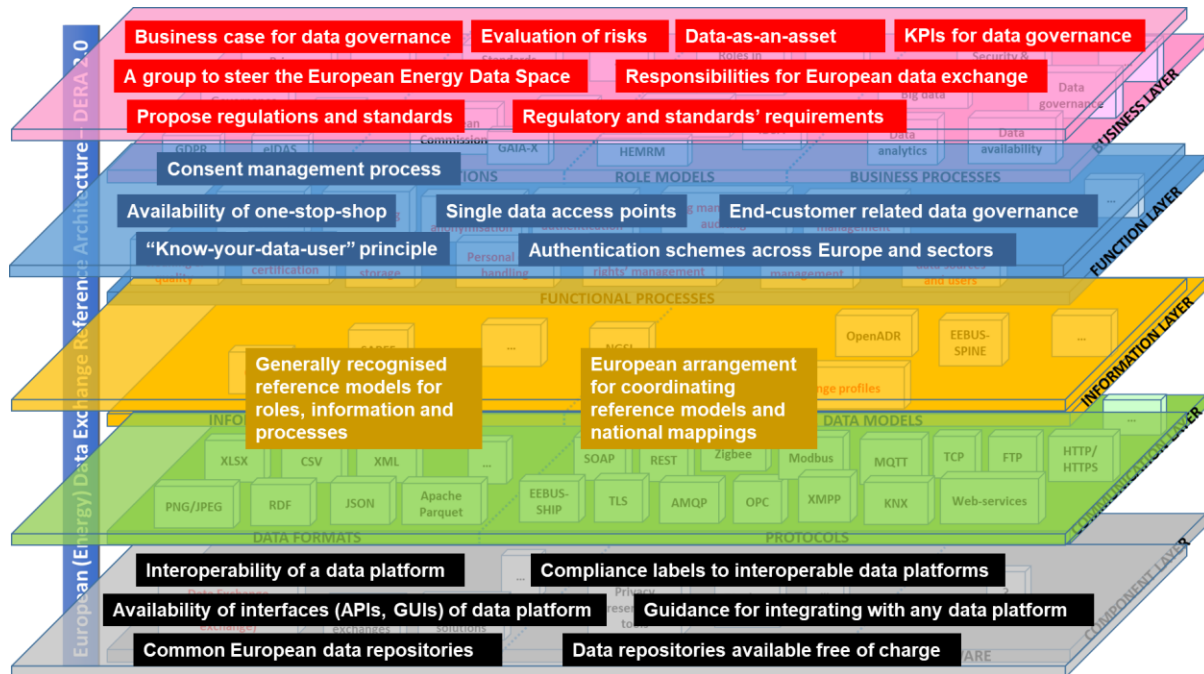


Figure 10: Data governance layers per SGAM interoperability layers

4.2 Elaboration of data governance requirements

4.2.1 Data governance business case

According to John Ladley (2020 [42]), data governance (DG) is a business programme, which means that these are not normally sponsored by IT departments. The DG programme calls for collaboration between the structures inside an organisation and alignment of data programmes with organisation's objectives (Cheong and Chang, 2007 [11]). As with any other business activity, it should have its own business case and should be in line with organisation's strategy. Henderson (2017 [34]) distinguishes between strategy (related to general scope of DG efforts and "articulated in relation to the overall business strategy, as well as to data management and IT strategies") and policies (related to "creation, acquisition, integrity, security, quality, and use of data and information").

The data governance framework aims at better decision-making, transparent and standardised processes, efficiency, training management and employees (Thomas [61]). The data governance framework is about standards, policies and processes, organisational structure and technology infrastructure (Panian, 2010 [53]).

The Data Governance business case should address the financial and/or socioeconomic profitability (e.g., by using the business model canvas type approach) as well as process description, including objectives, actors, KPIs,

data description, requirements (e.g., by using the IEC 62559-2 standard template for use cases). While this can be quite graspable on project or organisation level, it is definitely not easy for European wide cross-border and cross-sector data exchange for different types of data (“multi-multi-multi” data exchange). However, it would serve moving toward European Data Spaces.

A data governance strategy defines the scope and approach to governance efforts. DG strategy should be defined comprehensively and articulated in relation to the overall business strategy, as well as to data management and IT strategies. It should be implemented iteratively as the pieces are developed and approved.

Risk management should be inherent part of data governance. Likelihoods and impacts of risks should be evaluated regularly using risk assessment methodologies. As such it is not different nor distinct from the overall risk management of an organisation. Risks relate to the personnel responsible for preparing and implementing the governance programme, to the available technical capabilities, to the financial resources, to the communication plan, to the external environment, etc. “Appropriate due diligence will be conducted to ensure data complies with all applicable statutes and regulations.” Ladley (2020 [42])

Effective data management is the precondition for good data quality – “accuracy, timeliness, relevance, completeness, trustworthiness and contextual definition” (Cheong and Chang, 2007 [11]). Ladley (2020 [42]) designed a set of principles based on Generally Accepted Accounting Principles (GAAP) and called these GAIP™ (Generally Accepted Information Principles). GAIP™ identifies nine principles:

- data is **assets** like any other assets of organisation and therefore should be managed similarly;
- data has **real value** for the organisation;
- data is critical to the continuation of organisation’s activities – **going concern**;
- the **risks** associated with data must be accounted as a liability or costs to manage these risks;
- risks must be reported and confirmed – **due diligence**;
- the **quality** of data is relevant for the financial capability of the organisation;
- **independent audits** are required for the accuracy of data;
- **accountability** for data of the involved parties of the organisation needs to be set;
- parties have **financial liability** for regulatory and ethical misuse of data.

“Over time, your DG programme will need to evolve a means to monitor its own effectiveness.” (Ladley, 2020 [42]). Key Performance Indicators (KPIs) used for monitoring could be grouped into two categories. First, KPIs of a DG programme should address its cost-efficiency, impact on main business, environmental sustainability. Second, KPIs of specific data exchanges include the easy access to data, shareability and portability, data quality, interoperability, the value resulting from data, respect for privacy.

Cheong and Chang (2007 [11]), based on their literature review, also point on the need to use metrics for measuring data governance success as well as the need to regularly assess policies and procedures, so they are followed. According to Henderson (2017 [34]), for demonstrating the movement towards desired changes and

objectives and for discovering the effectiveness of DG programme “it is important to measure progress of the rollout of data governance, compliance with the data governance requirements, and the value data governance is bringing to the organisation”.

KPIs contribute to implementing and monitoring the DG programme as whole and individual components of it. There are even suggestions that more focus should be put on implementation and monitoring of data governance instead of defining what the governance should be about (Alhassan et al., 2016 [3]).

- Define **business case** for data governance on relevant level [project / organisation / country / EU], e.g., by means of business model canvas or standardised IEC 62559-2 template.
- Evaluate regularly the risks associated to the implementation of data governance programme using **risk assessment** methodologies.
- Define and follow the **principles of data-as-an-asset**.
- Define and monitor **KPIs** for data governance programme itself and for specific data exchanges.

4.2.2 Orchestrated data governance

The main factor for European wide governance for (energy) data exchange is about coordination and cooperation – the orchestration. Data interoperability between Member States as well as inside the countries to support seamless exchange of data between data owners, data providers and data users requires a lot of consistency – either through centralised institutions or close coordination between national organisations.

The European Interoperability Framework (EC, 2017 [24]) notices the need for collaboration based on public sector’s data: “... efforts to digitise the public sector should be well coordinated at European and national levels to avoid digital fragmentation of services and data, and help the EU’s digital single market to work smoothly.” Relating to engagement with interoperability in mind, some specific European level proposals should be quoted:

- “On the way to interoperability of national practices for accessing and exchanging data, all relevant stakeholders must get involved, discuss and negotiate.” (EU SGTF EG1, 2019 [30]; 2022 [31])
- “Ensure cooperation between appropriate associations, countries and sector representatives to work on cross-sector and cross-border data management by establishing European data cooperation agency.” (BRIDGE, 2022 [9])
- “Support the establishment of sector-specific and cross-sectoral communities that aim to create open information specifications and encourage relevant communities to share their results on national and European platforms.” (EC, 2017 [24])

Most recently, the European Commission has proposed in its communication on Digitalising the energy system - EU action plan (DESAP) to establish a working group called Data for Energy including Member States

and stakeholders, in coordination with European Data Innovation Board⁶ and to be supported by the Data Spaces Support Centre⁷, in order to coordinate between existing data exchange initiatives as well as to develop and implement the common European energy data space (EC, COM(2022)552 [27]).

For some authors like Alhassan et al. (2016 [3]), data governance starts from actions related to roles and responsibilities. For a proper DG programme, the responsibilities of involved parties should be clear and accepted, enabling motivation and engagement. This includes vertical responsibilities – from experts to leaders inside the organisation –, and horizontal responsibilities – the organisation itself and its cooperation partners, suppliers, customers, etc. “[...] get leadership engaged and ensure the approach maintains the engagement.” (Ladley, 2020 [42])

Cheong and Chang (2007 [11]) with references to Thomas (2006 [62]) and other authors stress the accountability based on executive leadership to drive DG, clear definitions of the roles and responsibilities of people involved in DG, requirements towards partner organisations for sharing data with them.

According to Henderson (2017 [34]), DG programmes even need organisations to change their cultures by communicating “the benefits of improved data governance and the behaviours necessary to successfully manage data as an asset” because “even with the best data strategy, data governance and data management plans will not succeed unless the organisation accepts and manages change”.

- Establish a **group to steer** the European Energy Data Space, open to European initiatives and stakeholders to participate, and ultimately leading to cooperation between energy and other sectors.
- Define the **responsibilities and accountability** for European data exchange, including European Commission, Member states, data providers, data users, etc.

4.2.3 Rules and norms

Coordinated data governance assumes rules and norms: regulations and standards. The regulation should require governments, municipalities, utilities, monopolies to open up the data; make available information where and how to access data; avoid heavy registration and certification schemes (e.g., for data users).

Often setting up the data governance itself is driven by regulatory requirements, whereas it contributes to monitoring and ensuring regulatory compliance within the organisation (Henderson, 2017 [34]). However, the distinction should be made between data-related regulation and data-governance-related regulation. For example, while electricity market directive insists easy access to metering data and GDPR tells to protect

⁶ To be established according to Data Governance Act.

⁷ <https://dssc.eu/>: “Funded by the European Commission as part of the Digital Europe Program, the Data Spaces Support Centre will explore the needs of data space initiatives, define common requirements and establish best practices to accelerate the formation of sovereign data spaces as a key element of digital transformation at all levels.”

personal data (“data-related”), the data interoperability implementing acts will prescribe the data exchange reference models, Member State obligations for handling the data access, etc. (“data-governance-related”) (EU SGTF EG1, 2019 [30]; 2022 [31]). Basically, the first is about “what?” and the other about “how?”.

On European level, network codes are key legal regulations that stipulate the management of different electricity data (grid data, electricity data, real-time data, etc.). From the governance perspective there are many relevant legal acts:

- Data Governance Act
- Regulation on harmonised rules on fair access to and use of data (Data Act) – EC proposal
- Free Flow of Non-Personal Data Regulation
- Digital Markets Act – EC proposal
- General Data Protection Regulation (GDPR)
- ePrivacy Regulation (replacing current ePrivacy Directive)
- Regulation on electronic identification and trust services (eIDAS Regulation)

EU-SysFlex project (D5.1, 2021 [19]) reviewed the European electricity legislation to see if the concept of Data Exchange Platform can be implemented for supporting different data exchanges. BRIDGE Initiative (2022 [9]) suggests establishing a “minimum set of requirements for data spaces and data governance” in order to support “cross-sector exchange of any type of both private data and public data”. Governance aspects should be addressed in data interoperability implementing acts. The European Commission’s Digitalisation of Energy Action Plan (EC, COM(2022)552 [27]) lists several governance components, at least to mention Energy Data Space.

Standards can be enforced in legal acts, or these can be the agreement of the community.

EU SGTF EG1 (2019; 2022) recommends to “adopt and use available European standards as a basis to improve interoperability”. European Interoperability Framework (EC, 2017 [24]) makes recommendations about having clear procedures for selecting and evaluating relevant standards and specifications as well as monitoring their implementation. EU-SysFlex project (D5.5, 2021 [20]) concludes that while the standardisation is the responsibility of standardisation organisations, “the research and innovation projects like EU-SysFlex can contribute to ‘pre-standardisation’ activities”. BRIDGE (2021 [8]) proposes the 4-steps approach for collecting from projects information about usage and gaps in CIM standards (providing structured information about applied business objects and CIM profiles; synthesis of business objects and CIM profiles provided by individual projects; management of an UML repository for business objects and CIM profile; and management of a repository of instance files).

- Propose and promote **regulations and standards** facilitating improved data governance.
 - Understand regulatory and standards’ **requirements** driving the need for proper data governance.

4.2.4 Data ownership governance

Stemming from the data ownership principle, consent management needs to be a central feature of data platforms. Granting of consent by the data owner and requesting of consent by the data user should be equally seamless as the data exchange itself. The processes related to consent granting and revocation should be clear, in line with regulatory requirements, controllable by data owners (SmartEn, 2021 [58]; mydata.org [43]; ASSET Project, 2020 [4]). Consumers should be always informed about the usage of their data (SmartEn, 2021 [58]).

But while the content of the data is more of a concern for the participants exchanging the data, the consent management requires stronger regulatory oversight. It should be standardised or at least similar across Europe in order to avoid learning different practices. There must be privacy policies in place which the individuals can understand (mydata.org [43]).

As an example, the Australian Competition and Consumer Commission has established the Consumer Data Right package of regulations and standards, including for energy data [5]. This allows energy consumers to request its supplier and based on consent to share consumption data with trusted service providers. Similar examples in Europe include Elering's Estfeed and Energinet's DataHub.

- Ensure **consent management process** which is accessible to any party willing to provide or use any data and not limited to single country.

4.2.5 Data access governance

Easy data access is about once-only principle – one-stop-shops for general information and single data access points need to be available. Data owners, data providers, data intermediaries and data users should not be bothered with multiple integrations, very often using different data standards and policies. This principle should include cross-border and cross-sector data access. It concerns private and public (open) data.

In order for a national government's data to be open, it has to be made public in a way that satisfies several principles: complete, primary, timely, accessible, machine processable, non-discriminatory, non-proprietary, licence free, online & free, permanent, trusted, presumption of openness, documented, safe to open, designed with public input (opengovdata.org [51]). User-centric digital services should be available online, accessible, simple, clear, secure and fair (Tallinn Declaration on e-Government, 2017 [59]).

The European Interoperability Framework (EC, 2017 [24]) recommends providing a single access point for European public services "in order to hide internal administrative complexity", to ask users of public services "once-only and relevant-only information", and to "communicate clearly the right to access and reuse open data". The Data Governance Act (Regulation (EU) 2022/868 [55]) requires public sector bodies to make available certain personal and sensitive non-personal data for re-use and requires Member States to facilitate single information points and data intermediation services. Most of the personal data is still subject of GDPR.

The draft data interoperability implementing act requires Member States to make easily available the information about the roles and data involved in metering data exchange to final customers and eligible parties (EU SGTF EG1, 2022 [31]). Future implementing acts will add further data types.

It could be the national regulator who provides a website or even the EC to providing a European website where information about “the role models, data formats and all standard as well as non-standard procedures for processes” of national practices would be published (ASSET Project, 2020 [4]).

While data access is important for any type of data, the sub-meter data discussion is considerably emerging in energy domain. Sub-meter data is increasingly needed for business processes (flexibility service provision, system observability), but it is also even more sensitive – “going into people’s homes”. More granular and closer to real-time data concerning households and other end-customers implies different approaches to data handling. It requires special attention to privacy and to the capability to manage massive amounts of data.

Governance of sub-meter data should start with proper recognition in the legislation. ENTSO-E and European DSO associations propose in their Roadmap on the Evolution of the Regulatory Framework for Distributed Flexibility (CEDEC et al., 2021 [10]) to include sub-meter data access in data interoperability implementing acts. This would complement the planned Data Act which requires access to data generated by the “products” – i.e., by any device connected to internet (EC, COM(2022)68 [26]).

