Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HaDEA). Neither the European Union nor HaDEA can be held responsible for them.

DEPLOYTOUR
European Tourism Data Space

Call for proposals	DIGITAL-2023-CLOUD-DATA-AI-05	**Type of action**	DIGITAL-SIMPLE
Grant Agreement No.	101173388	Start date	1 October 2024
Project duration	36 months	End date	30 September 2027

Contact: projects@anysolution.eu

Website: www.deploytour.eu

Project consortium – Coordinator: ANYSOLUTION			
POLITECNICO DI MILANO	BEN - POLIMI	NTT DATA SPAIN	BEN - NTTDES
AMADEUS DATA PROCESSING GmbH	BEN - ADP	AMADEUS GERMANY GmbH	AE - AMADEUS GERMANY
EONA-X	BEN – EONA-X	ITALIAN MINISTRY OF TOURISM	BEN - MITUR
FUNDACIÓN TECNALIA RESEARCH & INNOVATION	BEN - TECNALIA	NECSTOUR	BEN - NECSTOUR
CITY DESTINATIONS ALLIANCE	BEN - CityDNA	INTELLERA	BEN - INTELLERA
ARCTUR	BEN - ARCTUR	INSTITUTO TECNOLÓGICO DE INFORMÁTICA	BEN - ITI
GMV SOLUCIONES GLOBALES INTERNET	BEN - GMV	AVORIS CENTRAL DIVISION	BEN - AVORIS
AUSTRIA TOURISM (OSTERREICH WERBUNG)	BEN – AUSTRIA TOURISM	EUROPEANA	BEN - EF
TURISMO ANDALUCIA	BEN – EPGTDA SA	AMADEUS SAS	BEN – AMADEUS SAS
PLEXUS TECH	BEN – PLEXUS TECH	TECNOLOGÍAS PLEXUS SL	AE - PLEXUS
FRAUNHOFER	BEN - FRAUNHOFER	HIBERUS TECNOLOGIAS DIFERENCIALES SL	BEN - HIBERUSTECH
HIBERUS IT DEVELOP	AE - HIBIT	UNPARALLEL INNOVATION	BEN - UNPARALLEL
PLEIADES CLUSTER	BEN - PLEIAD	UNI SYSTEMS SYSTIMATA	AE - UNIS
THE DATA APPEAL COMPANY	BEN – DATA APPEAL CO	INDUSTRYINNOVATION CLUSTER SLOVAKIA	BEN - IIC
TOURISM BOHINJ SLOVENIA	BEN – TURIZEM BOHIN	LAPLAND UNIVERSITY OF APPLIED SCIENCES	BEN – LAPLAND UAS
DISSET CONSULTORES	BEN - DISSET	UNIVERSITY ILLES BALEARS	BEN - UIB
ADQUIVER	BEN - ADQUIVER	ADQUIVER DATA & ADVANCED ANALYTICS, SL	AE - ADDATA
TRENITALIA	BEN - TRIT	TOURISM PORTUGAL	BEN – TURISMO PT
UNIVERSITY NOVA LISBOA	BEN - UNL	LIBELIUM LAB	BEN – LIBELIUM
MODUL UNIVERSITY VIENNA GMBH	AP - MODUL	YPOURGEIO TOURISMOU	AP - MINTUR
AGENCIA D ESTRATEGIA TURISTICA DE LES ILLES BALEARS	AP - AETIB	STICHTING BREDA UNIVERSITY OF APPLIED SCIENCES	BEN - BUAS
FIWARE FOUNDATION EV	AP - FIWARE	ASOCIACIÓN INSTITUTO TECNOLÓGICO HOTELERO	BEN - ITH

DEPLOYTOUR
European Tourism Data Space

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HaDEA). Neither the European Union nor HaDEA can be held responsible for them.

D2.5 ETDS Architecture (M14)

Document Identification			
Status	Draft pending approval	**Due Date**	30/11/2025
Version	1.0	**Submission Date**	24/11/2025

Related WP	WP2	**Document Reference**	D2.5
Related Deliverable(s)	D2.1 & D2.4	**Dissemination Level (*)**	PU/SEN
Lead Partner	NTTDES	**Lead Author**	NTTDES
Contributors	Amadeus Germany GmbH, ADP, EF, FRAUNHOFER, HIBERUSTEC, LIBELIUM LAB, GMV, ANYSOL, UNL, LAPLAND, EONA-X, TECNALIA, PLEXUS, PLEIAD, DATA APPEAL	**Reviewers**	AMAD

Co-funded by the European Union

Document Information

Document History			
Version	Date	Change editors	Changes
0.1	17/09/2025	Carme Moreu	Initial version
0.2	18/10/2025	All partners contributing	General contributions
0.3	19/10/2025	AMD	Final review
1.0	24/11/2025	AnySolution	Final

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	NTTDES	20/11/2025
Project Coordinator	AnySol	24/11/2025

Table of content

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HaDEA). Neither the European Union nor HaDEA can be held responsible for them.

List of Tables

List of Figures

List of Acronyms

Abbreviation / acronym	Description
AB	Advisory Board
AE	Affiliated entity
AIA	Artificial Intelligence Act - Regulation (EU) 2024/1689
AP	Associated Partner
BEN	Beneficiary
CA	Consortium Agreement
COO	Coordinator
CSA	Coordination and Support Action
DA	Data Act
DATES	An EU project that aims to explore approaches and options for the deployment of a secure and trusted tourism data space
DCM	Dissemination & Communication Manager (DCM)
DGA	Data Governance Act
DMOs	Destination Management Organisation
DPO	Data Protection Officer
DSFT	Data Space for Tourism
Dx.y	Deliverable number y, belonging to WP number x
EC	European Commission
ETDS	European Tourism Data Space (the ecosystem of Tourism data spaces)
EU	European Union
GA	Grant Agreement
GDPR	General Data Protection Regulation - Regulation (EU) 2016/679
KPI	Key Performance Indicator
NTO	National Tourism Office
PC	Project Coordinator
PCT	Project Coordination Team
PMB	Project Management Board
QA	Quality Assurance
QM	Quality Manager
SMEs	Small and Medium-sized Enterprises
RASCI	Responsible/Accountable/Supportive/Consulted/Informed
TL	Task Leader
WP	Work Package
WPL	Work Package Leader

Glossary

Term	Description[1]
Business model	A description of the way an organisation creates, delivers, and captures value. Such a description typically includes who benefits from the value (the customer) and what the value proposition is. Normally, a tool called the business model canvas is used to describe or design a business model, but alternatives more suitable for specific situations, such as data spaces, are available.
Canvas	See Business model.
Capability	See Data Space Building Block.
Data Model	A structured representation of data elements and relationships used to facilitate semantic interoperability within and across domains, encompassing vocabularies, ontologies, application profiles and schema specifications for annotating and describing data sets and services. These abstraction levels may not need to be hierarchical; they can exist independently.
Data Model Provider	An entity responsible for creating, publishing, and maintaining data models within data spaces. This entity facilitates the management process of vocabulary creation, management, and updates.
Data Product	Data sharing units, packaging data and metadata, and any associated license terms. Explanatory Texts: • We (the DSSC) borrow[s] the definition from the CEN Workshop Agreement Trusted Data Transactions. • The definition of data products is still evolving in the data space community. • The data product may include, for example, the data product's allowed purposes of use, quality and other requirements the data product fulfils, access and control rights, pricing and billing information, etc.
Data Product Offering[2]	An offering, in a general sense, refers to data, services, or a combination of both that a data provider offers to data recipients, and includes attributes such as description, provider, creator, pricing, license, data format, current version, previous version, and access rights.
Data Service	A collection of operations that provides access to one or more datasets or data processing functions. For example, data selection, extraction, and data delivery.
Dataset[3]	A collection of data, published or curated by a single agent or identifiable community.