Access to sub-meter data should be granted to customers (as data owners) themselves but also to aggregators, ESCOs, TSOs, DSOs: “Facilitate the free flow of sub-meter data (based on customer consent) and define the technical requirements for multilateral data exchange, incl. for cross-border data exchange.” (CEDEC et al., 2021 [10]) and SmartEn (2021 [58]) stress the need to “Contemplate relevant energy data from both smart meters and sub-meters, integrating all relevant submetering devices aggregated through Energy Management Systems”.

- Ensure the availability of **one-stop-shop** providing information about and access guidance to different types of data.
- Make available **single data access points** and ensure everyone’s rights to access data.
- Ensure legislative grounds for sub-meter and other **end-customer related data** governance.

4.2.6 Data security governance

When talking data security, it should stem from the *know-your-data-user* principle. Data is delicate in several ways. Any data that is not public is private. Private data can be personal or otherwise sensitive, e.g., for commercial, military reasons. Secure data exchanges between APIs are required.

Standardised/agreed rules are needed for secure data exchanges between participants/endpoints. This can be based on certificates. Data that is provided to third parties needs to be encrypted and transported in secured channels.

Users need identification and authentication (persons, roles, organisations ...). Before one can use any User Interface the user identification and authentication must take place. Identification handled centrally could be useful. On a European scale, the regulation on electronic identification and trust services (eIDAS) guides the implementation on high level.

Role based access for data/service implies accepting only secure requests of authenticated roles. Every data/service responds to authenticated requests only. In case a third party need the access, then the authentication/secure channel needs to be established.

Visualisation and analytical tools for activity logs increase trust among data owners, data providers and data users. Logs should be generated and made available to concerned parties. Logs are generated in multiple levels and reasons – user activity trace logs, technical performance or problem related logs. These can also be used for different purposes (data audit trace, activity audit trace, technical log to tune the system). Log handling can be a standardised process.

Proper security and privacy measures should be applied to the extent which is absolutely necessary. Otherwise, these may become too burdensome and start hindering novel business models and active participation of the consumers (SmartEn, 2021 [58]).

The European Interoperability Framework (EC, 2017 [24]) recommends defining a common security and privacy framework (for data exchange between and with public administrations), to make authoritative sources of information available to others, and to use trust services according to European regulation.

- Apply **“know-your-data-user” principle** by making data usage information available to data owners easily and free of charge.
- Harmonise **authentication schemes** across Europe and sectors.

4.2.7 Data vocabulary governance

The EC recognises in its e-Government Core Vocabularies handbook that “Unfortunately, the environment in which data exchange takes place amongst EU Member States is complex, creating many semantic interoperability conflicts during the execution of European public services.” (EC, 2015 [23]) Regardless of the classification of public services, this statement is definitely valid for energy services and energy data also. Yes, there is the need to focus on cross-border exchanges. And yes, there is the need to talk the same “data language”.

The OPEN DEI project recommends to use ontologies like SAREF as common vocabularies to exchange data between platforms and between different sectors in order to unlock the value of combining data from different sources; “Data models are elementary baseline for B2B data exchange, since the infrastructure of a digital energy system will be built on numerous devices from appliances to electric vehicles, heating systems and heat pump to solar panels from various stakeholders; all these components have to act in concert with another, requiring a common language for data exchange.” (Dognini, et al., 2022 [15])

Data models which are agnostic to different stakeholder needs, business processes, data formats, and communication protocols can be a powerful starting point. “The most common objective of Data Governance programmes is to standardise data definitions across an enterprise.” (Thomas [61]) Hohpe and Woolf (2003 [36]) conclude that while the “Message Translator” may be good in case of couple of application using different data formats, a bigger number of applications can be made interoperable by using the “Canonical Data Model”.

At the same time, the number of available data models should be kept low and rather focus on single or very few “reference models”. Otherwise, the interoperability efforts for models to “understand each other” would outweigh the value of models themselves. Similar to the recommendation to map different data models to the Core Vocabularies “as a common foundational data model allowing to bridge different data models” (EC, 2015 [23]), would be to propose CIM for the energy sector. The latter could be also mapped to Core Vocabularies, or vice versa, in order to ensure cross-sectoral interoperability.

EU-SysFlex project (D5.5, 2021 [20]) introduced the term “CIMification” indicating the benefits of promoting interoperability through CIM, by extending and developing new profiles within energy domain (e.g., for data hubs, sub-metering) and also by entering into cross-sector domain (e.g., consent management) or at least integrating other sectors’ information models with CIM.

Canonical information models, ontologies:

- 1) CIM
- 2) SAREF
- 3) NGSI-LD

According to IDSA (2019 [37]), also in the Governance Perspective of their RAM the vocabulary plays a key role. The European Interoperability Framework (EC, 2017 [24]) recommends using common vocabularies for metadata. Recommendations by EU SGTF EG1 (2019; 2022) recognise the need to adopt and use a common European role model, common information model for semantics (for example, CIM) and core process model as well as to monitor the gaps between these reference models and national practices, preferably at European level.

Building upon and adding to “commonly accepted standards, ontologies, libraries and schemas” can help “to decrease friction in the data flow from data sources to data using services, while eliminating the possibilities of

data lock-in” (mydata.org [43]). Governance is needed for nominating core/reference models, mapping other models to core/reference models, and mapping core/reference models themselves to each other.

- In data modelling, follow the generally recognised **reference models** for roles, information and processes.
- Establish European arrangement for **coordinating reference models** and national mappings.

4.2.8 Data platforms

In an organisation there can be many “messaging systems”, usually not interoperable even if using same standards, which can be confusing for application to integrate with and at the same time to ensure that the “message” is available in all systems – this leaves the challenge to integrate multiple solutions (Hohpe and Woolf, 2003 [36]). While this is so true on the level of an organisation it becomes even more challenging for data exchanges between different organisations, not to mention different countries.

Based on the example of demand side flexibility (DSF) data needs to flow through the variety of IT infrastructure components like Smart Meters, Consumer Energy Management Systems, Smart Appliances and Gateways between the home and external networks, and this should be based on aligned communication standards like SAREF (EC, DNV GL, ESMIG, TNO, 2018 [28]).

The alternative basic option to standardised communication would be to integrate the individual systems into one. And there are solutions in-between, benefitting from standards and from some centralised components. Such hybrid arrangements could be labelled as Data Exchange Platforms (DEPs)⁸ – middlewares⁹ relying on distributed architecture¹⁰ and data federation¹¹ concepts. Using the case of energy metering data, the example of standards-based arrangement is EDA – Energy Data Exchange Austria, the example of physical

⁸ The definition of DEP according to EU-SysFlex project (D5.1, 2021 [19]): „Data exchange platform (DEP) is a communication platform the basic functionality of which is to secure data transfer (routing) from data providers (e.g. data hubs, flexibility service providers, TSOs, DSOs) to the data users (e.g. TSOs, DSOs, consumers, suppliers, energy service providers). DEP stores data related to its services (e.g. cryptographic hash of the data requested). The DEP does not store core energy data (e.g. meter data, grid data, market data) while these data can be stored by data hubs. Several DEPs may exist in different countries and inside one country.”

⁹ The definition of middleware according to Tutorials Point (https://www.tutorialspoint.com/software_architecture_design/distributed_architecture.htm): „Middleware is an infrastructure that appropriately supports the development and execution of distributed applications. It provides a buffer between the applications and the network. It sits in the middle of system and manages or supports the different components of a distributed system. Examples are transaction processing monitors, data convertors and communication controllers etc.”

¹⁰ The definition of distributed architecture according to Tutorials Point (https://www.tutorialspoint.com/software_architecture_design/distributed_architecture.htm): „In distributed architecture, components are presented on different platforms and several components can cooperate with one another over a communication network in order to achieve a specific objective or goal. In this architecture, information processing is not confined to a single machine rather it is distributed over several independent computers.”

¹¹ The definition of data federation according to TIBCO website (<https://www.tibco.com/reference-center/what-is-a-data-federation>): „A data federation is a software process that allows multiple databases to function as one. This virtual database takes data from a range of sources and converts them all to a common model. This provides a single source of data for front-end applications.”

integration is a central data hub as operating in many countries (e.g., Datadis in Spain, DataHub in Denmark), and the example of DEP is Estfeed in Estonia (connecting data hub and data users).

The report on Data Exchange in Electric Power Systems: European State of Play and Perspectives (ENTSO-E, THEMA, 2017 [18]) stated that DEPs improve coordination and market access and new business opportunities due to improved data and information access. The E.DSO position paper (2020 [16]) explains two technical solutions for data management to be considered equally – DEP based centralised data exchange and bilateral decentralised data exchange. GEODE (2020 [33]) introduces also the hybrid model, combining decentralised and centralised models, whereby market participants communicate in a decentralised manner, but there can be “task-specific central structures”.

“Regulated governance models” and “self-governance model” have been distinguished for data (and also for energy market services): “Typically, collective self-governance rules such as reputation, transparency and accountability shall replace trusted intermediary services offered by centralised IT platforms.” (AIOTI et al., 2021 [2]). While data hubs in many countries are the examples of regulated models, these may not be suitable for local, distributed, peer-to-peer data exchanges.

In April 2020, Elering, together with the other 8 system operators organised a competition to select EU Data Access Pilots of innovative energy products and services which need access to metering data. As a conclusion of those pilots, some main necessary functionalities of grid data interoperability were defined:

- Harmonised standard(s) of data formats and access
- Security, trust, non-repudiation
- Authentication solutions for users and service providers
- Identification of metering points of the user
- Consent management system
- Transparency of data usage/processing history
- Easy integration of additional data sources
- Cloud-based and cloud-agnostic solutions simplify integration and scaling of business

The competition indicated the need for cross-border data interoperability. The initiative called Data Bridge Alliance was launched. (However, it was discontinued due to COVID-19.) The EU-SysFlex project investigated the business model of such an alliance (D11.30, 2022 [21]). “This diversity of formats and procedures of data access becomes a problem for app owners in the energy sector (retailers, aggregators, Energy service companies (ESCOs), etc.), as they incur high software development costs to reach data hubs of different types and countries. The Data Bridge Alliance (DBA) proposes to solve this problem by creating a cross-border Data Exchange Platform (DEP) to render energy data hubs interoperable and to connect energy-related app owners with data hubs.”

“The Data Bridge Alliance guarantees secure data exchange and non-intrusiveness since the platform does not visualise or store the data itself. App owners can access the pool of data hubs with one single Application Programming Interfaces (API), resulting in a cost saving opportunity. This easy access to a large pool of European energy data will improve the creation and scale-up of energy-related businesses. Moreover, the European regulation will oblige its member states to implement cross-border interoperability of energy data, as defined in the EU Directive 2019/944, Article 55.”

The figure below illustrates the Value Creation Ecosystem (VCE) of DBA.

European Energy data space provisioned in the Digitalisation of Energy Action Plan (EC, COM(2022)552 [27]) could take the European wide role to ensure the interoperability of individual data platforms. Furthermore, the interoperability should be targeted with other sectoral European data spaces. According to SmartEn (2021 [58]) the Energy data space would support competitive energy services market through seamless data exchange; the fragmentation of data platforms and marketplaces should be avoided by developing European data-sharing infrastructure; data exchange platforms should be overseen by a neutral facilitator; the European data space could be built on existing federated cloud infrastructures like GAIA-X¹³.

¹³ <https://www.data-infrastructure.eu/GAIA/Navigation/EN/Home/home.html>

Open source is recognised increasingly as a key aspect for having access to data platforms. The European Interoperability Framework (EC, 2017 [24]) recommends to “ensure a level playing field for open source software, taking into account the total cost of ownership of the solution”.

- Make efforts and demonstrate the **interoperability of a data platform** with other European data platforms.
- Call the common European (Energy) data space to keep the registry of and to issue **compliance labels** to interoperable data platforms.

4.2.9 Interfaces

“APIs can be enablers of products, components of products, or even products themselves, even if an external customer never sees them. This gives APIs tremendous potential in any enterprise context, as they can be reused in abstract ways to allow for unbundling and bundling of value. [...] API products — like all products — are vehicles for delivering value from producers to consumers. As digital products, APIs can provide value with immediacy, and as software interfaces, they are easily updated, automated, and composed.” (Fishman and McLarty, 2021 [32]).

Connecting participants like FSPs, market operators, system operators, data hubs to a data platform should entail minimum amount of expertise, time and costs in order not to scare them off. APIs and GUIs (graphical user interfaces) are the options that should be made available by data platforms always. It should be recognised that for some participants (consumers, smaller FSPs) GUIs may be the preferred option for interfacing, enabling more flexible interaction between the platform and the user of the platform. Furthermore, public web portals (like dashboards) should be promoted as they may be often a starting point for the data provider and data user to find more information from the data platform, including about the access to other participants they wish to exchange data with.

Open APIs should be available to support interoperability and specifically portability as part of interoperability. APIs should be directly downloadable, user friendly and enable close to real-time data access (Hofheinz and Osimo, 2017 [35]). The public sector can serve as an example in using “well-formed APIs” for the portability, this could apply to public data and non-public data (in latter case the access would be limited to entitled persons like a company accessing its tax data) (Ilves and Osimo, 2019 [40]).

The European Interoperability Framework (EC, 2017 [24]) recommends ensuring data portability for transferring data easily between systems, and to publish open data in machine-readable formats.

Technical integration has to be as seamless as possible, while respecting privacy and security requirements. Clear guidelines for integrating with any data platform must be available and the integration itself must be as seamless and affordable as possible. “However, the energy domain currently lacks an overall accepted,

collaborative and community driven governance which supports the development and documentation of adequate technical frameworks and respective integration profiles in accordance to community requirements and provides the necessary means for integration tests.” (Schütz et al., 2021 [57])

The European Interoperability Framework (EC, 2017 [24]) recommends to “develop interfaces with base registries and authoritative sources of information, publish the semantic and technical means and documentation needed for others to connect and reuse available information” and to “match each base registry with appropriate metadata including the description of its content, service assurance and responsibilities, the type of master data it keeps, conditions of access and the relevant licences, terminology, a glossary, and information about any master data it uses from other base registries”.

- Make available **interfaces** – Application Programming Interfaces and Graphical User Interfaces – of the data platform.
- Provide unified European wide **guidance for integrating** with any of the European data platform for developers, data intermediaries, data providers and data users, regardless of their physical location and data type.

4.2.10 Repositories

In current context, a repository (or catalogue) means a systemised set of objects, which are needed for the semantics (and possibly syntax) of data exchange. These objects may include roles, data objects, data profiles, processes. Such repositories should facilitate the data exchange, basically enabling to pick from the “drop-down” lists relevant predefined and unified objects.

Repositories can be part of the platforms, i.e., each platform developing and operating its own repositories. However, it seems to make more sense to decouple the repositories from data platforms. This would have three main benefits. First, it contributes to interoperability if different platforms use the same repositories. Second, there is no need to duplicate the efforts for setting up the repositories with the same content. Third, the risk of having separate repositories with the same kinds of objects but different meanings can be minimised.

Access to repositories should be easy and free of charge for the users. According to Schütz et al. (2021 [57]) “repository for technical frameworks” to implement business cases should be provided, published and be freely available. Tools like GitHub¹⁴ and the EIRIE platform newly promoted by EC¹⁵ already exist for hosting repositories and enabling access to these. Zenodo¹⁶ is a platform for opening data produced in EC funded research projects.

¹⁴ <https://github.com/>

¹⁵ <https://ses.jrc.ec.europa.eu/eirie/>

¹⁶ www.zenodo.org

The BRIDGE Initiative makes reference to several existing or proposed future repositories in its recommendations related to the implementation of DERA 2.0 (BRIDGE, 2022 [9]):

- “Harmonise the development, content and accessibility of data exchange business use cases for cross-sector domain through BRIDGE use case repository.
- Use BRIDGE use case repository for aligning the role selection. Harmonise data roles across electricity and other energy domains by developing HERM – Harmonised Energy Role Model and ensure access to model files. Look for consistency with other domains outside energy based on this HERM – cross-sectoral roles.
- Define and harmonise functional data processes for cross-sector domain, using common vocabulary, template and repository for respective use cases’ descriptions.
- Define, maintain and ensure access to model files of a generic canonical data model facilitating cross-sector data exchange, e.g. by extending Common Information Model (CIM) and/or integrating other sectors’ canonical data models with CIM.
- Develop cross-sector data models and profiles, with specific focus on private data exchange. Enable access to model files.”

BRIDGE (2021 [8]) proposes four steps to establish a CIM repository:

1. “Collect business objects and CIM profiles with links to use cases per project.
2. Generate overview of business objects and CIM profiles and identify the commonalities.
3. Create an UML repository for business objects and CIM profiles.
4. Manage a repository of instance files (a data set conformant with the profile).”