[1] Term and description provided by the DSSC Glossary: https://dssc.eu/space/BVE2/1071252161/Alphabetical+List+of+All+Defined+Terms+in+Blueprint+v2.0; otherwise, term source is provided in footnote.

[2] "Data Product Offering", found in the DSSC "Data, Services, and Offerings Descriptions" section: https://dataspacessupportcentre.atlassian.net/wiki/spaces/bv15e/pages/766069419/Data+Services+and+Offerings+Descriptions

[3] "Dataset", found in DCAT: https://www.w3.org/TR/vocab-dcat/#dcat-scope

Term	Description[1]
Data source[4]	System or entity that generates information, and provides this data and metadata, but they are not yet integrated in the governance of the dataspace.
Data Space	An interoperable framework, based on common governance principles, standards, practices and enabling services, that enables trusted data transactions between participants. Explanatory Texts: • Note for users of V0.5 and V1.0 of this blueprint: we (the DSSC) have[as] adopted this new definition from CEN Workshop Agreement Trusted Data Transactions, in an attempt to converge with ongoing standardisation efforts. Please note that further evolution might occur in future versions. For reference, the previous definition was: "Distributed system defined by a governance framework that enables secure and trustworthy data transactions between participants while supporting trust and data sovereignty. A data space is implemented by one or more infrastructures and enables one or more use cases." • Note: some parties write dataspace in a single word. We (the DSSC) prefer[s] data space in two words and consider that both terms mean exactly the same.
Data Space Agreement	A contract that states the rights and duties (obligations) of parties that have committed to (signed) it in the context of a particular data space. These rights and duties pertain to the data space and/or other such parties.
Data Space Building Block	A description of related functionalities and/or capabilities that can be realised and combined with other building blocks to achieve the overall functionality of a data space. Explanatory Texts: • In the data space blueprint, the building blocks are divided into organisational and business building blocks and technical building blocks. • In many cases, the functionalities are implemented by Services.
Data Space Component	A specification for a software or other artefact that realises one service or a set of services that fulfil functionalities described by one or more building blocks. Explanatory Text: For technical components, that would typically be software, but for business components, this could consist of processes, templates or other artefacts.
Data Space Component Architecture	An overview of all the data space components and their interactions, providing a high-level structure of how these components are organised and interact within data spaces.
Data Space Connector	A technical component that is run by (or on behalf of) a participant and that provides participant agent services, with similar components run by (or on behalf of) other participants. Explanatory Text: A connector can provide more functionality than is strictly related to connectivity. The connector can offer technical modules that implement data interoperability functions, authentication, interfacing with trust services and authorisation, data product self-description,

[4] The "Data source" concept is chosen by the Consortium, aligning with deployEMDS.

Term	Description[1]
	contract negotiation, etc. We use "participant agent services" as the broader term to define these services.
Data Space Functionality	A specified set of tasks that are critical for operating a data space and that can be associated with one or more data space roles. Explanatory Text: The data space governance framework specifies the data space functionalities and associated roles. Each functionality and its associated role include rights and duties for performing tasks related to that functionality.
Data Space Initiative	A collaborative project of a consortium or network of committed partners to initiate, develop and maintain a data space.
Data Space Pilot	A planned and resourced implementation of one or more use cases within the context of a data space initiative. A data space pilot aims to validate the approach for a full data space deployment and showcase the benefits of participating in the data space.
Data Space Role	A distinct and logically consistent set of rights and duties (responsibilities) within a data space, that are required to perform specific tasks related to a data space functionality, and that are designed to be performed by one or more participants. Explanatory Texts: • The governance framework of a data space defines the data space roles. • Parties can perform (be assigned, or simply 'be') multiple roles, such as data provider, transaction participant, data space intermediary, etc.. In some cases, a prerequisite for performing a particular role is that the party can already perform one or more other roles. For example, the data provider must also be a data space participant.
Data Space Rulebook	The documentation of the data space governance framework for operational use. Explanatory Text: The rulebook can be expressed in human-readable and machine-readable formats.
Data Space Use Case	A specific setting in which two or more participants use a data space to create value (business, societal or environmental) from data sharing. Explanatory Texts: • By definition, a data space use case is operational. When referring to a planned or envisioned setting that is not yet operational, we can use the term use case scenario. • A use case scenario is a potential use case envisaged to solve societal, environmental or business challenges and create value. The same use case scenario, or variations of it, can be implemented as a use case multiple times in one or more data spaces.
Data Spaces Blueprint	A consistent, coherent and comprehensive set of guidelines to support the implementation, deployment and maintenance of data spaces. Explanatory Text: The blueprint contains the conceptual model of data space, the data space building blocks, and the recommended selection of standards, specifications, and reference implementations identified in the data spaces technology landscape.

Term	Description[1]
DSSC Asset	A sustainable open resource that is developed and governed by the Data Spaces Support Centre (DSSC). The assets can be used to create, deploy, and operationalise data spaces, and to enable knowledge sharing around them. The DSSC also develops and executes strategies to ensure continuity of the main assets beyond project funding.
Federated Data Spaces	A data space that enables seamless data transactions between participants across multiple data spaces, based on agreed-upon common rules, typically defined in a governance framework. Explanatory Texts: • The definition of a federation of data spaces is evolving in the data space community. • A federation of data spaces is a data space with its own governance framework, enabled by a set of shared services (federation and value creation) of the federated systems, and participant agent services that enable participants to join multiple data spaces with a single onboarding step.
End User Product[5]	The data product offering value for the end users of the dataspace use cases, i.e., business apps, training models, etc.
Intra-data Space Interoperability	The ability of participants to seamlessly access and/or exchange data within a data space. Intra-data space interoperability addresses the governance, business and technical frameworks (including the data space protocol and the data models) for individual data space instances.
Resource[6]	A dataset, a data service or any other resource that may be described by a metadata record in a catalog.

[5] The "Final Data Product" concept is chosen by the Consortium, aligning with deployEMDS.
[6] "Resource", found in DCAT: https://www.w3.org/TR/vocab-dcat/#dcat-scope

1 Executive summary

DEPLOYTOUR is a three-year project, starting in October 2024, aiming to develop and deploy a European Tourism Data Space (ETDS). It is preceded by two preparatory actions, DATES and DSFT, for which this deliverable has adopted their recommendations.

This second deliverable concerning the Reference Architecture provides the technical infrastructure for ETDS, influenced by the previous analysis on Interoperability & Data sharing. The proposed architecture is designed around the Minimum Viable Dataspace, remaining extensible to accommodate future functionalities. This is possible because its structure is based on the DSSC building blocks (DSSC blueprint v2.0), enabling adaptability and scalability. However, significant uncertainties remain regarding the implementation of the technology stack, particularly given the SIMPL decision.

The Consortium also highlighted key considerations for defining the reference architecture. They mainly concern specific questions about the participants, their roles, and the difference between visibility and accessibility of data. Decisions on whether data is centralised or federated, and on correctly understanding private- and public-sector data usage, are essential for aligning business models with the ETDS objectives. In this sense, the maturity of the use cases remains a foundational requirement for DEPLOYTOUR.

1.1 Note on this new version

The architectural updates that are introduced derive from the D2.4-ETDS Architecture document. This document reflects the latest developments and ensures alignment with European standards or European technical recommendations.