Needs for further repositories may emerge in future, especially while developing and implementing data spaces. For example, Cheong and Chang (2007 [11]) refer in their Data Governance Framework to Metadata Repository. The European Interoperability Framework (EC, 2017 [24]) recommends “put in place catalogues of public services, public data, and interoperability solutions” and by doing that to describe these using common models.

- Create common **European data repositories** at least for cross-sector data roles, data types (objects, profiles) and processes (use cases).
- Make the common European data repositories available **free of charge**.

4.3 Results of data governance survey among OneNet partners

A survey was prepared and conducted jointly with some other Horizon 2020 and Horizon Europe projects in the framework of BRIDGE Initiative’s Data Management Working Group (see Appendix B). The survey contained

all the above-described 22 data governance requirements. Ranking in three categories was requested for each requirement from 1 to 5: relevance, (i.e., positive impact); feasibility, (i.e., risks); and actual implementation in demo.

Answers were requested from OneNet partners – targeting demo partners and ICT partners developing OneNet middleware. In total, 12 partners provided the answers.

Figure 11 highlights most and least relevant data governance requirements – average ranks based on the responses from OneNet partners. The most relevant requirements relate to consent management, know-your-data-user principle, access to APIs and GUIs, and availability of repositories. The least relevant relate to data governance KPIs, proposing new legislation and standards, risk assessment, and EU level steering group.

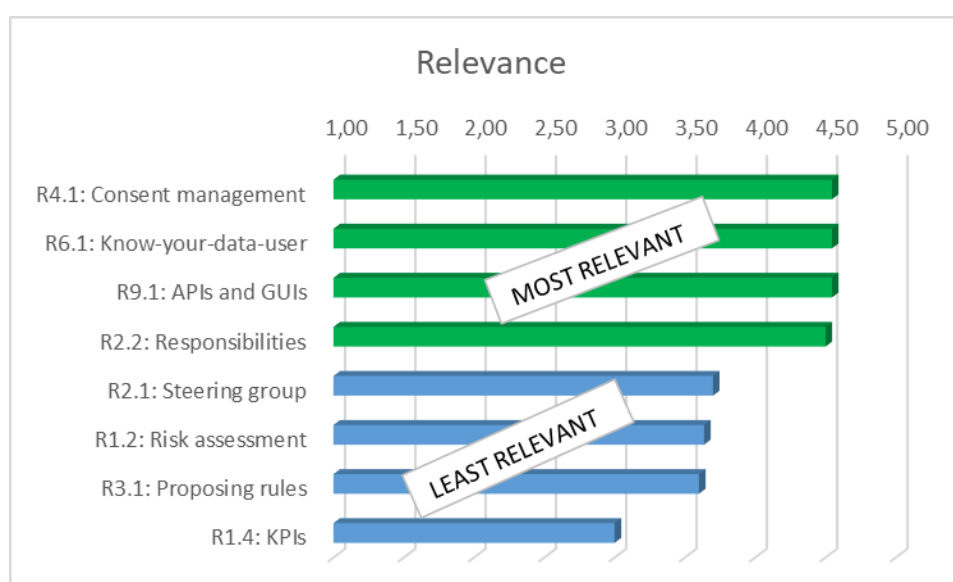


Figure 11: 4 most and 4 least relevant data governance requirements according to OneNet partners

Figure 12 highlights the most and least feasible data governance requirements – average ranks based on the responses from OneNet partner. The most feasible requirements relate to free of charge access to repositories, authentication of data users, risk assessment, and availability of reference models. The least feasible (i.e., the riskiest) relate to EU level steering group, know-your-data-user principle, and availability of single data access points and one-stop-shops.

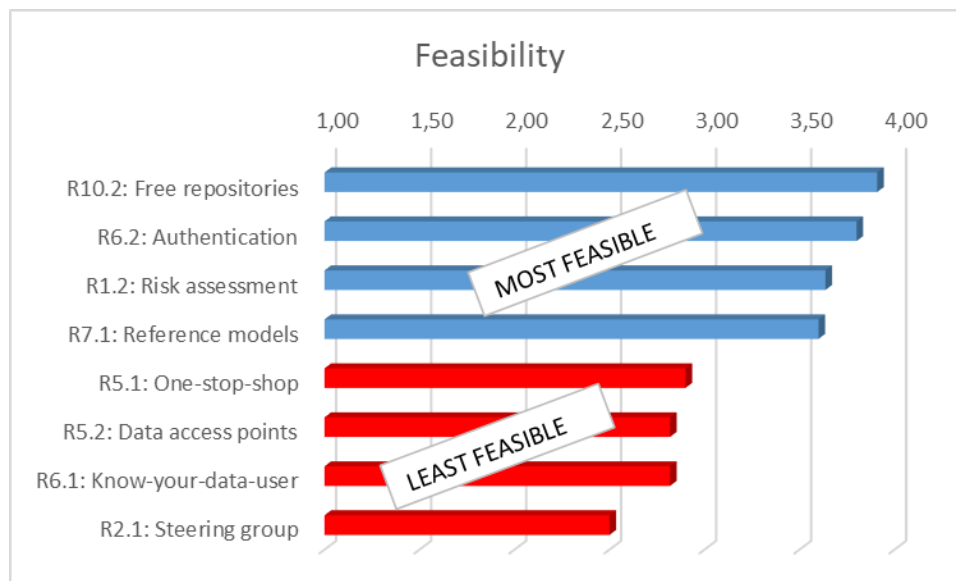


Figure 12: 4 most and 4 least feasible data governance requirements according to OneNet partners

Figure 13 lists ten data governance requirements which are most implemented in OneNet project according to the partners' information, however, only three of them being above the average rank (3,0) - consent management, access to APIs and GUIs, and availability of reference models. This may be explained by the fact that, while development of OneNet Framework explicitly targets many of the requirements, the individual demos and partners do not have the data governance per se high in the agenda.



Figure 13: Top-10 data governance requirements implemented in OneNet

Table 5 presents the average ranks of individual requirements per data exchange elements. Regarding the relevance category all ranks are well above the average rank (from 3,66 to 4,55). But for the feasibility all ranks are close to the average rank (from 2,75 to 3,55). It seems to indicate that while all elements are considered rather important for proper data governance, they may entail quite some risks for realisation. The most important relates to data ownership but the feasibility has only the score of 3. Even less feasible is orchestration, but at the same time assessed to be one of the highest importance. Total score varies from 6,85 to 7,68 – it is the sum of relevance and feasibility ranks. It is supposed to highlight the elements where to start from – combination of the importance and implementation easiness being the best. Outstanding ones here relate to data security, repositories, data vocabulary and data ownership.

Table 5: Relevance and feasibility of data exchange governance elements for OneNet partners

	Relevance (A)	Feasibility (B)	TOTAL SCORE (A) + (B)
1. DATA GOVERNANCE BUSINESS CASE	3,66	3,33	7,00
2. ORCHESTRATED DATA GOVERNANCE	4,10	2,75	6,85
3. RULES AND NORMS	3,80	3,30	7,10
4. DATA OWNERSHIP GOVERNANCE	4,55	3,00	7,55
5. DATA ACCESS GOVERNANCE	4,06	3,04	7,10
6. DATA SECURITY GOVERNANCE	4,37	3,31	7,68
7. DATA VOCABULARY GOVERNANCE	4,20	3,44	7,63
8. DATA PLATFORMS	3,89	3,19	7,08
9. INTERFACES	4,23	3,18	7,41
10. REPOSITORIES	4,10	3,55	7,65

5 OneNet implementation and demonstration of cross-stakeholder Governance for Energy Data Exchange

This Chapter aims to identify and present the data governance developments of the OneNet reference architecture at its current status, including also specifications for future development during the lifecycle of OneNet project. The methodological approach applied is based on the following steps: 1) creation of the Governance Requirements Traceability Matrix (GRTM) for the specific functional requirements that are relevant to governance aspects; 2) reflection of specific functional requirements linking to the Reference Data Governance Model (described in Chapter 4); and 3) reference to the OneNet project participation in the BRIDGE DERA implementation focusing specifically on cross-sector stakeholder governance perspective.

5.1 OneNet governance requirements identification

5.1.1 Governance Requirements Traceability Matrix

This section provides the detailed representation of cross-stakeholder Governance Requirements Traceability Matrix (GRTM) following a two-step approach. In the first stage there is a sorting of OneNet Functional Requirements (FRs) (OneNet D5.3, 2021 [48]) into the ones that have relevance with data governance per se. Hence, in this section the sorted functional requirements are reported as Governance Functional Requirements (GFRs) and are accordingly defined and matched with the governance dimensions as described in Chapter 3.3 (i.e., Access, Usage, Standardisation, Integrity, Structure). In the second stage, the governance requirements of the Reference Data Governance Model described in Chapter 4 will be checked for their compliance with OneNet technical approaches and discussed from the future potential developments and enhancements perspective.

The GRTM is developed following the approach suggested in (PM² Alliance, 2020 [54]). The proposed GRTM is presented in Table 6. Hereby, the applied matrix is slightly modified to accommodate the needs of this analysis.

Table 6: Requirement traceability matrix (based on PM² Alliance, 2020 [54])

Requirement traceability matrix	
ID	Unique identifier.
Name	Short and descriptive name.
Status	The status of a requirement can e.g. be any of the following: Specified, Proposed, Approved, Incorporated, Implemented, Validated, For Fixing & Rejected.
Priority	Statement of relative importance of the requirement, as e.g. High, Medium, Low, or Must-have, Should-have, Could-have, Won't-have.
Size	An indication of the level of effort needed or how hard it will be to implement the requirement. (Big, Medium, Small)
Comments	Comments on the requirement. If the requirement has been REJECTED the reason for rejection must be described here.
Derived From	Identifier of the Requirement from what requirement it was derived (for example a Feature must be always derived from a high level Business requirement or Stakeholder Need, and a detailed requirement from a Feature).
Related WBS code	Identifier of the Work Breakdown Structure (WBS) element that produces the deliverable for which this is a requirement.
Specification of documentation	Name of the document where the requirement is specified and the file location.
Test Plan	Name and file location of the document where the test plan or acceptance criteria for this requirement is described.

Based on the list of functional requirements of the OneNet reference architecture, the effort hereby relies on sorting the ones that implement data governance features. Table 7 details those functionalities assigning their relevance vis-a-vis data governance.

Table 7: OneNet Governance Functional Requirements list

GFR ID	GFR title	Governance dimension
GFR01	Configuration of OneNet Connector: Configure data format/ semantic annotation	Standardisation, Integrity
GFR02	Configuration of OneNet Connector: Configure data quality	Integrity
GFR03	Configuration of OneNet Connector: Configuration of transaction logging	Usage, Access
GFR04	Configuration of OneNet Connector: Configuration of data reception endpoints	Access
GFR05	ONBOARDING_Connector Configuration and Provisioning: Define connector configuration model- General information	Access
GFR06	ONBOARDING_Connector Configuration and Provisioning: Define connector configuration model- Lifecycle- Data Flow	Access
GFR07	Middleware Features: Available services and data sources discovery	Access, Usage
GFR08	Middleware Features: Registration of the OneNet Connector	Access
GFR09	Data exchange through REST APIs: Exchange harmonised payload data	Structure, Standardisation
GFR10	Data exchange through REST APIs: Authentication in OneNet System	Access
GFR11	Data exchange through REST APIs: Data Retrieval	Access
GFR12	Middleware Features: Any Data sources is integrable with OneNet Middleware	Structure, Standardisation
GFR13	Data Exchange: Publish Data	Access, Usage
GFR14	Data Exchange: Subscribe as service consumer	Access
GFR15	Data Exchange: Subscribe to a data source	Access, Usage
GFR16	Monitor OneNet Connector status: Monitor network traffic	Access
GFR17	Monitor OneNet Connector status: Monitor known data sources	Access, Structure
GFR18	Monitor OneNet Connector status: Monitor transaction logs	Access
GFR19	Monitor OneNet Connector status: Monitor results from data quality checks	Integrity
GFR20	Registration and Configuration: Registering as OneNet Participant	Access
GFR21	Registration and Configuration: Discovery/search data sources	Access, Structure
GFR22	IDS-based Service: Usage Control - Policy definition	Usage
GFR23	File Upload	Structure
GFR24	ONBOARDING_Security Setup: IDS Consumer/Provider configures data access restrictions	Usage/Access
GFR25	IDS-based Service: Clearing House	Access
GFR26	ONBOARDING_Connector Configuration and Provisioning: Define connector configuration model	Access
GFR27	EXCHANGE OF DATA_ Invoke Data Operation: Notification of data operation call at clearing House	Access
GFR28	EXCHANGE OF DATA_ Invoke Data Operation: Notification of data operation call reception at clearing House	Access
GFR29	EXCHANGE OF DATA_ Invoke Data Operation: Clearing house logs in a persistence database all transactions	Access

GFR30	EXCHANGE OF DATA_ Invoke Data Operation: Notification of data operation result sent at clearing House	Access
GFR31	EXCHANGE OF DATA_ Invoke Data Operation: Notification of data operation result received at clearing House	Access
GFR32	ONBOARDING_ Availability Setup: Broker provider functions for searching	Access, Structure
GFR33	EXCHANGE OF DATA_ Find Data Provider: Connector provides proper interface to find data provider	Access
GFR34	Access OneNet Framework: Register or change data access consents	Usage
GFR35	IDS-based Service: Usage Control - Access Control and Enforcement	Usage
GFR36	Middleware Features: Data Quality Checking	Integrity
GFR37	OneNet Additional Services: Data Quality	Integrity
GFR38	Middleware Features: Development of semantic models	Standardisation
GFR39	OneNet Additional Services: Data Harmonisation	Standardisation
GFR40	EXCHANGE OF DATA_ Invoke Data Operation: Data consumer negotiate policy with data provider	Usage
GFR41	Cybersecurity: Ensuring the security and privacy of data exchanged	Access
GFR42	Cybersecurity: Tracking all the data processes and flows	Access
GFR43	Cybersecurity: Providing a testing environment to identify and solve potential security breaches	Access
GFR44	Access OneNet Framework: Register or modify account	Access
GFR45	Access OneNet Framework: Login to Framework Dashboard	Access
GFR46	Monitoring and Analytics Tools: Administrative and configuration tools	Access
GFR47	Access OneNet Framework: Monitor overall performance	Access, Integrity
GFR48	Middleware Features: Import/Export for analytics	Access
GFR49	Monitoring and Analytics Tools: Data Analytics Dashboard	Access
GFR50	Monitoring and Analytics Tools: Monitoring and Alerting Dashboard	Access

Based on the GRTMs presented in Table 7, one may perceive a couple of outlines of the focal points of the current and future developments of the OneNet reference architecture. A graphical representation of the discussed GFRs is in Figure 14. It is clearly reflected that there is high coverage and focus on the Access dimension of data governance aspect, assuming the several mechanisms for seamless data access, policy and security. This is due to the focus of OneNet implementation to allow the OneNet participants to act as provider and/or consumer of data and to define their own access policies for any kind of data exchange. The identification of the OneNet participants is completely ensured by the Identity Manager included in the OneNet Middleware, creating a trusted data space where the OneNet participants can cooperate with each other. A specific security layer is also included for ensuring authentication and authorisation for participating in the OneNet ecosystem. Reflected in the bar graph of the Figure 14, is a lower share of GFRs related to standardisation dimension. This is due to the fact that OneNet design follows the general principles of the IDS RAM towards the standardisation

of specific functions that are related to data management, data trust and sovereignty which is reflected on the access dimension. Additionally, the OneNet solution suggests the standardisation of data services adopting a standard, yet open, definition of the cross-platform services (i.e., as a living directory) accompanied by harmonised semantics.