The following changes have been implemented:

- Revision of the introduction, objectives and scope of the document.
- Modifications applied to section 3.1 “Analysis of the preparatory action blueprint”
- Section 3.2.4 “SIMPL Initiative” comprehensively updated in accordance with the latest SIMPL publication on GitLab.
- New section 4.2.6.1 “European Interoperability Reference Architecture (EIRA) and eGovERA” created.
- FIWARE added to section 4 “Assessment of Data Space Stacks” and its sections
- Section 4.1 renamed to “Data Space Service according to the DSSC Blueprint”

The enhancements introduced in section 5.2.2 “ETDS high-level architecture” mark a significant step toward a more comprehensive and multidimensional framework. Specifically, the addition of the Legal Layer (section 5.2.2.1), Organisational Layer (section 5.2.2.2), and Semantic Layer (section 5.2.2.3) provides essential structural depth, complementing the previously established Technical Layer (section 5.2.2.4). The ETDS architecture ensures that legal, organisational, semantic, and technical considerations are coherently addressed in the design and implementation of interoperable solutions within the ETDS.

2 Introduction

The present document unites efforts to launch DEPLOYTOUR and to kick-start the European Tourism Data Space (ETDS). The main goal of this document is to define the envisaged solution architecture for the ETDS from a bottom-up approach that is consistent with the Data Spaces Support Centre (DSSC) design principles.

The Consortium ("partners") is responsible for developing the ETDS sectoral data space, which results in the proposal of DEPLOYTOUR and its minimal viable data space (MVDS). The initiative benefits from the involvement of coordinators from the two preparatory actions (DATES/DSFT Blueprint), ensuring continuity and coherence throughout the deployment phase.

As the second official deliverable, this document establishes the architectural principles of ETDS. This second deliverable sets the principles of the DEPLOYTOUR architecture. It builds on the recommendations from the preparatory actions and integrates insights from the first deliverable, *ETDS Interoperability & Data Sharing*. Among the defined work packages of DEPLOYTOUR (WP1 to WP6), WP2 ("TOURISM DATA SPACE BUILDING BLOCKS AND OPERATIONALIZATION.") has settled up this document and has served from WP4 ("REAL-WORLD DEPLOYMENT OF ETDS THROUGH USE CASES BASED ON THE VARIOUS TYPES OF DATA IN THE TOURISM SECTOR") to elaborate the strategic decisions for shaping this deliverable structure and its content.

Although the specific requirements from pilots and use cases (WP4) are still under development, these will be incorporated into the architecture and appended to this document as an annex in future releases.

This document is divided into seven broad sections:

- Section 1 covers the Project Executive Summary;
- Section 2 introduces this document, objectives and scope;
- Section 3 covers the preparatory action blueprint and the state-of-the-art of the data space architectures;
- Section 4 describes the analysis of the technical stacks of the data space architectures and initiatives, as well as the high-level data space architecture, the building blocks and the MVDS of ETDS;
- Section 5 proposes the architecture of ETDS and the evolution plan;
- Section 6 provides the conclusions and next steps in the deployment of the ETDS.

2.1 Objectives

This deliverable focuses on defining the components of the target solution architecture for the ETDS, building on the outcomes of the DATES/DSFT projects. The objectives of this document are structured as follows:

- Identify and analyse the key technical issues and challenges involved in establishing the MVDS for the ETDS;
- Outline the high-level architectural building blocks required for the deployment of the ETDS, distinguishing between mandatory and optional components.
- Identify the technical stack that already exists on the market.

Specific requirements from pilots and use cases will be appended to this document as an annex in future iterations.

2.2 Scope of this document

This document outlines the architectural and operational scope of the ETDS, addressing key regulatory and organisational aspects, such as legal prerequisites for participation, membership contracts, and the terms governing data space involvement. It also defines onboarding procedures and operational roles depicted in the ETDS *Rolebook* (developed by WP3).

Additionally, the scope covers semantic alignment requirements, including the use of standardised semantic artefacts for data publishing and processing, as well as data usage policies and agreements. It also considers connector certification, conformance and security compliance measures.

3 Review of documents and preparation

The European Tourism Data Space (ETDS) roadmap lays a strong foundation for a sustainable, efficient, and future-proof data-sharing framework in the European tourism sector.

3.1 Analysis of the preparatory action blueprint

The preparatory action DATES/DSFT Blueprint[7] sets guidelines for reusing and deploying a reference architecture for the ETDS. The blueprint builds on the OpenDEI Design principles.[8] (position-paper) document, the DSSC Glossary[9], and the IDS Rulebook 2.0[10], as well as considering other relevant programs, i.e., GAIA-X, EONA-X, TDH022, among others.

The blueprint emphasises stakeholder engagement and identifies the main technical challenges of deploying the ETDS. This document reshapes the high-level building blocks defined in the preparatory action. The Consortium will review the feedback gathered from the pilot canvas sessions, which identified that the building blocks outlined in the preparatory action are suitable for deploying a minimum viable data space.

The legal aspect is a key topic regarding the operationalisation of the data space, particularly in terms of handling personal data and ensuring compliance with the Data Governance Act.[11] (DGA), Data Act[12] (DA) and General Data Protection Regulation[13] (GDPR). The document mentions several technologies (i.e., SOLID, MyData, EU Wallet) that have already addressed these issues and recommends using the DIGITAL building blocks provided by the European Commission (EC) for identity management and data delivery.

The reference architecture also addresses the ETDS' data models and interoperability. The Consortium must consider initiatives conducted by local SMEs or national boards working in the tourism domain, such as EONA-X or TDH022, leveraging their solutions alongside the existing ontologies proposed by the ETDS blueprint (e.g., Smart Data Models[14]). The results from the pilot canvas sessions are essential for gaining a clear understanding of data sources and, consequently, shaping the data product offerings. The recommended approach for data transfer is to use connectors that implement the Dataspace Protocol (DSP)[15], which is currently realised by EDC DSP (and formerly, by IDSA data space protocol), characterised by the decoupling of the control and data planes in data transfer technologies, which makes it possible to use any transfer protocol or technology available. The Eclipse Data Space Connector (EDC)[16] is the connector used by the main data space implementations that follow this new approach. However, FIWARE also offers additional functionalities that are limited to a verifiable credentials approach. For the deployment of the ETDS, it is recommended to follow two paths simultaneously: a theoretical roadmap (focusing on formalisation and compliance, utilising frameworks like Gaia-X) and a pragmatic roadmap (deploying real use cases with stable

[7] Blueprint and Roadmap for Deploying the European Tourism Data Space: https://transition-pathways.europa.eu/knowledge-documents/strategic-blueprint-european-tourism-data-space-pathway-innovation-and

[8] OpenDei 2021: Design Principles for Data Spaces: https://h2020-demeter.eu/wp-content/uploads/2021/05/Position-paper-design-principles-for-data-spaces.pdf

[9] DSSC Glossary 1.0: https://dssc.eu/wp-content/uploads/2023/03/DSSC-Data-Spaces-Glossary-v1.0.pdf

[10] IDS Rulebook 2.0: https://docs.internationaldataspaces.org/ids-knowledgebase/idsa-rulebook

[11] DGA: https://eur-lex.europa.eu/eli/reg/2022/868/oj/eng

[12] DA: https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng

[13] GDPR: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

[14] Smart Data Models: https://github.com/smart-data-models/SmartDestination

[15] DSP (formely, an IDSA specification): https://eclipse-dataspace-protocol-base.github.io/DataspaceProtocol/2025-1/

[16] EDC Connector: https://eclipse-edc.github.io/documentation/

connectors, such as EDC Connector and FIWARE), working toward the eventual convergence of both approaches.

Tools supporting personal data sharing include MyData.[17] operators (for GDPR consent management and personal data stores), Solid[18] PODs (decentralised data stores), and the potential EU Wallets[19] (allowing European citizens to store and manage personal data in standard wallets). A significant technical challenge involves SMEs, as the process and technology needed for their participation in a data space are often too complex, costly, and far removed from their usual business practices. To address this, approaches like "Connector as a Service" and the more ambitious "Data Space as a Service" are highly useful and need to be technologically defined, aiming to provide software with a user interface that hides the technical and operational complexity, thereby facilitating onboarding.

The ETDS must attract a critical mass of participants and generate a network effect by communicating a convincing message about the value it offers. Several viable business models were identified for data space actors (providers, consumers, and intermediaries), including: Freemium Access (offering free basic access and charging for detailed data); Freemium Access with Paid Data-Based Products/Services (free basic data access but charging for customised products or services, like analytics reports); Participation-Based Reductions (providing incentives like discounts or tax cuts for actively contributing data); Partnership-Based Agreements (collaborations for non-paid data exchange or joint projects); Yearly Subscription Fees; and Membership Fees. Stakeholder consultation showed that the preferred consumer business models included those that reduced the monetary cost of data, such as fee reduction schemes or partnership agreements.

3.2 Analysis of existing reference architectures

This section provides an overview of existing reference architectures in the current data spaces paradigm and explores their synergies with the Smart Middleware Platform for European Data Spaces (SIMPL.[20]). While some SIMPL components are already in use and have been adopted by various data space initiatives, the development of SIMPL-Open and its technological stack is ongoing. Consequently, the European Commission's Directorate-General for Communications Networks, Content and Technology is implementing the SIMPL architecture in multiple phases (Annex I).

3.2.1 DSSC Blueprint

The Data Spaces Support Centre (DSSC) offers a comprehensive framework for building, managing, and operating interoperable, secure, and trusted data spaces. The DSSC, as an EU initiative, provides means to work collaboratively (i.e., Data Spaces Toolbox.[21]) and aims to consolidate with other initiatives (i.e., IDSA, Gaia-X) to establish a sovereign, interoperable, and trustworthy data-sharing environment[22].

[17] MyData: https://julkaisut.valtioneuvosto.fi/handle/10024/78439
[18] SOLID: https://github.com/solid/specification
[19] EUDI Wallet Architecture and Reference Framework: https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/latest/architecture-and-reference-framework-main/
[20] SIMPL: https://simpl-programme.ec.europa.eu/
[21] Data Spaces Toolbox: https://toolbox.dssc.eu/
[22] "Development of the DSSC Blueprint, which encompasses business and technical specifications essential for data space implementation.", reference found in: https://docs.gaia-x.eu/technical-committee/architecture-document/25.05/gaia-x_context/#dssc

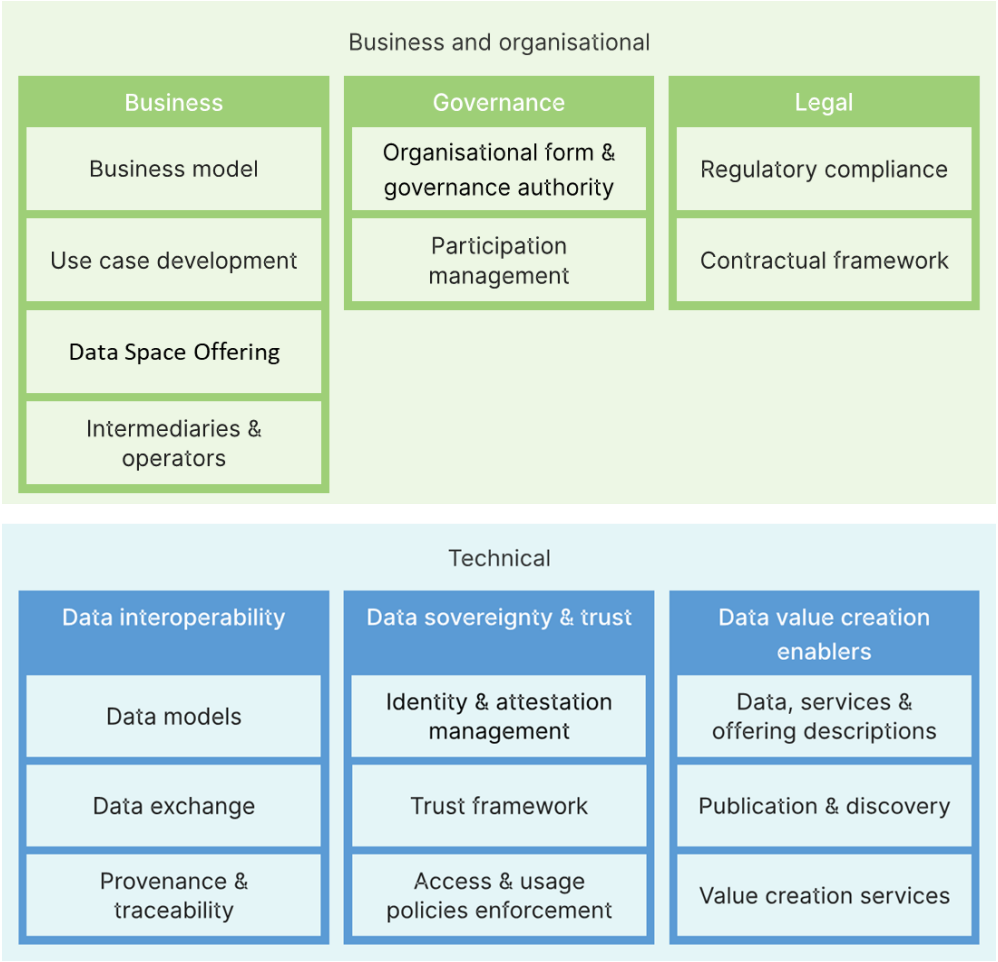

Figure 1 DSSC Building Blocks.

From the DSSC, the Consortium adopts the ETDS blueprint roadmap in analysing and designing the components of the data space (Figure 1). Decisions on crucial components, such as the Data Plane and Control Plane, ensure seamless data exchange and governance. Key standards such as Verifiable Credentials, DCAT v3, and ODRL drive data interoperability, while protocols like the Dataspace Protocol (DSP) enforce data sharing in accordance with defined policies and agreements. Governance frameworks ensure that data access and usage comply with regulations, including the Data Act. SIMPL extends DSSC by implementing a software stack that realises the conceptual preparations done by DSSC. Both are equally dedicated to facilitating interoperability, seamless interactions, data sovereignty and FAIR principles. While DSSC provides the concepts and specifications of the necessary technical infrastructure for data spaces, SIMPL provides the software stack needed to set up the data space. Together, they foster a secure environment for data sharing, enabling collaboration, innovation, and the growth of the digital economy

3.2.2 IDSA reference architecture model (RAM)

The International Data Spaces Reference Architecture Model[23] serves as the fundamental standard for constructing data spaces, enabling trustworthy and self-determined data exchange. While the provided sources do not explicitly detail each specific layer of the IDS-RAM, they do highlight key components and related documents that are integral to its

[23] IDSA-RAM: https://internationaldataspaces.org/offers/reference-architecture/; RAM 4 is the current version, although the Preliminary draft of IDS RAM 5 is also available.

architecture. Notably, RAM 5 is mentioned as having a modular approach to structuring its five layers and three perspectives.