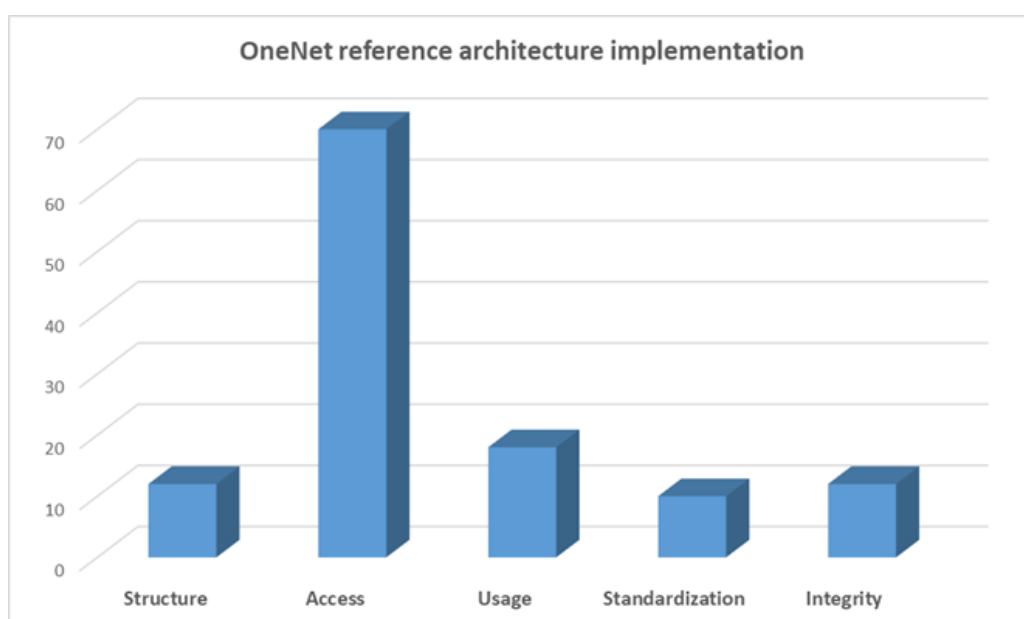


Figure 14: Illustrative data governance dimensions of OneNet reference architecture

5.1.2 Governance Functional Requirements' mapping to Reference Data Governance Model

This section aims at mapping the elements of Reference Data Governance Model (Chapter 4) to the GFRs. Table 8 reports the corresponding links. Because not all RDGM elements are related to functional requirements as such, only selected elements of RDGM could be mapped to OneNet GFRs.

Table 8: OneNet Governance Functional Requirements reflected in Reference Data Governance Model

Requirements of Reference Data Governance Model	OneNet Governance Functional Requirements
Define business case for data governance on relevant level [project / organisation / country / EU], e.g., by means of business model canvas or standardised IEC 62559-2 template.	-
Evaluate regularly the risks associated to the implementation of data governance programme using risk assessment methodologies.	-

Define and follow the principles of data-as-an-asset	All GFRs reported related to Access, Usage dimensions do address data-as-an-asset principles, such as addressing: 1) what is the value, 2) how you can access them, 3) what are the policies.
Define and monitor KPIs for data governance programme itself and for specific data exchanges.	GFR42, GFR43, GFR50
Establish a group to steer the European Energy Data Space, open to European initiatives and stakeholders to participate, and ultimately leading to cooperation between energy and other sectors.	Not entirely addressed, yet cross-platform services can be seen as an intra-energy approach towards data spaces. Hence, GFR07, GFR14 are relevant.
Define the responsibilities and accountability for European data exchange, including European Commission, Member states, data providers, data users, etc.	Same as previous.
Propose and promote regulations and standards facilitating improved data governance.	-
Understand regulatory and standards' requirements driving the need for proper data governance.	Not entirely addressed, yet cross-platform services can be seen as an intra-energy approach towards data spaces. Hence, GFR07, GFR14 are relevant. The conception of cross-platform services as a living directory of OneNet users and a potential user/association that deals with the management, maintenance and definition of them towards harmonised syntax and semantics.
Ensure consent management process which is accessible to any party willing to provide or use any data and not limited to single country.	GFR07, GFR21, GFR22, GFR35, GFR40
Ensure the availability of one-stop-shop providing information about and access guidance to different types of data.	GFR07, GFR14
Make available single data access points and ensure everyone's rights to access data.	GFR07, GFR21, GFR22, GFR35, GFR40
Ensure legislative grounds for sub-meter and other end-customer related data governance.	-
Apply "know-your-data-user" principle by making data usage information* available to data owners easily and free of charge.	GFR14, GFR15
Harmonise authentication schemes across Europe and sectors.	GFR08, GFR10, GFR44

In data modelling, follow the generally recognised reference models for roles, information and processes.	GFR01, GFR38
Establish European arrangement for coordinating reference models and national mappings.	GFR01, GFR38
Make efforts and demonstrate the interoperability of a data platform with other European data platforms.	This is the general approach of deploying the data space connector of OneNet.
Call the common European (Energy) data space to keep the registry of and to issue compliance labels to interoperable data platforms.	Under specification.
Make available interfaces – Application Programming Interfaces and Graphical User Interfaces – of the data platform.	GUI features: GFR01, GFR23, API-based: GFR09, GFR10, GFR11.
Provide unified European wide guidance for integrating with any of the European data platform for developers, data intermediaries, data providers and data users, regardless of their physical location and data type.	OneNet Connector connectivity. All GFRs can be relevant to this for the data space connector realisation.
Create common European data repositories at least for cross-sector data roles, data types (objects, profiles) and processes (use cases).	Federated catalogue to be developed in the context of OneNet & BRIDGE Data Management Working Group synergies, stemming from cross-platform services directory.
Make the common European data repositories available free of charge.	Cross-platform services concept and the available easy discoverable data sources, GFR07, GFR14.

5.2 OneNet involvement in BRIDGE data exchange reference architecture implementation

The European energy Data Exchange Reference Architecture, called DERA, has been defined in 2020 and elaborated upon during 2021/2022 (DERA 2.0). It has been an action of the BRIDGE Initiative, based on the identified elements and recommendations for interoperability between platforms and systems, related to both intra- and cross-sector operation, and thus the development of a conceptual European data exchange model, involving elements like functionalities, governance, data access, open source.

The OneNet project reflects its developments and compliance with DERA and promotes the cross-project data exchange implementation by exploiting its technical developments for the realisation of open services. Based on these services, the proposed approach is to utilise the OneNet connector as the facilitator of seamless and secure cross-project data exchange. The technological developments allow for the discoverability of third party platforms from different projects opening the path for cross-sector interconnectivity.

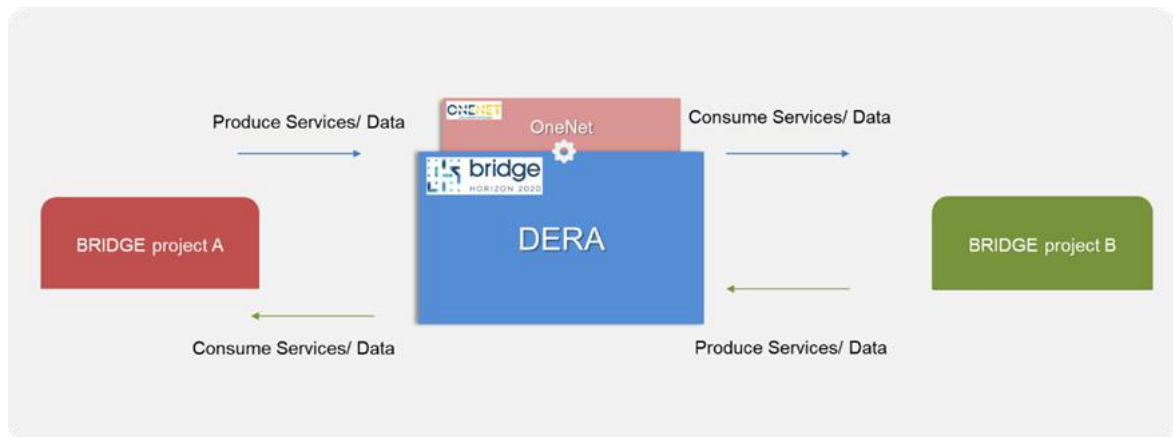


Figure 15: OneNet connector as facilitator of data exchanges

The OneNet connector instantiates a broad part of BRIDGE DERA recommendations (2022 [9]), including the usage of domain agnostic principles such as IDS Connector and FIWARE Context Broker. This enables the trusted data exchange, a virtual data space leveraging existing standards and technologies, as well as governance models well-accepted in the data economy, to facilitate secure and standardised data exchange and data linkage in a trusted business ecosystem. The utilisation of the OneNet connector provides access to a set of standardised data services (i.e., the cross-platform services), common authorisation and authentication services, peer-to-peer data exchange, easy to use via GUI or open APIs.

OneNet is significantly supporting the implementation of BRIDGE DERA. An initial approach proposes the development of a standardised process for cross-sector services specification towards the establishment of stakeholders' governance, beyond the utilisation of OneNet connector as the facilitator (as an evolving data space connector potentially) of third-party platforms (including test cases with cross-sector incorporation). The main conception of this approach stems from the cross-platform services directory, allowing for a public tool where stakeholders can define standard data services or applications that can be exploited for cross-sector integration.

The proposed cross-sector services are foreseen to be in place as the BRIDGE Federated Catalogue, leveraging multiple domain services, for supporting the gradual development of data spaces. This proposed Federated Catalogue is foreseen to be an open catalogue that can be utilised in a wider context, assuming the specification of data services (i.e., functional specification, semantic definition, relevant etc.) as well as for service applications (i.e., service definition: privacy policy, service agreement, semantic compliance input/output specification, data flow definition).

5.3 Reference Data Governance Model elements in OneNet Data

Governance Framework

The OneNet Data Governance Framework defined in Chapter 3.3 converges almost completely with Reference Data Governance Model described in Chapter 4.

In fact, the five dimensions of the OneNet Data Governance Framework reflect the characterising governance elements mapped on four of the five SGAM interoperability layers. The Business Layer is the only one not addressed in the OneNet analysis, since is partially out of the scope of the OneNet System vision.

All the other elements are easily matchable with the five dimensions of the OneNet Data Governance Framework, following the schema reported in Figure 16:.

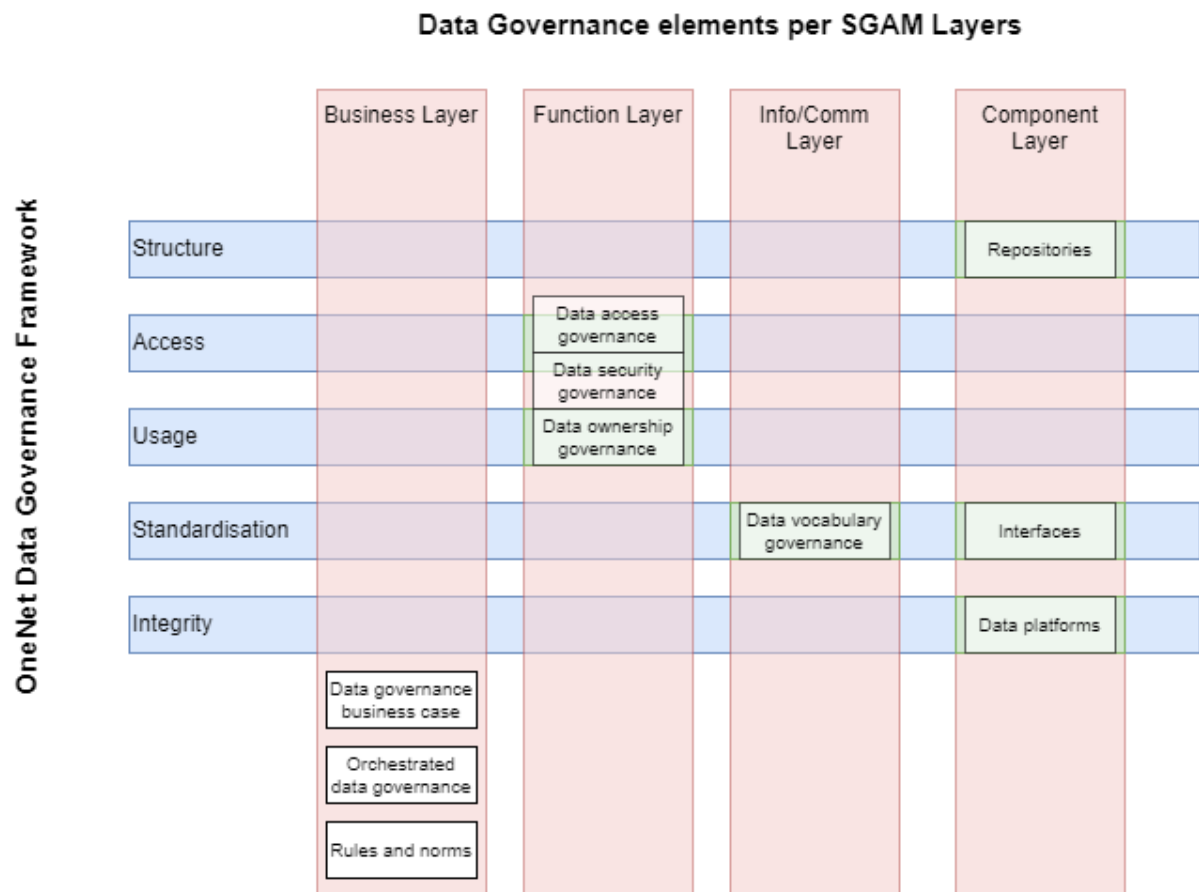


Figure 16: OneNet Data Governance Framework mapping to SGAM based Data Governance Reference Model

6 Conclusion

Main recommendations on interoperability were collected from literature and were compared with existing initiatives from European and independent projects. It was concluded that the majority of the recommendations are yet to be addressed, with the main work being done within the data portability topic, through application and creation of different standards, data models, data formats and ontologies. Licensing is another topic well regarded both within the recommendations and within the initiatives considered. However, despite the recommendations are pointing more towards the open-source of data models and data architecture, the approach chosen by the initiatives is split between open-source and closed-source, possibly due to market competition reasons; therefore, greater efforts in this essential item need to be conducted.

These conclusions are related to a sample of seven initiatives; therefore, it is not possible to infer any clear trend in each of the topics addressed. Hence, a close monitoring on the success of these initiatives can later shed some light on what approach becomes more dominant in the energy sector.

One of the main goals during the design and definition of the OneNet data exchange framework was to make available and accessible data from different sources (actors) in a secure and trusted way ensuring data ownership and privacy. For this reason, it is useful to analyse how the OneNet architecture: defines the concepts of data providers and data consumers; implements the concept of fully decentralised data exchange; ensures the data ownership and consent management; and facilitates the cross-platform integration in a secure and interoperable way.

These aspects are strictly connected with the Data Governance concept and for this reason a specific OneNet Data Governance Framework was designed and implemented. The framework consists of 5 important dimensions:

- Structure – defines how data will be organised, retrieved, and stored;
- Access – defines how the data can be accessed, the policy and the security;
- Usage – establishes parameters and restrictions on use of the data;
- Standardisation – ensures conformance of the data, as well as the portability, reusability, and interoperability;
- Integrity – establishes characteristics to ensure the quality of the data (accuracy, validity, and reliability).

All the OneNet processes rely on these five dimensions. Furthermore, these are also aligned with the more generic and universal Reference Data Governance Model elaborated in this deliverable. A Reference Data Governance Model is proposed consisting of 10 elements and a set of requirements corresponding to each element. Data governance elements include:

1. Data governance business case
2. Orchestrated data governance

3. Rules and norms
4. Data ownership governance
5. Data access governance
6. Data security governance
7. Data vocabulary governance
8. Data platforms
9. Interfaces
10. Repositories

A survey was prepared and conducted jointly with some other Horizon 2020 and Horizon Europe projects in the framework of BRIDGE Initiative's Data Management Working Group. The survey addressed all the 22 data governance requirements. In total, 12 OneNet ICT and demo partners provided the answers. According to partners' average answers, while all identified elements are considered rather important for proper data governance, they may entail quite some risks for realisation. On the level of requirements, the most relevant relate to consent management, know-your-data-user principle, access to APIs and GUIs, and availability of repositories.

The most feasible requirements relate to free of charge access to repositories, authentication of data users, risk assessment, and availability of reference models. The least feasible (i.e., the riskiest) relate to EU level steering group, know-your-data-user principle, and availability of single data access points and one-stop-shops. The most implemented requirements in OneNet project are consent management, access to APIs and GUIs, and availability of reference models.

Finally, the analysis of OneNet project's governance functional requirements was performed through the Governance Requirements Traceability Matrix. The analysis also considered the categorisation of these functional requirements into the five governance dimensions of OneNet Data Governance Framework. This analysis indicated that there is an extended focus of OneNet developments on the data access dimension. This is justified since OneNet adopts IDSA RAM domain agnostic principles that enable participants to act as provider and/or consumer of data and to define their own access policies for any kind of data exchange assuming common authorisation and clearing services.