A central component within this architecture is the Dataspace Protocol (DSP)[24]. This is a standardised framework developed by IDSA and maintained by Eclipse to integrate key processes common to all data spaces, ensuring interoperability and trust. The document "Making the Dataspace Protocol an international standard"[25] Emphasises its significance as a step towards standardising interoperability across data spaces, with the potential to revolutionise data sharing. Importantly, RAM 5 is aligned with the latest developments in the Dataspace Protocol.

Furthermore, several crucial documents support the security and governance within IDS data spaces. IDS Certification is of fundamental importance for trustworthy and sovereign data exchange[26]. It ensures that components and organisations participating in data sharing meet the highest security standards, derived from industry-proven criteria like ISO/IEC 27001 and IEC 62443, along with IDS-specific criteria. The certification encompasses both component certification and operational environment certification, each with varying trust and assurance levels.

The IDSA Rulebook[27] is another relevant document, with RAM 5 being aligned with its latest developments. Although the sources do not provide an in-depth explanation of the Rulebook's contents, its mention alongside the Dataspace Protocol and Certification suggests its role in defining the rules and agreements governing participation and data exchange within IDS spaces.

In summary, while a detailed breakdown of each layer of the IDS-RAM is not provided in the sources, the architecture includes essential components such as the DSP for ensuring interoperability, and relies on critical documents like those pertaining to security (integrated within IDS Certification), the IDS Certification scheme itself for establishing trust, and the IDSA Rulebook for defining governing regulations. RAM 5, with its modular structure, aims to further refine this architectural framework and to leverage European regulations and policies: notably, the General Data Protection Regulation (GDPR) which has primacy on data usage over relevant regulations such as the Data Act (DA) and the Data Governance Act (DGA). The IDS-RAM guarantees fair access and prevents monopolisation of data sources, as well as enforcing policies on personal data protection and privacy in cross-border exchanges. This aligns with FAIR principles and ensures the development of scalable and replicable architectures.

[24] Dataspace Protocol: https://eclipse-dataspace-protocol-base.github.io/DataspaceProtocol/2025-1-RC1/
[25] IDSA Statement on the "Making the Dataspace Protocol an international standard": https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-Statement_Making-the-Dataspace-Protocol-an-international-standard.pdf
[26] IDSA Certification & Trust Framework: https://internationaldataspaces.org/offers/certification/
[27] IDSA Rulebook: https://internationaldataspaces.org/idsa-rulebook/

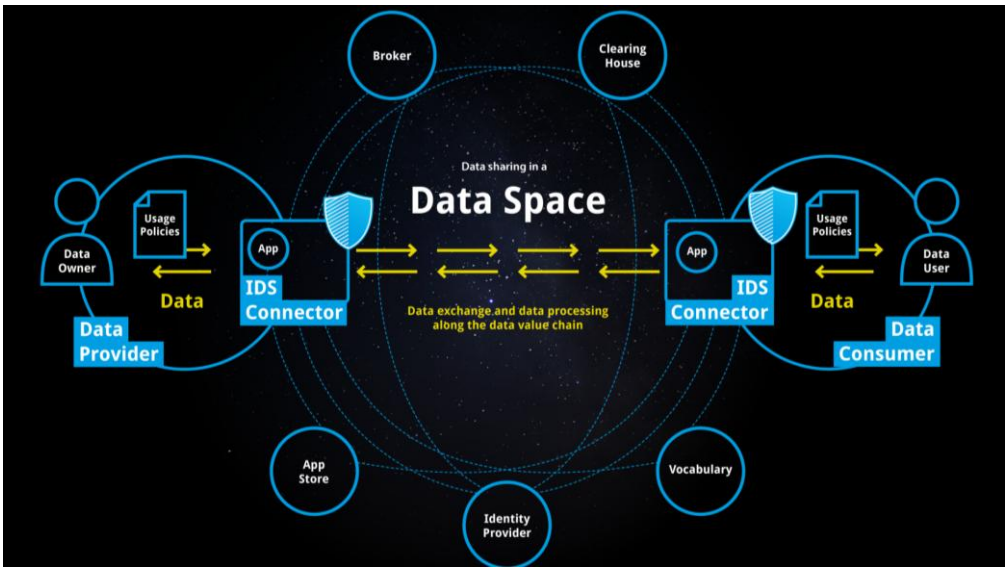

Figure 2 IDS-RAM.

3.2.3 Gaia-X

The Gaia-X Architecture Document[28] serves as a comprehensive guide to the design and implementation of the Gaia-X ecosystem, detailing its conceptual models, components, and services. It outlines the framework for creating a federated, secure data infrastructure grounded in European values of data sovereignty and transparency.

- Conceptual models and components: At the heart of the Gaia-X Architecture is the Conceptual Model, which defines the structure and relationships within the Gaia-X ecosystem. This model encompasses various entities such as Participants, Resources, and Services, each described by Gaia-X-compliant credentials. These credentials ensure adherence to the compliance schemes established by the Gaia-X Association, fostering trust and interoperability among stakeholders.
- Gaia-X Digital Clearing House (GXDCH): The Gaia-X Digital Clearing House functions as a central entity within the Gaia-X framework, providing automated verification services to ensure that Participants and their Service Offerings comply with Gaia-X standards. By issuing compliance credentials, the GXDCH plays a crucial role in maintaining the integrity and trustworthiness of the Gaia-X ecosystem.
- Federation services: To support the operation of a federated data infrastructure, Gaia-X introduces Federation Services. These services include identity and trust mechanisms, compliance verification, and cataloguing of service offerings, all designed to facilitate secure and efficient data sharing among Participants. The Federation Services ensure that interactions within the Gaia-X ecosystem adhere to established policies and standards.
- Gaia-X Compliance Document: Complementing the Architecture Document, the Gaia-X Compliance Document delineates the policies and rules that govern the Gaia-X ecosystem. It sets forth high-level objectives to safeguard the core European values of Gaia-X, such as openness, transparency, and data protection. These objectives are underpinned by specific criteria and frameworks that enable validation and enforcement of compliance across the ecosystem.

[28] Gaia-X Architecture Document: https://gaia-x.eu/wp-content/uploads/2022/06/Gaia-x-Architecture-Document-22.04-Release.pdf

- Alignment with IDSA RAM Principles: Gaia-X aligns with the principles outlined in the International Data Spaces Reference Architecture Model (IDSA RAM), which provides a structured approach to designing and implementing data spaces. The IDSA RAM emphasises aspects like data sovereignty, interoperability, and trust, guiding stakeholders through the decision-making process when building data spaces. By incorporating these principles, Gaia-X ensures its architecture supports secure, sovereign data exchange, thereby facilitating the creation of a robust, trustworthy data-sharing ecosystem.

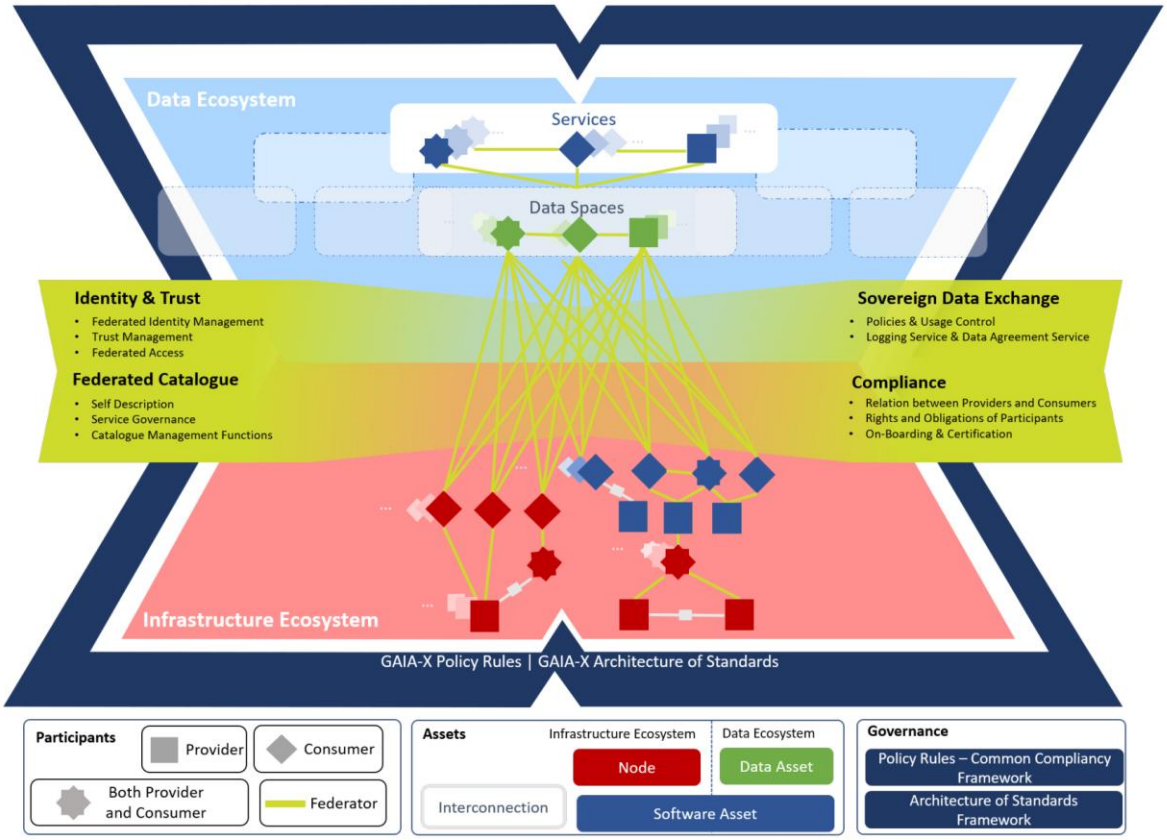

Figure 3 Gaia-X Ecosystem.

3.2.4 SIMPL Initiative

The SIMPL initiative is a project funded by the European Commission. Its objective is to provide an open-source middleware platform that facilitates data access and interoperability among various European data spaces, supporting values such as digital sovereignty, privacy, and fair market practices.

3.2.4.1 SIMPL products

SIMPL comprises three main products: SIMPL-Open, SIMPL-Labs, and SIMPL-Live.

- SIMPL-Open:
  This is the open-source software stack that powers data spaces and other cloud-to-edge federation initiatives. SIMPL-Open focuses on leveraging and collaborating with data spaces and the open-source community to facilitate the integration and development of interoperable solutions. This intelligent middleware brings together the components essential to operating data spaces, enabling data providers to control who

accesses their information.

- SIMPL-Labs:
  Serving as a testing environment for SIMPL-Open, SIMPL-Labs enables rapid interoperability assessments. Developers can create prototypes of data spaces to evaluate the scalability and modularity of their ideas. Additionally, SIMPL-Labs helps identify existing interoperability levels, determine current gaps, and highlight functionalities that could be incorporated from SIMPL-Open.

- SIMPL-Live:
  This component focuses on the practical adoption of SIMPL-Open in specific data space instances. SIMPL-Live includes studies analysing the feasibility of implementing the SIMPL-Open software stack across various data spaces funded by the European Commission. Currently, this encompasses:

  - Public Procurement Data Space
  - European Health Data Space
  - Language Data Space
  - European Open Science Cloud
  - Destination Earth
  - Data Space for Smart and Sustainable Cities and Communities

To engage with the SIMPL initiative, it is recommended to attend community events such as the SIMPL Annual Community Event, which offers live demonstrations of SIMPL products and interactive sessions to contribute to the platform's development.

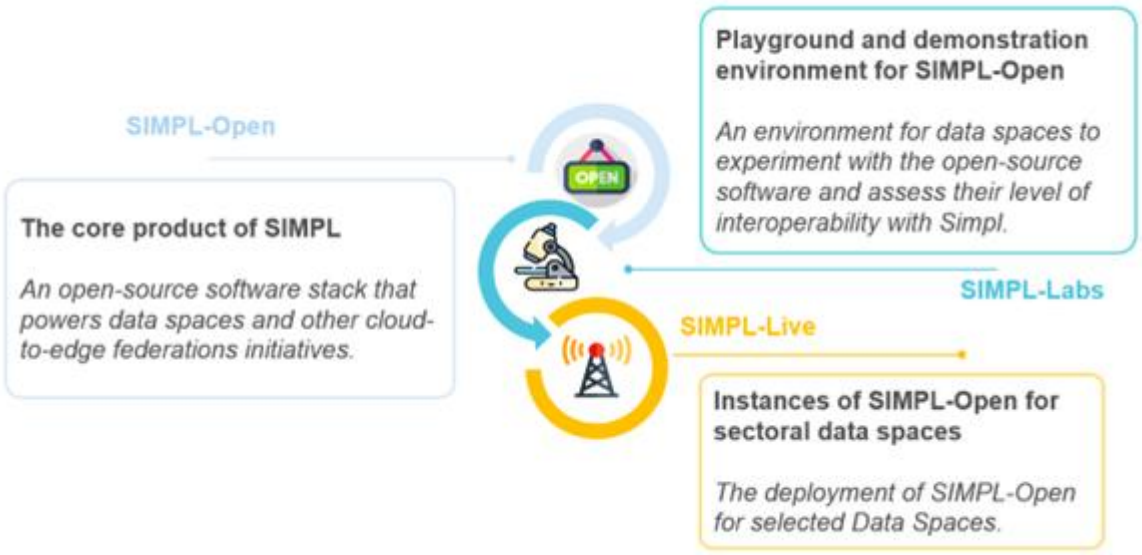

Figure 4 SIMPL Products.

3.2.4.2 SIMPL-OPEN architecture

SIMPL's conceptual architecture is designed to be modular and scalable, allowing for the replacement or addition of components without affecting the rest of the system. Furthermore, it is based on open-source principles, ensuring public accessibility and facilitating continuous collaboration and evolution of the platform.

The architecture of SIMPL-OPEN is defined in GitLab.[29]. Its architecture is based on the TOGAF methodology.[30], which is coupled with specific design principles and a documented set of architectural assumptions and decisions.

TOGAF Layer	Purpose
Business Architecture	Data Architecture describes how Simpl-Open should achieve its business goals and respond to the strategic drivers set out in the Architecture Vision, including an update on functional capabilities and business processes.
Application Architecture	Application Architecture develops the target application architecture, identifying components through Solution Views (based on business processes, both static and dynamic) and Deployment Views (based on agent type).
Data Architecture	Data Architecture presents the data entities and collections, and how they are structured within the system, detailing the architecture through Conceptual, Logical, and Physical Data Models.
Technology Architecture	Technology Architecture develops the target technology architecture by mapping application building blocks to technology components and services (using both Solution and Deployment Views).
Security Architecture	Security Architecture covers the security aspects and requirements of the overall architecture.

Figure 5 TOGAF architecture description into five distinct views.

From the architectural point of view, the SIMPL connector is defined as the technical core component required for a participant to join the data space. It is implemented as a fundamental software component within the SIMPL-Open Agent, which is the middleware deployed on each participant's node to act as a local gateway for communication regardless of the participant's role (i.e., data consumer, data provider, service provider):

- Enabling data sharing and exchange,
- Incorporating modules for data interoperability functions,
- Providing authentication and authorisation interfacing,
- Providing resource description,
- Providing contract negotiation.