OneNet participation in the implementation of the DERA reference architecture of the BRIDGE Initiative was explored referring to the fact that OneNet connector can be the mediator to establish cross-demo and cross-sector secure and trusted information and data exchanges. BRIDGE DERA, given its alignment with DESAP, will consider the OneNet connector as a potential data space ecosystem. Towards the implementation of BRIDGE DERA, the designation of Federated Catalogue (data services and application services) was discussed extending the notion of the OneNet cross-platform services as part of cross-stakeholders governance.

References

- [1] Ahle, U.; Hierro, J.J. (2022). FIWARE for Data Spaces. In: Otto, B., ten Hompel, M., Wrobel, S. (eds) Designing Data Spaces. Springer, Cham. https://doi.org/10.1007/978-3-030-93975-5_24
- [2] AIOTI, EIT, ENTSO-E, SDA Bocconi (2021). Open Energy Marketplaces evolution. Beyond Enabling Technologies. <https://aioti.eu/wp-content/uploads/2021/03/Open-Energy-Marketplaces-Evolution-Published.pdf>
- [3] Alhassan, I.; Sammon, D.; Daly, M. (2016). Data governance activities: an analysis of the literature. Journal of Decision Systems, 25:sup1, 64-75, DOI: 10.1080/12460125.2016.1187397. <https://doi.org/10.1080/12460125.2016.1187397>
- [4] ASSET Project (2020). Format and procedures for electricity (and gas) data access and exchange in Member States. <https://op.europa.eu/en/publication-detail/-/publication/0be7e230-6505-11eb-aeb5-01aa75ed71a1/language-en>
- [5] Australian Competition and Consumer Commission's webpage: Consumer Data Right rollout. <https://www.accc.gov.au/focus-areas/consumer-data-right-cdr/cdr-in-the-energy-sector>
- [6] BRIDGE Data Management WG: Genest, O; Pons, L.; Valckenaers, P.; Crihan, F. (2019-1). Main findings and recommendations. <https://bridge-smart-grid-storage-systems-digital-projects.ec.europa.eu/sites/default/files/documents/working-groups/BRIDGE-Data-Management-WG-Findings-and-Reco-July-2019.pdf>
- [7] BRIDGE Data Management WG and Regulation WG: Gerard, H.; Jarry, G.; Kuk, K.; Genest, O.; Oliveira, F.; Lambert, E.; Bilidis, N.; Paunovic, N.; O'Doherty, G.; Rivero Puente, E.; Metenier, L. (2019-2). TSO-DSO Coordination. https://bridge-smart-grid-storage-systems-digital-projects.ec.europa.eu/sites/default/files/documents/working-groups/D3.12.f_BRIDGE-TSO-DSO-Coordination-report.pdf
- [8] BRIDGE Data Management WG: Kuk, K.; Kotsalos, K.; Lambert, E.; Bouladakis, G.; Bilidis, N. (2021). European energy data exchange reference architecture. https://energy.ec.europa.eu/system/files/2021-06/bridge_wg_data_management_eu_reference_architecture_report_2020-2021_0.pdf
- [9] BRIDGE Data Management WG: Kuk, K.; Kotsalos, K. (2022). European (energy) data exchange reference architecture 2.0. <https://data.europa.eu/doi/10.2833/142689>

- [10] CEDEC, E.DSO, ENTSO-E, Eurelectric, GEODE (2021). Roadmap on the Evolution of the Regulatory Framework for Distributed Flexibility. https://edsoforsmartgrids.eu/wp-content/uploads/210722_TSO-DSO-Task-Force-on-Distributed-Flexibility_proofread-FINAL-2.pdf
- [11] Cheong, L. K.; Chang, V. (2007). The Need for Data Governance: A Case Study. ACIS 2007 Proceedings. 100. <http://aisel.aisnet.org/acis2007/100>
- [12] CoordiNet D2.4: Bauschmann, C.; Köhlke, J. (2021). Interoperable Platforms for procuring system services from consumers, storage and generators: specification of the interfaces linking the markets for grid services, the advanced monitoring tools for grid operation and the flexibility provided. https://private.coordinet-project.eu/files/documentos/602588d390d27CoordiNet_WP2_D2.4_Interoperable%20Platforms%20for%20procuring%20system%20services%20from%20consumers,%20storage%20and%20generators_V1.0_10.02.2021.pdf
- [13] CoordiNet D2.6: Uslar, M.; Köhlke, J. (2022). Creation of service overview for the DSO interactions: Documentation of services provided. https://private.coordinet-project.eu/files/documentos/6203a7ec05fe1COORDINET_WP2_D2.6%20Creation%20of%20service%20overview%20for%20the%20DSO_V1.0_09.02.22.pdf
- [14] Data Governance Institute's webpage: Governance and Decision-Making. <https://datagovernance.com/governance-and-decision-making/#:~:text=%E2%80%9CData%20Governance%20is%20a%20system,Governance%20is%20about%20enforcing%20rules>
- [15] Dognini, A.; Temal, L.; Challagonda, C.; Genest, O.; Maqueda Moro, E.; Calvez, P.; Helmholt, K.; Ebrahimi, R.; Madsen, H.; Riemenschneider, R.; Daniele, L.; Böhm, R.; Schmitt, L.; Ben Abbas, S. (2022). Data spaces for energy, home and mobility. <https://www.opendei.eu/wp-content/uploads/2022/09/OPEN-DEI-Energy-Data-Spaces-EHM-v1.06.pdf>
- [16] E.DSO (2020). Facilitating customers energy data management and interoperability – DSOs' perspective. <https://www.edsoforsmartgrids.eu/wp-content/uploads/EDSO-Data-management-position-paper.pdf>
- [17] E.DSO: Mataczyńska, E.; Rodríguez, J. M.; van der Heijden, S.; Kula, J.; Voumvoulakis, M. (2022). Grid observability for Flexibility. [20220513_TF1_ANM_-_Go4Flex_Report.pdf \(edsoforsmartgrids.eu\)](https://edsoforsmartgrids.eu/20220513_TF1_ANM_-_Go4Flex_Report.pdf)
- [18] ENTSO-E, THEMA Consulting Group (2017). Data Exchange in Electric Power Systems: European State of Play and Perspectives. <https://www.entsoe.eu/news/2017/06/26/study-data-exchange-in-electric-power-systems-european-state-of-play-and-perspectives/>

- [19] EU-SysFlex D5.1: Kukk, K.; Suignard, E.; Jover, R.; Szczech, P.; Ranaivo Rakotondravelona, M.; Vernhet, P.; Siöstedt, S.; Wang-Hansen, M.; Tkaczyk, A.; Sochynskyi, S.; Abdullayeva, G.; Wiliński, A. (2021). Recommended data exchange conceptual model for Europe. <https://eu-sysflex.com/wp-content/uploads/2021/11/EU-SysFlex-D5.1-Data-exchange-model-v.1.pdf>
- [20] EU-SysFlex D5.5: Kukk, K.; Winiarski, L.; Requardt, B.; Suignard, E.; Effantin, C.; Sochynskyi, S.; Tkaczyk, A.; Lambert, E.; Anton, P.; Rossøy, O.; Good, N.; Jover, R.; Trees, K.; Albers, W. (2021). Proposal for data exchange standards and protocols. <https://eu-sysflex.com/wp-content/uploads/2021/05/Deliverable-5.5-report-FINAL-2021.04.29.pdf>
- [21] EU-SysFlex D11.30: Vinaixa, J.; Vanrespaille, W.; Musleman, H. (2022). Exploitation Report of Selected Results.
- [22] EUniversal D2.2: Vanschoenwinkel, J. et al. (2021). Business Use Cases to unlock flexibility service provision. https://euniversal.eu/wp-content/uploads/2021/05/EUniversal_D2.2.pdf
- [23] European Commission (2015). e-Government Core Vocabularies handbook. <https://ec.europa.eu/isa2/sites/isa/files/publications/e-government-core-vocabularies-handbook.pdf>
- [24] European Commission (2017). New European Interoperability Framework. Promoting seamless services and data flows for European public administrations. https://ec.europa.eu/isa2/sites/default/files/eif_brochure_final.pdf
- [25] European Commission, COM(2020)66. A European Strategy for Data. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN>
- [26] European Commission, COM(2022)68. Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN>
- [27] European Commission, COM(2022)552. Digitalising the energy system – EU action plan. https://energy.ec.europa.eu/communication-digitalising-energy-system-eu-action-plan-com20225522_en
- [28] European Commission, DNV-GL, ESMIG, TNO (2018). Study on ensuring interoperability for enabling Demand Side Flexibility. <https://op.europa.eu/en/publication-detail/-/publication/a61d67de-9ecd-11e9-9d01-01aa75ed71a1/language-en/format-PDF>
- [29] European Commission's webpage: Principles of the GDPR. https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr_en

- [30] European Smart Grids Task Force EG1 (2019). Towards Interoperability within the EU for Electricity and Gas Data Access & Exchange. https://energy.ec.europa.eu/system/files/2019-05/eg1_main_report_interop_data_access_0.pdf
- [31] European Smart Grids Task Force EG1 (2022). Accompanying Report to the EG1 advice on the Implementing acts on data access and interoperability – metering and consumption data. <https://circabc.europa.eu/ui/group/f5b849d3-26ae-4cba-b9f9-6bc6688c5f58/library/8b045f60-f9f0-46a8-8fa0-c64bae71167c/details>
- [32] Fishman, S.; McLarty, M. (2021). Develop a winning API product strategy. https://www.mulesoft.com/lp/whitepaper/api/develop-winning-api-product-strategy?utm_source=email&utm_medium=referral&utm_campaign=newsletter&mkt_tok=NTY0LVNaUy0xMzYAAAF93AWQlhSLPx4fvCT2hasK_zGTNiXeELfAb43xFrXWuKThWk3QNLfN4CTdm5FxBdnNj-AZyWtS0MbWkCdwqfrjKLFIVM8_uX2WcHE3WIWuOty8QHs
- [33] GEODE (2020). Fact sheet data management. <https://www.geode-eu.org/wp-content/uploads/2020/05/202005-Fact-sheet-GEODE-Data-Management-FINAL.pdf>
- [34] Henderson, D. (2017). DAMA - DMBOK. Data Management Body of Knowledge. Published by Technics Publications, DAMA International.
- [35] Hofheinz, P.; Osimo, D. (2017). Making Europe a Data Economy: A New Framework for Free Movement of Data in the Digital Age. <https://lisboncouncil.net/wp-content/uploads/2020/08/LISBON-COUNCIL-Making-Europe-A-Data-Economy.pdf>
- [36] Hohpe, G.; Woolf, B. (2003). Enterprise Integration Patterns: Designing, Building, and Deploying Messaging Solutions. Published by Addison Wesley.
- [37] IDSA (2019). Reference architecture model. <https://internationaldataspaces.org/wp-content/uploads/IDS-Reference-Architecture-Model-3.0-2019.pdf>
- [38] IDSA (2021). Usage Control in the Data Spaces. https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-Position-Paper-Usage-Control-in-the-IDS-V3..pdf
- [39] IDSA webpage: Data Governance Model. https://docs.internationaldataspaces.org/ids-ram-4/perspectives-of-the-reference-architecture-model/4_3_governance_perspective/4_3_2_data_governance_model.
- [40] Ilves, L. K.; Osimo, D. (2019). A Roadmap for a Fair Data Economy. <https://lisboncouncil.net/publications/a-roadmap-for-a-fair-data-economy/>

- [41] ISO 25000 webpage: ISO/IEC 25012. <https://iso25000.com/index.php/en/iso-25000-standards/iso-25012>.
- [42] Ladley, J. (2020). Data Governance. How to Design, Deploy, and Sustain an Effective Data Governance Program. Second Edition. Published by Academic Press, Elsevier Inc.
- [43] mydata.org webpage: Declaration of MyData Principles. <https://www.mydata.org/participate/declaration/>
- [44] Nagel, L.; Lycklama, D. (2021). Design Principles for Data Spaces. Position Paper. <https://design-principles-for-data-spaces.org/>
- [45] Newman, D.; Logan, D. (2006). Governance Is an Essential Building Block for Enterprise Information System. Published by Gartner Research. <https://www.gartner.com/en/documents/492444>
- [46] OneNet D2.1: Tzoumpas, A.; Drivakou, K.; Bachoumis, T.; Troncia, M.; Dominguez Iniguez, F. (2021). Review on markets and platforms in related activities. [D2.1-Review-on-markets-and-platforms-in-related-activities-1.pdf](https://onenet-project.eu/wp-content/uploads/2022/12/OneNet_D2.1-Review-on-markets-and-platforms-in-related-activities-1.pdf) (onenet-project.eu)
- [47] OneNet D5.2: Bosco, F.; Ziu, D.; Triveri, A.; Croce, V.; Sakas, V.; Kapetainos, A.; Kotsalos, K.; Haghgoo, M.; Campos, J.; Alves, T.; Samovich, N.; Damas Silva, C.; Lucas, A.; Kuk, K. (2021). OneNet Reference Architecture. https://onenet-project.eu/wp-content/uploads/2022/12/OneNet_D5.2_v1.0.pdf
- [48] OneNet D5.3: Haghgoo, M.; Happ, S.; Campos, J.; Alves, T.; Cruz, J. M.; Damas Silva, C.; Bosco, F.; Kotsalos, K.; Sakas, V.; Kuk, K.; Mirz, M.; Makula, E. (2021). Data and Platform Assets Functional Specs and Data Quality Compliance. <https://onenet-project.eu/wp-content/uploads/2022/12/OneNet-D5.3-v1.0.pdf>
- [49] OneNet D5.7: Bosco, F.; Croce, V.; Ziu, D.; Triveri, A. (2022). Report on Data Enforcement Policies Design for Sovereignty preserving data access. https://onenet-project.eu/wp-content/uploads/2022/12/OneNet_D5.7_v1.0.pdf
- [50] OneNet D5.8: Zafeiropoulou, M.; Bachoumis, T.; Drivakou, K.; Tzoumpas, A.; Bosco, F.; Ziu, D.; Toots, A.; Jörgi, A.; Petron, M. (2021). Report on Cybersecurity, privacy and other business regulatory requirements. https://onenet-project.eu/wp-content/uploads/2022/10/OneNet_957739_D5_8_v1_final.pdf
- [51] opengovdata.org webpage: Principles of open government data. <https://opengovdata.org/>
- [52] Otto, B.; Steinbuss, S.; Teuscher, A.; Lohmann, S. et al. (2019). IDS Reference Architecture Model (Version 3.0). International Data Spaces Association. <http://doi.org/10.5281/zenodo.5105529>

- [53] Panian, Z. (2010). Some Practical Experiences in Data Governance. Published in World Academy of Science, Engineering and Technology 62 2010.
<https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.190.6948&rep=rep1&type=pdf>
- [54] PM² Alliance, 2020. Requirements Management Plan. https://www.pm2alliance.eu/wp-content/uploads/2020/11/11.I.PM2-Template.v3.Requirements_Management_Plan.ProjectName.dd-mm-yyyy.vx..x.docx
- [55] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act).
<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R0868&from=EN>
- [56] SAP webpage: What is data governance? <https://www.sap.com/insights/what-is-data-governance.html>
- [57] Schütz, J.; Uslar, M.; Meister, J. (2021). A case study research on interoperability improvement in Smart Grids: state-of-the-art and further opportunities. <https://open-research-europe.ec.europa.eu/articles/1-33>
- [58] SmartEn (2021). Setting a digital strategy for a cost-effective decarbonisation of the energy system.
<https://smarten.eu/wp-content/uploads/2021/11/Setting-a-digital-strategy-for-a-cost-effective-decarbonisation-of-the-energy-system.pdf>
- [59] Tallinn Declaration on e-Government, 2017.
<https://ec.europa.eu/newsroom/dae/redirection/document/47559>
- [60] Tauberer, J. (2014). Open Government Data (The Book). Second Edition. <https://opengovdata.io/>
- [61] Thomas, G. The DGI Data Governance DGI Data Governance Framework.
https://datagovernance.com/wp-content/uploads/2020/07/dgi_data_governance_framework.pdf
- [62] Thomas, G. (2006). Alpha Males and Data Disaster. Published by Brass Cannon Press.