The connector integration options in the SIMPL-Open architecture primarily focus on the use of Eclipse Dataspace Connector (EDC). Others, such as the FIWARE connector, are designed as an integrated suite of components that can be deployed to "connect" to a data space by leveraging Verifiable Credentials (VC) and Attribute-based Access Control (ABAC). If integrated, the FIWARE components would either replace or complement the current EDC architecture.[31].

[29] SIMPL-OPEN GitLab – Functional and Technical requirements (Architecture): https://code.europa.eu/simpl/simpl-open/architecture/-/blob/463b44e6a1f62d8f53aded0a26df066a7e39e987/functional_and_technical_architecture_specifications/Functional-and-Technical-Architecture-Specifications.md

[30] TOGAF: https://www.opengroup.org/togaf

[31] A leverage EDC-FIWARE-SIMPL requirements should be carried out using SIMPL requirements in https://simpl-programme.ec.europa.eu/book-page/simpl-requirements.

3.2.5 EUDI Wallet ARF

The EUDI Wallet is an innovative project that aims to provide European Union citizens with a secure, unified digital identity for activities such as travelling, working, accessing public services, making payments, and signing documents. This project is closely linked to the eIDAS Regulation.[32] and its update, eIDAS 2.0[33], approved in March 2024.

- EUDI Wallet Architecture and Reference Framework (ARF):

The EUDI Wallet Architecture and Reference Framework (ARF) is a document that provides the necessary specifications to develop an interoperable EUDI Wallet solution based on common standards and practices. The ARF defines the technical architecture, standards, and technical specifications, as well as a set of guidelines and best practices to ensure consistency and security within the EUDI Wallet ecosystem.

- Relationship with the European Digital Identity Regulation:

The ARF is grounded in the European Digital Identity Regulation, which establishes a common framework to facilitate the consistent implementation of the EUDI Wallet across all Member States. By adhering to the ARF specifications, digital identity solutions are ensured to be interoperable and compliant with the legal and technical requirements established at the European level.

- Implementation and Development:

To support the implementation of the ARF, the European Commission has developed a Reference Implementation of the EUDI Wallet. This implementation serves as a model to demonstrate a robust and interoperable platform for digital identification, authentication, and electronic signatures based on common standards across the European Union.

3.2.6 European Interoperability Framework

The European Interoperability Framework[34] (EIF) is a commonly agreed approach to the interoperable delivery of European public services. This framework defines basic interoperability guidelines for Member States in the form of common principles, models and recommendations, ensuring the long-term success of the Digital Single Market.

The European Commission is actively working on the adoption of the EIF within the EU, and most EU member states are currently monitoring their interoperability activities in relation to the EIF specification to track progress in its implementation via the IOPEI Monitoring Observatory[35]. A new governance structure, the Interoperable Europe Board (the 'Board'), resulting from the Interoperable Europe Act[36] (IEA), should be established and should have a legal mandate to drive, together with the Commission, the further development of cross-border interoperability in the EU, including the European Interoperability Framework (EIF) and other common legal, organisational, semantic and technical interoperability solutions, such as specifications and applications. The Board is empowered to update the EIF as needed, meaning that the adoption of the framework should be considered for the deployment of the

[32] eIDAS (Regulation (EU) No 910/2014): http://data.europa.eu/eli/reg/2014/910/oj
[33] eIDAS 2.0 (Regulation (EU) 2024/1183): https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng
[34] EIF: https://ec.europa.eu/isa2/eif_en/
[35] IOPEI monitoring: https://interoperable-europe.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory
[36] IEA: https://eur-lex.europa.eu/eli/reg/2024/903/oj

ETDS, ensuring that its architecture is fully aligned with European interoperability principles and governance frameworks.

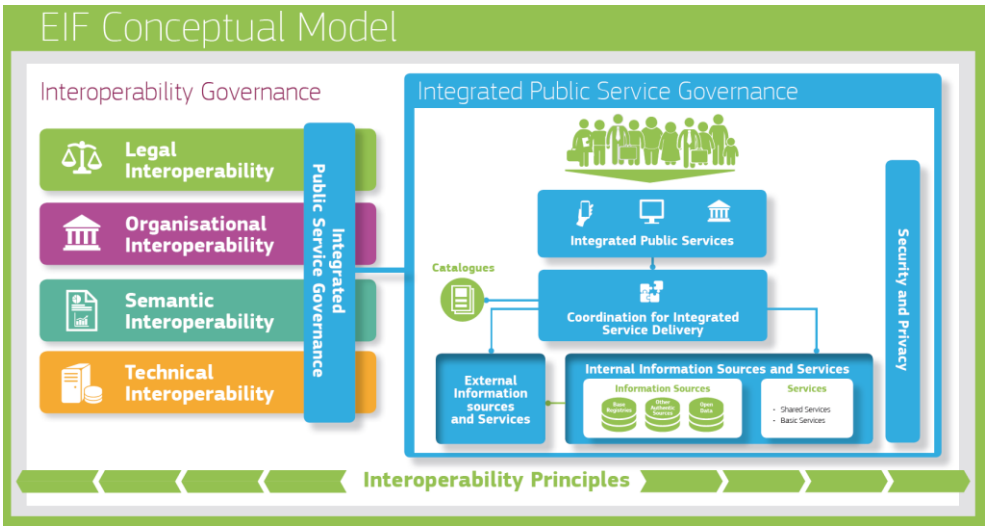

Figure 6 EIF Conceptual Model.

3.2.6.1 European Interoperability Reference Architecture (EIRA) and eGovERA

The European Interoperability Reference Architecture[37] (EIRA©) is a reference architecture promoting a common framework for designing interoperable solutions within the EU. Among the main objectives are:

- the analysis of requirements in a reference architecture, and
- the design of a target solution use case in an agnostic manner.

EIRA is closely related to the EIF and supports its implementation by providing a structured approach to interoperability. As a reference architecture, it can be seen as a blueprint for the creation of interoperable digital services, serving as: 1) a guide for creating services that meet specific needs; 2) best practices, standards, and guidelines to create systems that are efficient, scalable, and interoperable; 3) common language and approach for technology development and deployment that reduces complexity and costs.

In this context, EIRA© should be considered when defining the ETDS reference architecture, ensuring that its solutions and processes can be published and reused through the portal in accordance with the Interoperable Europe Act (IEA).

Building upon this foundation, EIRA© acts as a quality assurance specification and a blueprint for designing and analysing interoperable digital public services. The latest version, EIRA v6.1.0, introduces structured Architecture Building Blocks (ABBs) that represent key capabilities across the EIF interoperability views:

- **Legal View**: Ensures compliance with legislative and policy requirements.
- **Organisational View**: Defines governance structures, roles, and relationships among stakeholders.
- **Semantic View:** Addresses how data and information are structured, represented, and shared.
- **Technical Application View**: Focuses on the technical components and interfaces supporting service delivery.
- **Technical Infrastructure View:** Describes infrastructure services (e.g. hosting, networking, and storage).

[37] EIRA: https://interoperable-europe.ec.europa.eu/collection/european-interoperability-reference-architecture-eira/solution/eira

Through these views, EIRA enables both rigorous requirements analysis and robust solution design, independent of any particular technology stack.

To ensure alignment with EIRA, the EIRA Validator.[38] part of the European Commission's Interoperability Test Bed[39], allows architects to test ArchiMate® models against EIRA business rules and principles. This tool is particularly relevant when deploying solutions in public administrations and data spaces. eGovERA© builds on EIRA's foundation and extends it for eGovernment and Data Space domains, offering more specific modelling guidance, business rules, and reusable architectural templates. The eGovERA Business Agnostic version 6.1.0[40] is a recognised reference in this regard.