Appendix A Survey responses from existing data exchange initiatives

A.1 Survey Responses - CoordiNet Platform

Topic	Response
<p>Data access and storage</p> <p>Specify the strategy for data management (whether a shared/central storage for data is used or message-based integration of remote systems – distributed/decentralised approach).</p>	<p>Both ways, depending on the coordination schemes.</p> <p>There are several possible communications:</p> <ul style="list-style-type: none"> • (Common) CoordiNet Platform • Local CoordiNet platform • FSP to SOs directly • FSP, SOs to the Market platform
<p>Flow of data (end-to-end/end-to-platform)</p> <p>In the case of end-to-end approach, please specify the entity pairs that exchange information. Otherwise, specify the entities that connect to the platform.</p>	<ul style="list-style-type: none"> • End-to-Platform: <ul style="list-style-type: none"> ○ DSOs – CoordiNet/local CoordiNet platform: bidirectional communication ○ TSO - CoordiNet platform: bidirectional communication ○ Small FSPs - Local CoordiNet platform: bidirectional communication ○ CP – FSP: The FSP is only a receiver here • End-to-End: <ul style="list-style-type: none"> ○ FSPs – SOs: Bidirectional ○ SFSPs – DSO: The SFSP sends info to the DSO ○ TSO- Market Operator: Bidirectional ○ DSO/Regional DSO – Market Operator: Bidirectional ○ Regional DSO – Consumer: DSO send to consumer info ○ DSO- Market Platform ○ FSP Market Platform <p>More info in CoordiNet D2.4 (2021 [12])</p>
<p>Data portability</p> <ol style="list-style-type: none"> 1. How do entities connect to the framework/platform/interface? (e.g.: plug-and-play APIs, software connectors, etc.) 2. Which compatibility and interoperability mechanisms are used in the transactions? (standards, data models, data format, ontologies) 	<ol style="list-style-type: none"> 1. Platforms and interfaces 2. Interfaces based on IEC standards (CIM, 61850)
<p>Identification/registration mechanisms of the participants</p> <p>Which mechanisms (either automated or manual) are used to manage data participants in the framework/platform/interface? (e.g.: user registries, certification, identity provisioning). Including who bears the responsibility for managing the above-mentioned mechanisms.</p>	<p>-</p>

<p>Data ownership</p> <p>Detail which are the individual data usage policies that data owners can use to exert their rights over the data they provide (once only data provision/access, release/blocking of data for certain users).</p>		Table 5: Exemplary RBAC for platform use																																		
		<table><tr><th>ACTOR GROUPING</th><th>ACTOR NAME</th><th>ROLE NAME</th><th>DESCRIPTION</th></tr><tr><td>Business Actor</td><td>Platform Administrator</td><td>System Administrator</td><td rowspan="2">In this example, the System Administrator has the role of a System Administrator and has all rights to modify the platform as well as to manage the data on the platform. Here, for example, the DSO and the Platform Administrator are the System Administrators.</td></tr><tr><td>Business Actor</td><td>Distribution System Operator</td><td>System Administrator</td></tr><tr><td>Business Actor</td><td>Transmission System Operator</td><td>External Project User</td><td rowspan="5">In this example, the role of External Project Users have the right to operate specific functions of the data exchange platform. The External Project User, such as in this example the TSO, Flexibility Operator, Supplier, Market Aggregator and the Smart Meter are able to interact with each other and are able to download/reuse uploaded data.</td></tr><tr><td>External Component</td><td>Smart Meter</td><td>External Project User</td></tr><tr><td>Business Actor</td><td>Flexibility Operator</td><td>External Project User</td></tr><tr><td>Business Actor</td><td>Supplier</td><td>External Project User</td></tr><tr><td>Business Actor</td><td>Market Aggregator</td><td>External Project User</td></tr><tr><td>Business Actor</td><td>Significant grid user (e. g. producer, active consumer etc.)</td><td>External Project Consumer</td><td>External Projects Consumer have the fewest rights than other actors. Therefore, consumers should be able to read and see different data, but they could have less rights in modifying data.</td></tr></table>				ACTOR GROUPING	ACTOR NAME	ROLE NAME	DESCRIPTION	Business Actor	Platform Administrator	System Administrator	In this example, the System Administrator has the role of a System Administrator and has all rights to modify the platform as well as to manage the data on the platform. Here, for example, the DSO and the Platform Administrator are the System Administrators.	Business Actor	Distribution System Operator	System Administrator	Business Actor	Transmission System Operator	External Project User	In this example, the role of External Project Users have the right to operate specific functions of the data exchange platform. The External Project User, such as in this example the TSO, Flexibility Operator, Supplier, Market Aggregator and the Smart Meter are able to interact with each other and are able to download/reuse uploaded data.	External Component	Smart Meter	External Project User	Business Actor	Flexibility Operator	External Project User	Business Actor	Supplier	External Project User	Business Actor	Market Aggregator	External Project User	Business Actor	Significant grid user (e. g. producer, active consumer etc.)	External Project Consumer	External Projects Consumer have the fewest rights than other actors. Therefore, consumers should be able to read and see different data, but they could have less rights in modifying data.
		ACTOR GROUPING	ACTOR NAME	ROLE NAME	DESCRIPTION																															
		Business Actor	Platform Administrator	System Administrator	In this example, the System Administrator has the role of a System Administrator and has all rights to modify the platform as well as to manage the data on the platform. Here, for example, the DSO and the Platform Administrator are the System Administrators.																															
		Business Actor	Distribution System Operator	System Administrator																																
		Business Actor	Transmission System Operator	External Project User	In this example, the role of External Project Users have the right to operate specific functions of the data exchange platform. The External Project User, such as in this example the TSO, Flexibility Operator, Supplier, Market Aggregator and the Smart Meter are able to interact with each other and are able to download/reuse uploaded data.																															
		External Component	Smart Meter	External Project User																																
		Business Actor	Flexibility Operator	External Project User																																
		Business Actor	Supplier	External Project User																																
		Business Actor	Market Aggregator	External Project User																																
Business Actor	Significant grid user (e. g. producer, active consumer etc.)	External Project Consumer	External Projects Consumer have the fewest rights than other actors. Therefore, consumers should be able to read and see different data, but they could have less rights in modifying data.																																	
Three different rights were elaborated:																																				
(R) - the user could use the right to read on the platform. This means that the user is only able to read data that is open for reading.																																				
(W) the user can write on the platform and is able to create new information, as well as delete this data or information.																																				
(M)- the user could be also able to manage the data, which means that the user is able to manage data and information on the platform.																																				
More info in CoordiNet D2.6 (2022 [13])																																				
Consent management	Portability of consents (e.g., Sharing consents between countries)	Above																																		
	“Reuse” of data which was not the original purpose for granting the access	Above																																		
	Representation right	Above																																		
Logging What information is logged, where is it logged, by whom and during how much time is it kept? (e.g.: transaction metadata logging, entire transaction logging, participants logging)		More info in CoordiNet D2.6 (2022 [13])																																		
Licensing Are there any licensed components? Please specify accordingly (e.g.: open-source licenses – Apache, MIT, etc.; closed sourced licenses)		-																																		
Ownership and Maintenance		-																																		

Is there (or is it foreseen) any responsible party for running and maintaining the solution) that are part of the framework?

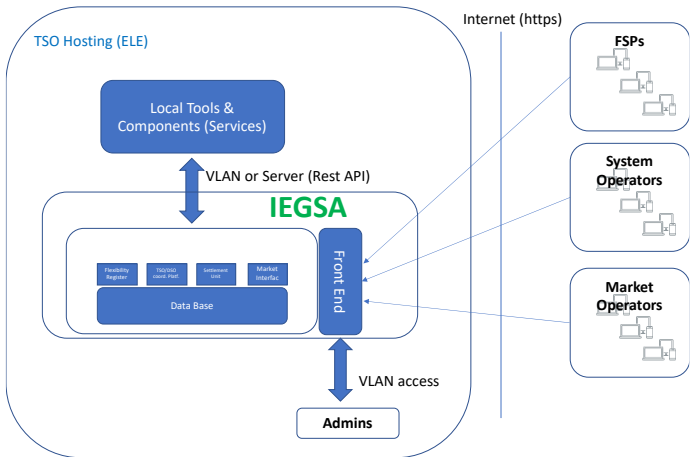
A.2 Survey Responses - ECCo SP

Topic		Response
Data access and storage Specify the strategy for data management (whether a shared/central storage for data is used or message-based integration of remote systems – distributed/decentralised approach).		ECCo SP is a message-based integration of remote systems, the purpose of the SW is not data storage, but to exchange data instead. It is both centralised (broker and component directory) and distributed between the actors.
Flow of data (end-to-end/end-to-platform) In the case of end-to-end approach, please specify the entity pairs that exchange information. Otherwise, specify the entities that connect to the platform.		ECCo SP has no platform with business application purpose, it is only a data exchange tool. The ECP Endpoint and EDX toolbox are the entities that connect to the platform, which communicates to the client.
Data portability 1. How do entities connect to the framework/platform/interface? (e.g.: plug-and-play APIs, software connectors, etc.) 2. Which compatibility and interoperability mechanisms are used in the transactions? (standards, data models, data format, ontologies)		1. APIs 2. Standard (based on MADES 62325-351).
Identification/registration mechanisms of the participants Which mechanisms (either automated or manual) are used to manage data participants in the framework/platform/interface? (e.g.: user registries, certification, identity provisioning). Including who bears the responsibility for managing the above-mentioned mechanisms.		The ECCo SP is not a business application, but a data exchange application. Thus, there is no participant identification nor registration. The ECP client needs to register the ECP Component Directory to be allowed to exchange data from ECP network. The EDX toolbox must be registered in the EDX service catalogue. The responsibility for managing user registration and certification is from the project manager making use of ECCo SP to exchange the data (component directory administrator).
Data ownership Detail which are the individual data usage policies that data owners can use to exert their rights over the data they provide (once only data provision/access, release/blocking of data for certain users).		During the registration of the endpoint, you are requested to accept the GDPR rules for the collected data such as name, email, phone number and organisation. Then it is connected.
Consent management	Portability of consents (e.g., Sharing consents between countries)	Consent management for ECCo SP is done by the TSOs.

	“Reuse” of data which was not the original purpose for granting the access	
	Representation right	
Logging What information is logged, where is it logged, by whom and during how much time is it kept? (e.g.: transaction metadata logging, entire transaction logging, participants logging)		Refer to the attached excel files: ECP AuditLog and EDX AuditLog. It is stored locally by default for seven days.
Licensing Are there any licensed components? Please specify accordingly (e.g.: open-source licenses – Apache, MIT, etc.; closed sourced licenses)		Yes. The licensing terms are attached. This product includes software developed by the Apache Software Foundation (http://www.apache.org/) and the following third-party components: <ul style="list-style-type: none"> • Apache tomcat (http://tomcat.apache.org/) • ActiveMQ (http://activemq.apache.org/) • Qpid JMS (http://qpid.apache.org/components/jms/) • Apache Camel (http://camel.apache.org/) • Spring Framework (https://spring.io/projects/spring-framework/) • Apache OpenJPA (http://openjpa.apache.org/) • AngularJS (https://angularjs.org/) • Liquibase (http://www.liquibase.org/)
Ownership and Maintenance Is there (or is it foreseen) any responsible party for running and maintaining the solution) that are part of the framework?		Yes, ENTSO-E is the owner and responsible for maintaining of the ECCo SP tool.

A.3 Survey Responses - IEGSA

Topic	Response
Data access and storage Specify the strategy for data management (whether a shared/central storage for data is used or message-based integration of remote systems – distributed/decentralised approach).	There is a central data-sink. Yet, there are different User Interface environments (Flexibility Register, TSO/DSO Coordination Platform) that can be accessed based on Role-Based-Access-Control (RBAC) mechanism. This is “a policy neutral access control mechanism defined around roles and privileges” as security model, which means that users can be assigned one or more roles governing what each INTERFACE stakeholder is allowed to access, modify, and execute.
Flow of data (end-to-end/end-to-platform) In the case of end-to-end approach, please specify the entity pairs that exchange information. Otherwise, specify the entities that connect to the platform.	<p>FSP -> IEGSA (UI) for resource registration, resource group creation (portfolio management), overview of bids per MTU/product, trades overview, get settlement results</p> <p>FSP -> IEGSA (API) for uploading measurements for settlement</p> <p>Market Operator -> IEGSA (UI) product qualification, assess product requests</p> <p>TSO/DSO -> IEGSA (UI) resource/resource groups preview, merit order list (perform activations), trades</p> <p>IEGSA <-> marketplace (API) to obtain bids, to send merit order list</p>

<p>Data portability</p> <ol style="list-style-type: none"> How do entities connect to the framework/platform/interface? (e.g.: plug-and-play APIs, software connectors, etc.) Which compatibility and interoperability mechanisms are used in the transactions? (standards, data models, data format, ontologies) 	<ol style="list-style-type: none"> Both APIs and User Interface are used as described above. CIM ESMP profiles are used for all flexibility bidding, trading, activation and settlement processes. 						
<p>Identification/registration mechanisms of the participants</p> <p>Which mechanisms (either automated or manual) are used to manage data participants in the framework/platform/interface? (e.g.: user registries, certification, identity provisioning). Including who bears the responsibility for managing the above-mentioned mechanisms.</p>	<p>The first IEGSA release implements User Authentication through JSON Web Tokens (JWT). As such, user information is entered and administered within IEGSA and each user has to be created by the system administrator.</p> <p>Future releases of IEGSA are intended to integrate an OAuth service in order to facilitate access for registered users in other (relevant) systems.</p>  <p>Figure 1: Typical IEGSA deployment installation</p>						
<p>Data ownership</p> <p>Detail which are the individual data usage policies that data owners can use to exert their rights over the data they provide (once only data provision/access, release/blocking of data for certain users).</p>	<p>Access only to specific <u>metadata</u>, relies on RBAC mechanism as explained above earlier.</p>						
<p>Consent management</p>	<table> <tr> <td>Portability of consents (e.g., Sharing consents between countries)</td><td>IEGSA integrated with Estfeed datahub fetch consents. In case no integration with data hub, FSP was asked if there is proper legitimacy to represent resources.</td></tr> <tr> <td>“Reuse” of data which was not the original purpose for granting the access</td><td>Authorisation for publishing/viewing metadata of resource to system operators was a question posed upon each resource registration.</td></tr> <tr> <td>Representation right</td><td>-</td></tr> </table>	Portability of consents (e.g., Sharing consents between countries)	IEGSA integrated with Estfeed datahub fetch consents. In case no integration with data hub, FSP was asked if there is proper legitimacy to represent resources.	“Reuse” of data which was not the original purpose for granting the access	Authorisation for publishing/viewing metadata of resource to system operators was a question posed upon each resource registration.	Representation right	-
Portability of consents (e.g., Sharing consents between countries)	IEGSA integrated with Estfeed datahub fetch consents. In case no integration with data hub, FSP was asked if there is proper legitimacy to represent resources.						
“Reuse” of data which was not the original purpose for granting the access	Authorisation for publishing/viewing metadata of resource to system operators was a question posed upon each resource registration.						
Representation right	-						

Logging What information is logged, where is it logged, by whom and during how much time is it kept? (e.g.: transaction metadata logging, entire transaction logging, participants logging)	Entire transaction logging for all process is developed at IEGSA platform. Specific notifications are also developed to ease the different operation and keep track of most important events/requests.
Licensing Are there any licensed components? Please specify accordingly (e.g.: open-source licenses – Apache, MIT, etc.; closed sourced licenses)	Usage of open-source tools, thus no special licenses are required.
Ownership and Maintenance Is there (or is it foreseen) any responsible party for running and maintaining the solution) that are part of the framework?	-

A.4 Survey Responses - Estfeed

Topic	Response
Data access and storage Specify the strategy for data management (whether a shared/central storage for data is used or message-based integration of remote systems – distributed/decentralised approach).	The current Estfeed platform enabling message-based distributed data exchange will be phased out within a couple of years and only the Estfeed data hub will remain in place. This is the central storage of electricity and gas metering data, other types of energy metering data (district heating) may be added in the future. Data can be accessed using a request method.
Flow of data (end-to-end/end-to-platform) In the case of end-to-end approach, please specify the entity pairs that exchange information. Otherwise, specify the entities that connect to the platform.	Direct integration (i.e., contract with platform, data user's confirmation to respect GDPR, data access right may be based on contract with the consumer) is to be enabled for energy service providers, suppliers, SOs, generators, BRPs, charging station operators. Any other person can have access based on explicit consent, via API and GUI. Representation rights only via GUI.
Data portability 1. How do entities connect to the framework/platform/interface? (e.g.: plug-and-play APIs, software connectors, etc.) 2. Which compatibility and interoperability mechanisms are used in the transactions? (standards, data models, data format, ontologies)	<ul style="list-style-type: none"> • GUI, RESTful API • JSON for data format
Identification/registration mechanisms of the participants Which mechanisms (either automated or manual) are used to manage data participants in the framework/platform/interface? (e.g.: user registries, certification, identity provisioning). Including who	Suppliers and SOs must be registered in national economic activity register. Not decided yet whether this will be required from energy service providers.

bears the responsibility for managing the above-mentioned mechanisms.		
Data ownership Detail which are the individual data usage policies that data owners can use to exert their rights over the data they provide (once only data provision/access, release/blocking of data for certain users).		Estfeed holds hourly data (corresponding to settlement period) from all electricity and gas metering points in Estonia. Based on consent the consumers/prosumers/generators can provide access to data to any natural or legal person. Based on the representation rights access can be granted to any natural person.
Consent management	Portability of consents (e.g., Sharing consents between countries)	Implicit consents can be given to domestic and foreign suppliers based on the predefined list and such suppliers can have access to data via API. While such lists are not available for other types of stakeholders, giving consents to non-residents (i.e., persons not having Estonian ID, SmartID) is currently not enabled.
	“Reuse” of data which was not the original purpose for granting the access	Reuse of private data seems to be complicated.
	Representation right	Representation rights can be given to natural persons, but only via GUI and currently access to non-residents (i.e., persons not having Estonian ID, SmartID) is not supported.
Logging What information is logged, where is it logged, by whom and during how much time is it kept? (e.g.: transaction metadata logging, entire transaction logging, participants logging)		Data owners (consumers) should have access to the logging information about the users of their data (who, when, which data).
Licensing Are there any licensed components? Please specify accordingly (e.g.: open-source licenses – Apache, MIT, etc.; closed sourced licenses)		There could be many licenced components the solution has been built on.
Ownership and Maintenance Is there (or is it foreseen) any responsible party for running and maintaining the solution) that are part of the framework?		Elering as TSO is the owner. Maintenance is provided by external contractor.

A.5 Survey Responses - Platone

Topic	Response
Data access and storage Specify the strategy for data management (whether a shared/central storage for data is used or message-based integration of remote systems – distributed/decentralised approach).	The Market Data are stored in the Market Platform and available to all the Market Participants (DSOs, TSOs, Aggregators) based on their identity and ownership. Each data stored is also registered in blockchain infrastructure for ensuring trustworthiness and transparency between the participants.
Flow of data (end-to-end/end-to-platform) In the case of end-to-end approach, please specify the entity pairs that exchange information. Otherwise, specify the entities that connect to the platform.	DSO Platform -> Market Platform (Flexibility Requests) Aggregator Platform -> Market Platform (Flexibility Offers) TSO Simulator -> Market Platform (Flexibility Requests)

		<p>Shared Customer Database -> Market Platform (Baseline and Measurements)</p> <p>Market Platform -> Market Participants (DSOs, TSOs, Aggregators) (Market Results)</p>
<p>Data portability</p> <ol style="list-style-type: none"> How do entities connect to the framework/platform/interface? (e.g.: plug-and-play APIs, software connectors, etc.) Which compatibility and interoperability mechanisms are used in the transactions? (standards, data models, data format, ontologies) 		<p>The Market Platform provides two types of connection mechanisms: Message Broker (Apache Kafka) and REST APIs.</p> <p>The data models used in the data transactions are developed within the Platone Project and not standard ones. Ontologies are not foreseen.</p>
<p>Identification/registration mechanisms of the participants</p> <p>Which mechanisms (either automated or manual) are used to manage data participants in the framework/platform/interface? (e.g.: user registries, certification, identity provisioning). Including who bears the responsibility for managing the above-mentioned mechanisms.</p>		<p>All the Actors are identified using OAuth2.0 Credentials (for REST APIs) and Client certification (for Message Broker) for ensuring secure access on the identity management. All the mechanisms are managed by the Market Platform.</p>
<p>Data ownership</p> <p>Detail which are the individual data usage policies that data owners can use to exert their rights over the data they provide (once only data provision/access, release/blocking of data for certain users).</p>		<p>At the moment there are not data access policies defined.</p>
Consent management	Portability of consents (e.g., Sharing consents between countries)	At the moment there is not a consent management mechanism implemented
	"Reuse" of data which was not the original purpose for granting the access	At the moment there is not a consent management mechanism implemented
	Representation right	At the moment there is not a consent management mechanism implemented
<p>Logging</p> <p>What information is logged, where is it logged, by whom and during how much time is it kept? (e.g.: transaction metadata logging, entire transaction logging, participants logging)</p>		<p>All the data transactions are registered on the blockchain layer and associated with its own provider.</p>
<p>Licensing</p> <p>Are there any licensed components? Please specify accordingly (e.g.: open-source licenses – Apache, MIT, etc.; closed sourced licenses)</p>		<p>The Market Platform has an open-source license (MIT).</p>
<p>Ownership and Maintenance</p>		<p>ENG is responsible of the platform and will maintain it for the duration of the project (until September 2023).</p>

Is there (or is it foreseen) any responsible party for running and maintaining the solution) that are part of the framework?

A.6 Survey Responses - SYNERGY

Topic	Response
<p>Data access and storage</p> <p>Specify the strategy for data management (whether a shared/central storage for data is used or message-based integration of remote systems – distributed/decentralised approach).</p>	<p>Within SYNERGY different storage modalities are utilised depending on the nature of the data (i.e., datasets, analytics models, analytics results and reports along with their metadata). Nevertheless, all storage modalities reside on the core cloud-based layer of the platform hence the shared/central storage approach is adopted. In addition to this, SYNERGY offers the option of the encryption of proprietary datasets while the access to them is regulated by an ABAC-based access control mechanism.</p>
<p>Flow of data (end-to-end/end-to-platform)</p> <p>In the case of end-to-end approach, please specify the entity pairs that exchange information. Otherwise, specify the entities that connect to the platform.</p>	<p>SYNERGY follows a multiple-layer architecture approach where the 3 main layers (and the components residing within each layer) intercommunicate through secure tokens and decryption keys in the case of encrypted data exchange. External applications can connect and consume the exposed services via an API Gateway with the use of API keys.</p>
<p>Data portability</p> <ol style="list-style-type: none"> 1. How do entities connect to the framework/platform/interface? (e.g.: plug-and-play APIs, software connectors, etc.) 2. Which compatibility and interoperability mechanisms are used in the transactions? (standards, data models, data format, ontologies) 	<p>External entities in SYNERGY are considered as Energy Applications that consume data, initiate the execution of the designed in the platform analytics pipelines and retrieve analytics results. All applications connect with the platform via the API Gateway through which they utilise the Open APIs of SYNERGY.</p> <p>All datasets are harmonised and stored in accordance to the SYNERGY Common Information (which is composed by various well-established energy data models and standards).</p>
<p>Identification/registration mechanisms of the participants</p> <p>Which mechanisms (either automated or manual) are used to manage data participants in the framework/platform/interface? (e.g.: user registries, certification, identity provisioning). Including who bears the responsibility for managing the above-mentioned mechanisms.</p>	<p>SYNERGY platform provides the single identity provider, as well as the authentication and authorisation mechanism of the platform. Within SYNERGY, the users are organised under the concept of the organisations. The organisation's manager (who is also the organisation's legal representative) initiates the organisation's registration to the platform. Upon the review and approval from the platform's administrator, the organisation's manager is able to invite new users to the organisation. Using the invitation token (received via email) the users are able to complete their registration.</p>
<p>Data ownership</p> <p>Detail which are the individual data usage policies that data owners can use to exert their rights over the data they provide (once only data provision/access, release/blocking of data for certain users).</p>	<p>Each data provider can define the appropriate license and IPR details for each dataset that he/she provides. The platform enables the drafting of custom licenses that correspond to the specific needs of a data provider while supporting the usage of predefined license templates based on well-established licenses. Data providers are able to set the preferred access</p>

		<p>policies in an ABAC-based manner that regulate the access to their data in conjunction with the defined licenses.</p>
Consent management	Portability of consents (e.g., Sharing consents between countries)	Not applicable.
	“Reuse” of data which was not the original purpose for granting the access	<p>The platform does not access data. Within SYNERGY data sharing between the organisations is performed through the provided marketplace. It provides the functionalities around initiating a data asset acquisition process, accepting/ denying such requests, drafting, negotiating over, and signing data sharing contracts among the involved parties where the exact terms of the “reuse” of data are defined.</p>
	Representation right	Not applicable.
Logging What information is logged, where is it logged, by whom and during how much time is it kept? (e.g.: transaction metadata logging, entire transaction logging, participants logging)		<p>Within SYNERGY, the minimum required information is logged. This includes all the CRUD operations that are performed on the datasets via the corresponding metadata update operations. Most of the information that is logged is on an organisation level and a small portion on a user level.</p>
Licensing Are there any licensed components? Please specify accordingly (e.g.: open-source licenses – Apache, MIT, etc.; closed sourced licenses)		<p>All developed components have closed sourced licenses.</p>
Ownership and Maintenance Is there (or is it foreseen) any responsible party for running and maintaining the solution) that are part of the framework?		<p>No yet at this stage of the project.</p>

A.7 Survey Responses – EUniversal

Topic	Response
Data access and storage Specify the strategy for data management (whether a shared/central storage for data is used or message-based integration of remote systems – distributed/decentralised approach).	<p>A distributed approach is considered, meaning that each entity that receive data has its own data storage.</p>
Flow of data (end-to-end/end-to-platform) In the case of end-to-end approach, please specify the entity pairs that exchange information. Otherwise, specify the entities that connect to the platform.	<p>An end-to-end approach is considered in this project:</p> <p>End-to-End:</p> <ul style="list-style-type: none"> ○ DSOs – FSPs ○ DSO – Flexibility Market Operator ○ FSP – Flexibility Market Operator <p>Relevant Deliverable: EUniversal D2.2 (2021)</p>
Data portability 5. How do entities connect to the framework/platform/interface? (e.g.: plug-and-play APIs, software connectors, etc.)	<p>1. UMEI - Universal Market Enabler Interface (implementation of a standard, agnostic, adaptable, and modular combination of different APIs to link DSOs and market parties with flexibility market platforms, in coordination with other flexibility users.)</p>

<p>6. Which compatibility and interoperability mechanisms are used in the transactions? (standards, data models, data format, ontologies)</p>	<p>2. The aim is to take into account parameters such as the preparedness of the DSOs to implement the solutions developed, the specific characteristics and requirements of the EUniversal project and the existing landscape, by reaching easy to implement data profiles agreed between multiple market operators, DSOs and FSPs.</p>
<p>Identification/registration mechanisms of the participants</p> <p>Which mechanisms (either automated or manual) are used to manage data participants in the framework/platform/interface? (e.g.: user registries, certification, identity provisioning). Including who bears the responsibility for managing the above-mentioned mechanisms.</p>	<p>Each entity is responsible for its own identification/registration mechanisms. Guidelines are proposed to harmonise this process, however, they are optional.</p>
<p>Data ownership</p> <p>Detail which are the individual data usage policies that data owners can use to exert their rights over the data they provide (once only data provision/access, release/blocking of data for certain users).</p>	<p>As this is a distributed (end to end) communication mechanism, each party is responsible for making sure that the right procedures are followed, namely regarding sensitive/third party data handling.</p>
<p>Consent management</p>	<p>Portability of consents (e.g., Sharing consents between countries)</p> <p>Not applicable</p>
	<p>“Reuse” of data which was not the original purpose for granting the access</p> <p>Not applicable</p>
	<p>Representation right</p> <p>Not applicable</p>
<p>Logging</p> <p>What information is logged, where is it logged, by whom and during how much time is it kept? (e.g.: transaction metadata logging, entire transaction logging, participants logging)</p>	<p>There’s no logged information apart from possible internal registries conducted by each participant.</p>
<p>Licensing</p> <p>Are there any licensed components? Please specify accordingly (e.g.: open-source licenses – Apache, MIT, etc.; closed sourced licenses)</p>	<p>Open-Source</p>
<p>Ownership and Maintenance</p> <p>Is there (or is it foreseen) any responsible party for running and maintaining the solution) that are part of the framework?</p>	<p>Ownership – Not applicable Maintenance – The EUniversal consortium during project duration, pending decision on a later exploitation analysis after the project end.</p>

Appendix B Data governance survey template

Governance element	Relevance, positive impact from 1 to 5: 1 (very low impact) ... 5 (very high impact)	Feasibility, risks from 1 to 5: 1 (non-feasible) ... 5 (easily feasible)	Actual implementation in project from 1 to 5: 1 (not applied at all) ... 5 (fully applied)
1. DATA GOVERNANCE BUSINESS CASE			
REQUIREMENT 1.1. Define business case for data governance* on relevant level [project / organisation / country / EU], e.g. by means of business model canvas or standardised IEC 62559-2 template.			
* Data governance as a business programme has its own objectives, responsibilities, processes, KPIs, costs & benefits etc., with the aim to organise data management effectively.			
EXPLAIN YOUR ANSWER (OPTIONAL):			
REQUIREMENT 1.2. Evaluate regularly the risks associated to the implementation of data governance programme using risk assessment methodologies.			
EXPLAIN YOUR ANSWER (OPTIONAL):			
REQUIREMENT 1.3. Define and follow the principles of data-as-an-asset*.			
* Data-as-an-asset means that quality of data is considered equally important with the quality of any other asset of the organisation – data should be accurate, data should have real value, data risks should be addressed, data misuse should be avoided etc.			
EXPLAIN YOUR ANSWER (OPTIONAL):			
REQUIREMENT 1.4. Define and monitor KPIs for data governance programme itself and for specific data exchanges.			
EXPLAIN YOUR ANSWER (OPTIONAL):			
2. ORCHESTRATED DATA GOVERNANCE			
REQUIREMENT 2.1. Establish a group to steer the European Energy Data Space, open to European initiatives and stakeholders to participate, and ultimately leading to cooperation between energy and other sectors.			
EXPLAIN YOUR ANSWER (OPTIONAL):			
REQUIREMENT 2.2. Define the responsibilities and accountability* for European data exchange, including European Commission, Member states, data providers, data users, etc.			
* Clarity about the actors and their responsibilities in data exchanges, especially outside the individual organisation and including cross-border data exchange.			
EXPLAIN YOUR ANSWER (OPTIONAL):			

3. RULES AND NORMS			
REQUIREMENT 3.1. Propose and promote regulations and standards facilitating improved data governance.			
EXPLAIN YOUR ANSWER (OPTIONAL):			
REQUIREMENT 3.2. Understand regulatory and standards' requirements driving the need for proper data governance.			
EXPLAIN YOUR ANSWER (OPTIONAL):			
4. DATA OWNERSHIP GOVERNANCE			
REQUIREMENT 4.1. Ensure consent management process* which is accessible to any party willing to provide or use any data and not limited to single country.			
<i>* A process enabling the data owners to grant access to their private data for other parties, including cross-border.</i>			
EXPLAIN YOUR ANSWER (OPTIONAL):			
5. DATA ACCESS GOVERNANCE			
REQUIREMENT 5.1. Ensure the availability of one-stop-shop* providing information about and access guidance to different types of data.			
<i>* One-stop-shop can be provided, for example, by the national regulator, containing information about where and how to access different data.</i>			
EXPLAIN YOUR ANSWER (OPTIONAL):			
REQUIREMENT 5.2. Make available single data access points* and ensure everyone's rights to access data.			
<i>* Single data access point means a gate where several types of data can be provided and obtained, no need for data providers and data users to be aware of multiple gates.</i>			
EXPLAIN YOUR ANSWER (OPTIONAL):			
REQUIREMENT 5.3. Ensure legislative grounds for sub-meter and other end-customer related data** governance.			
<i>* Sub-meter data are the measurements behind the main meter, e.g., on the level of individual heat pump. ** Other end-customer data includes, for example, information about their flexible resources.</i>			
EXPLAIN YOUR ANSWER (OPTIONAL):			
6. DATA SECURITY GOVERNANCE			
REQUIREMENT 6.1. Apply "know-your-data-user" principle by making data usage information* available to data owners easily and free of charge.			
<i>* Information for private data owners about who, when and why has accessed their data.</i>			
EXPLAIN YOUR ANSWER (OPTIONAL):			
REQUIREMENT 6.2. Harmonise authentication schemes across Europe and sectors.			
EXPLAIN YOUR ANSWER (OPTIONAL):			

7. DATA VOCABULARY GOVERNANCE			
REQUIREMENT 7.1. In data modelling, follow the generally recognised reference models for roles, information and processes.			
EXPLAIN YOUR ANSWER (OPTIONAL):			
REQUIREMENT 7.2. Establish European arrangement for coordinating reference models and national mappings*.			
<i>* National mapping means the comparison of national data exchange practice with the generally accepted reference model (consisting of role model, information model, process model).</i>			
EXPLAIN YOUR ANSWER (OPTIONAL):			
8. DATA PLATFORMS			
REQUIREMENT 8.1. Make efforts and demonstrate the interoperability of a data platform with other European data platforms.			
EXPLAIN YOUR ANSWER (OPTIONAL):			
REQUIREMENT 8.2. Call the common European (Energy) data space to keep the registry of and to issue compliance labels to interoperable data platforms.			
EXPLAIN YOUR ANSWER (OPTIONAL):			
9. INTERFACES			
REQUIREMENT 9.1. Make available interfaces – Application Programming Interfaces and Graphical User Interfaces – of the data platform.			
EXPLAIN YOUR ANSWER (OPTIONAL):			
REQUIREMENT 9.2. Provide unified European wide guidance for integrating with any of the European data platform for developers, data intermediaries, data providers and data users, regardless of their physical location and data type.			
EXPLAIN YOUR ANSWER (OPTIONAL):			
10. REPOSITORIES			
REQUIREMENT 10.1. Create common European data repositories at least for cross-sector data roles, data types (objects, profiles) and processes (use cases).			
EXPLAIN YOUR ANSWER (OPTIONAL):			
REQUIREMENT 10.2. Make the common European data repositories available free of charge.			
EXPLAIN YOUR ANSWER (OPTIONAL):			

Appendix C Appendix C: Governance Requirements Traceability Matrix (GRTM)

The following matrices present the analytical GRTMs analysing all OneNet GFRs.

ID	GFR01
Name	Configuration of OneNet Connector: Configure data format/ semantic annotation
Status	Validated
Priority	High
Comments	OneNet Participants have to be able to select the data formats and configure semantic annotation to be applied by the OneNet Connector so that data is harmonised (via OneNet Connector GUI).
Governance dimension	Standardisation, Integrity
Derived From	D6.1

ID	GFR02
Name	Configuration of OneNet Connector: Configure data quality
Status	Incorporated
Priority	High
Comments	OneNet Participants have to be able to select and configure data quality requirements and data quality checks to be applied by the OneNet Connector on outgoing data (via OneNet Connector dashboard).
Governance dimension	Integrity
Derived From	D6.1

ID	GFR03
Name	Configuration of OneNet Connector: Configuration of transaction logging
Status	Implemented
Priority	High
Comments	OneNet Participants have to be able to configure transaction logging (activate/ deactivate, logging intensity and details etc.) of the OneNet Connector (via OneNet Connector dashboard)
Governance dimension	Usage, Access
Derived From	D6.1

ID	GFR04
Name	Configuration of OneNet Connector: Configuration of data reception endpoints
Status	Validated
Priority	High
Comments	OneNet Participants have to be able to configure data reception endpoints in their systems/ platforms to subscribe themselves to the OneNet Connector context broker and receive incoming data in their systems
Governance dimension	Access
Derived From	D6.1
ID	GFR05

Name	ONBOARDING_Connector Configuration and Provisioning: Define connector configuration model- General information
Status	Validated
Priority	High
Comments	Service provider to define general information including connector type, version, timestamp of last change made to the configuration, configuration, name of contact person
Governance dimension	Access
Derived From	D6.1

ID	GFR06
Name	ONBOARDING_Connector Configuration and Provisioning: Define connector configuration model- Lifecycle- Data Flow
Status	Implemented
Priority	High
Comments	Service provider to define the configuration of tasks and connections established by the Data Router between the Data Services and the Data Bus (i.e., Networking: ports/IPs, for internal and external connections, Security: SSL certificates or public keys, Compliance /Data Sovereignty : rules before connector deployment (preventing incorrect configuration)
Governance dimension	Access
Derived From	D6.1

ID	GFR07
Name	Middleware Features: Available services and data sources discovery
Status	Validated
Priority	High
Comments	The middleware must allow to discovery for data sources
Governance dimension	Access/Usage
Derived From	D6.1

ID	GFR08
Name	Configuration of OneNet Connector: Configure data quality
Status	Incorporated
Priority	High
Comments	OneNet Participants have to be able to select and configure data quality requirements and data quality checks to be applied by the OneNet Connector on outgoing data (via OneNet Connector dashboard).
Governance dimension	Access
Derived From	D6.1

ID	GFR09
Name	Data exchange through REST APIs: Exchange harmonised payload data
Status	Validated
Priority	High
Comments	OneNet Participants have to be able to exchange harmonised payload data between OneNet Connectors using OneNet REST APIs
Governance dimension	Structure, Standardisation
Derived From	D6.1

ID	GFR10
Name	OneNet Participants have to be able to authenticate themselves/ their platform/ system for exchanges through the OneNet Middleware
Status	Validated
Priority	High
Comments	OneNet Participants have to be able to authenticate themselves/ their platform/ system for exchanges through the OneNet Middleware
Governance dimension	Access
Derived From	D6.1

ID	GFR11
Name	Data exchange through REST APIs: Data Retrieval
Status	Validated
Priority	High
Comments	OneNet Participants can retrieve data from a specific data source and filter it (e.g, time window)
Governance dimension	Access
Derived From	D6.1

ID	GFR12
Name	Middleware Features: Any Data sources is integrable with OneNet Middleware
Status	Validated
Priority	High
Comments	Allow data provider to make available a data source/entity within any data format/type (e.g., xml, json-ld, pdf).
Governance dimension	Structure, Standardisation
Derived From	D6.1

ID	GFR13
Name	Data Exchange: Publish Data
Status	Validated
Priority	High
Comments	Publish new data using the Connector, by posting metadata on the middleware instance
Governance dimension	Access, Usage
Derived From	D6.1

ID	GFR14
Name	Data Exchange: Subscribe as service consumer
Status	Validated
Priority	High
Comments	Register as consumer to a specific service, assuming a new service subscription upon acceptance by the service provider
Governance dimension	Access
Derived From	D6.1

ID	GFR15
Name	Data Exchange: Subscribe to a data source
Status	Validated
Priority	High
Comments	Register as consumer as subscriber (publish/subscribe mechanism)
Governance dimension	Access, Usage
Derived From	D6.1

ID	GFR16
Name	Monitor OneNet Connector status: Monitor network traffic
Status	Validated
Priority	High
Comments	OneNet Participants have to be able to monitor the network traffic between their own OneNet Connector and other OneNet Connectors and have to be notified about potential security breaches (metrics to be defined) through the OneNet Connector dashboard.
Governance dimension	Access
Derived From	D6.1

ID	GFR17
Name	Monitor OneNet Connector status: Monitor known data sources
Status	Validated
Priority	High
Comments	OneNet Participants have to be able to monitor the connected data sources (other OneNet Participants and their Connectors) and the current authentication and authorisation status through the OneNet Connector dashboard; sensitive information should only be exposed if a OneNet Participant agrees
Governance dimension	Access, Structure
Derived From	D6.1

ID	GFR18
Name	Monitor OneNet Connector status: Monitor transaction logs
Status	Validated
Priority	High
Comments	OneNet Participants have to be able to monitor the transaction logs through the OneNet Connector dashboard
Governance dimension	Access
Derived From	D6.1

ID	GFR19
Name	Monitor OneNet Connector status: Monitor results from data quality checks
Status	Specified
Priority	Medium
Comments	OneNet Participants have to be able to monitor results from data quality checks through the OneNet Connector dashboard.
Governance dimension	Integrity
Derived From	D6.1

ID	GFR20
Name	Registration and Configuration: Registering as OneNet Participant
Status	Validated
Priority	High
Comments	OneNet participant may register one or more users under the same connector allowing for its configuration as well.
Governance dimension	Access
Derived From	D6.1

ID	GFR21
Name	Registration and Configuration: Discovery/search data sources
Status	Validated
Priority	High
Comments	Data provider can register new data sources which are discoverable from data consumers that are registered under a specific service.
Governance dimension	Access, Structure
Derived From	D6.1

ID	GFR22
Name	IDS-based Service: Usage Control - Policy definition
Status	Validated (*with the inclusion of restricted service availability)
Priority	High
Comments	Data Provider is able to define policies for a specific data source
Governance dimension	Usage
Derived From	D6.1

ID	GFR23
Name	File Upload
Status	Validated
Priority	High
Comments	OneNet Participant are able to upload files and use them as data sources using the Connector GUI.
Governance dimension	Structure
Derived From	D6.1

ID	GFR24
Name	ONBOARDING_Security Setup: IDS Consumer/Provider configures data access restrictions
Status	Validated (*partially developed and validated, pricing options not available)
Priority	High
Comments	Connector provide appropriate functionality for Data Provider or Data Consumer to configure custom access restrictions for bilateral communications; The Data Provider may serve the same data using different representations or pricing options, so the Data Consumer may select a suitable offer from the Data Provider's Connector description.
Governance dimension	Usage, Access
Derived From	D6.1

ID	GFR25
Name	IDS-based Service: Clearing House
Status	Specified
Priority	High
Comments	All the data transactions are logged in based on IDS approaches.
Governance dimension	Access
Derived From	D6.1

ID	GFR26
Name	ONBOARDING_Connector Configuration and Provisioning: Define connector configuration model
Status	Specified
Priority	High
Comments	Connector communicates configuration to broker and/ or clearing house
Governance dimension	Access
Derived From	D6.1

ID	GFR27
Name	EXCHANGE OF DATA_Invoke Data Operation: Notification of data operation call at clearing House
Status	Specified
Priority	High
Comments	Upon data consumer request for data a notification is sent at clearing house for logging data operation request
Governance dimension	Access
Derived From	D6.1

ID	GFR28
Name	EXCHANGE OF DATA_Invoke Data Operation: Notification of data operation call reception at clearing House
Status	Specified
Priority	High
Comments	Upon data providers reception of data consumer's request, a notification is sent at clearing house for logging reception
Governance dimension	Access
Derived From	D6.1

ID	GFR29
Name	EXCHANGE OF DATA_Invoke Data Operation: Clearing house logs in a persistence database all transactions
Status	Specified
Priority	High
Comments	Clearing house logs in a persistence database all transactions ensuring data provenance tracking infrastructure
Governance dimension	Access
Derived From	D6.1

ID	GFR30
Name	EXCHANGE OF DATA_Invoke Data Operation: Notification of data operation result sent at clearing House
Status	Specified
Priority	High
Comments	Notification of data operation result sent at clearing House from data provider
Governance dimension	Access
Derived From	D6.1

ID	GFR31
Name	EXCHANGE OF DATA_Invoke Data Operation: Notification of data operation result received at clearing House
Status	Specified
Priority	High
Comments	Notification of data operation result received at clearing House
Governance dimension	Access
Derived From	D6.1

ID	GFR32
Name	ONBOARDING_Availability Setup: Broker provider functions for searching
Status	Validated
Priority	High
Comments	Broker provides functions for searching/browsing/querying for and retrieving registered Connector self-descriptions, including data sources, interfaces, security profiles, and current levels of trustworthiness.
Governance dimension	Access, Structure
Derived From	D6.1

ID	GFR33
Name	EXCHANGE OF DATA_Find Data Provider: Connector provides proper interface to find data provider
Status	Validated
Priority	High
Comments	Connector offers functionality to Data Consumer to be able to send a query
Governance dimension	Access
Derived From	D6.1

ID	GFR34
Name	Access OneNet Framework: Register or change data access consents
Status	Validated
Priority	High
Comments	OneNet Participants have to be able to register and change data access consents through accessing the OneNet Framework dashboard
Governance dimension	Usage
Derived From	D6.1

ID	GFR35
Name	IDS-based Service: Usage Control - Access Control and Enforcement
Status	Specified
Priority	High
Comments	Usage Control App verify all the policies during data exchange
Governance dimension	Usage
Derived From	D6.1

ID	GFR36
Name	Middleware Features: Data Quality Checking
Status	Validated
Priority	High
Comments	The middleware should include tool for data quality check
Governance dimension	Access
Derived From	D6.1

ID	GFR37
Name	OneNet Additional Services: Data Quality
Status	Validated
Priority	High
Comments	Implementing plug-in services for data quality checking
Governance dimension	Integrity
Derived From	D6.1

ID	GFR38
Name	Middleware Features: Development of semantic models
Status	Implemented
Priority	High
Comments	The Middleware should provide a semantic tool for the development of semantic models
Governance dimension	Standardisation
Derived From	D6.1

ID	GFR39
Name	OneNet Additional Services: Data Harmonisation
Status	Validated
Priority	High
Comments	OneNet Connector is able to map CIM Data models
Governance dimension	Standardisation
Derived From	D6.1

ID	GFR40
Name	EXCHANGE OF DATA_ Invoke Data Operation: Data consumer negotiate policy with data provider
Status	Specified
Priority	High
Comments	Data consumer to be able to negotiate with data providers sending counter offers for data usage policy
Governance dimension	Access
Derived From	D6.1

ID	GFR41
Name	Cybersecurity: Ensuring the security and privacy of data exchanged
Status	Specified
Priority	High
Comments	Data exchange shall concern cybersecurity governance aspect
Governance dimension	Access
Derived From	D5.8/D6.6

ID	GFR42
Name	Cybersecurity: Tracking all the data processes and flows
Status	Specified
Priority	High
Comments	Data exchange shall concern cybersecurity governance aspect by tracking data processes and flows
Governance dimension	Access
Derived From	D5.8/D6.6

ID	GFR43
Name	Cybersecurity: Providing a testing environment to identify and solve potential security breaches
Status	Specified
Priority	High
Comments	Cybersecurity: Providing a testing environment to identify and solve potential security breaches
Governance dimension	Access
Derived From	D5.8/D6.6

ID	GFR44
Name	Access OneNet Framework: Register or modify account
Status	Specified
Priority	High
Comments	OneNet Participants have to be able to register themselves with a username and email in the OneNet System with a new account or modify their existing accounts (i.e., change username, email or password) through accessing the OneNet Framework dashboard
Governance dimension	Access
Derived From	D6.1

ID	GFR45
Name	Access OneNet Framework: Login to Framework Dashboard
Status	Specified
Priority	High
Comments	OneNet Participants have to be able to login to the OneNet Framework dashboard after successful authentication; access to the dashboard shall not be possible without authentication
Governance dimension	Access
Derived From	D6.1

ID	GFR46
Name	Monitoring and Analytics Tools: Administrative and configuration tools
Status	Implemented
Priority	High
Comments	The Monitoring and Analytics dashboard must include administrative and configuration tools for the administrator and OneNet Participants
Governance dimension	Integrity
Derived From	D6.1

ID	GFR47
Name	Access OneNet Framework: Monitor overall performance
Status	Implemented
Priority	High
Comments	OneNet Participants have to be able to monitor performance KPIs (to be defined) and results from analytics algorithms (to be defined) in the OneNet Framework dashboard
Governance dimension	Access, Integrity
Derived From	D6.1

ID	GFR48
Name	Middleware Features: Import/Export for analytics
Status	Specified
Priority	High
Comments	The middleware should allow the possibility to import/export analytics result
Governance dimension	Integrity, Access
Derived From	D6.1

ID	GFR49
Name	Monitoring and Analytics Tools: Data Analytics Dashboard
Status	Implemented
Priority	High
Comments	The Monitoring and Analytics dashboard must include a dashboard with analytics
Governance dimension	Integrity
Derived From	D6.1

ID	GFR50
Name	Monitoring and Analytics Tools: Monitoring and Alerting Dashboard
Status	Specified
Priority	High
Comments	The Monitoring and Analytics dashboard must include a dashboard for monitoring data exchanges and setup alert notifications
Governance dimension	Integrity
Derived From	D6.1