By integrating both EIRA© and eGovERA© into the ETDS design, the resulting architecture benefits from conceptual rigour, reusability, and interoperability by design, ensuring full alignment with European interoperability strategies and compliance obligations.

[38] EIRA Validator: https://www.itb.ec.europa.eu/eira/upload

[39] Interoperability Test Bed: https://interoperable-europe.ec.europa.eu/collection/interoperability-test-bed-repository/solution/interoperability-test-bed

[40] eGovERA Business Agnostic Reference Architecture: https://interoperable-europe.ec.europa.eu/collection/european-interoperability-reference-architecture-eira/solution/egovera-business-agnostic-0/release/610

4 Assessment of Data Space Stacks

This section provides a high-level assessment of the main open-source technology stacks used to implement Data Space architectures, aligned with the DSSC blueprint v2.0. The analysis focuses on three representative implementations: EDC, SIMPL and FIWARE.

These technology stacks provide complementary approaches to implementing the participant Agent and Federation Services defined in the DSSC blueprint, enabling trusted, secure, and interoperable data exchange.

4.1 Data Space Service according to the DSSC Blueprint

According to the DSSC blueprint v2.0, different service types implement the technical building blocks of the data space. These are, in particular, the so-called Federation Services.[41] and Participant Agent Services[42]. The services are used to implement the core components of a data space. The following section uses these components to compare EDC, SIMPL, and FIWARE, highlighting the characteristics of the two software stacks.

4.1.1 Participant Agent Services

In DSSC terminology, the participant agent describes the gateway of the participant to the data space and thus refers to the connector, one of the most important components of the data space. The connector enables the implementation of the basic functionalities required by each participant in the data space, including access to the credential store, local catalogue publication, contract negotiation, transfer process, and the data plane. EDC, SIMPL, and FIWARE provide connectors that can be deployed either in the participant's infrastructure or by a cloud provider as software-as-a-service (SaaS).

A key distinction among EDC, SIMPL, and FIWARE is their architectural approach:

- EDC adopts a modular architecture that separates the control and data planes.
- FIWARE integrates existing FIWARE components into a unified connector, in line with DSBA technical convergence principles.
- SIMPL differentiates between agents for data providers and data consumers, assigning distinct functions to each. If a participant wishes to act as both a data provider and a data consumer in the data space, SIMPL requires two separate agents.

Figure 7 shows the participant agent services, the connector's functions according to DSSC, and their relations. These building blocks are described below.

[41] "Federation Services", as defined in the DSSC Rulebook: https://dssc.eu/space/BVE2/1071255059/Federation+Services

[42] "Participant Agent Services", as defined in the DSSC Rulebook: https://dssc.eu/space/BVE2/1071255120/Participant+Agent+Services

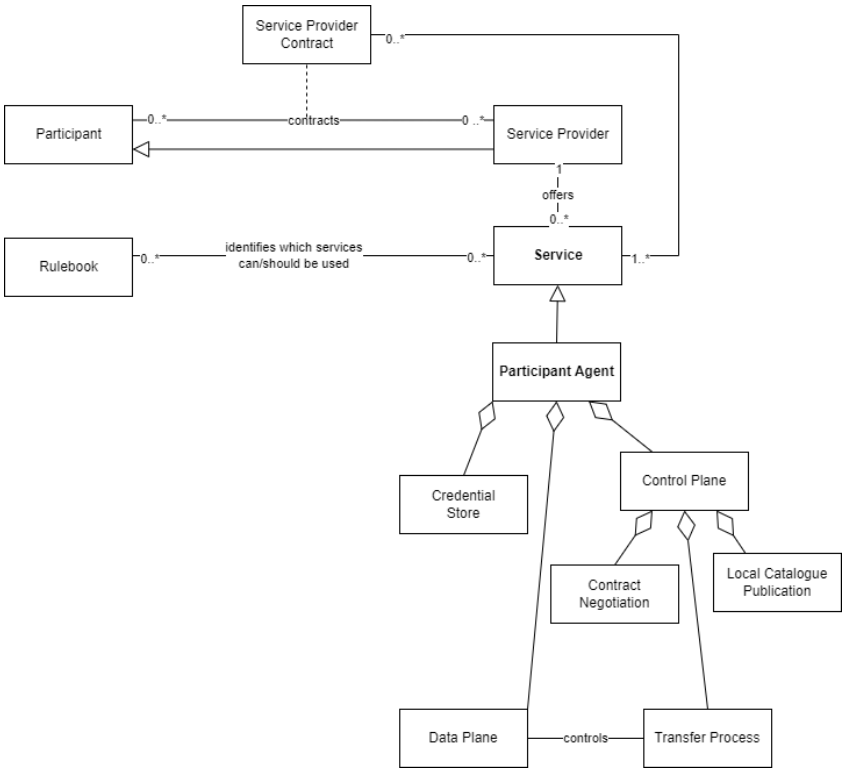

Figure 7 Participant Agent Services diagram.

4.1.1.1 Credential Store

The credential store tracks participants' identities and credentials. In addition, the credential store is used to present a participant's credentials to other participants and to validate the credentials of other participants, and is strongly aligned with the Federation's "Validation and Verification services." Therefore, the characteristics of both services are described together in this section. In earlier DSSC publications, the credential store was also referred to as the participant wallet. The DSSC recommends verifiable credentials (VCs) developed by the W3C for providing credentials, and EDC, SIMPL, and FIWARE use VCs for identity management.

EDC implements the Eclipse Decentralised Claims Protocol (DCP)[43] which is based on core standards of decentralised identity, including Decentralised Identifiers (DIDs)[44], the did: web method[45], and the VC Data Model v1.1[46] in the so-called Identity Hub. The Identity Hub manages organisational identity resources such as credentials for data space participants and can handle Machine-to-Machine (M2M) interactions.

The Identity Hub securely stores and manages VCs, including presentations. The issuance of the credentials is currently work in progress. Using the DCP and the Identity Hub ensures that VCs can be linked to data-sharing agreements effectively, without centralised identity management.

FIWARE follows a decentralised and standards-based approach to identity management, supporting Self-Sovereign Identity (SSI) principles and integrating with EBSI-compliant[47] Trust

[43] DCP: https://github.com/eclipse-dataspace-dcp
[44] DIDs: https://www.w3.org/TR/did-1.0/
[45] did:web Method Specification: https://w3c-ccg.github.io/did-method-web/
[46] VC Data Model v1.1: https://www.w3.org/TR/vc-data-model/
[47] EBSI: https://hub.ebsi.eu/

Services for credential issuance and validation. It implements W3C Decentralised Identifiers (DIDs) and Verifiable Credentials (VCs/VPs) as defined by the DSBA Technical Convergence Recommendations, and supports authentication via the SIOPv2[48] and OIDC4VP[49] protocols. Identity and access management are handled by the FIWARE Keyrock[50] Identity Manager, which acts as an OpenID Connect (OIDC)[51] and OAuth2 provider, managing credentials and tokens. Fine-grained access control is enforced through Attribute-Based Access Control (ABAC) mechanisms using the Open Policy Agent (OPA)[52] and Open Digital Rights Language (ODRL)[53] for policy definition. In contrast, the Wilma[54] PEP Proxy enforces authorisation rules and validates tokens.

The identification system in SIMPL is grouped into two tiers and therefore differs from EDC and FIWARE. The main reason for dividing users into two groups is that end users of an organisation verify themselves with the organisation's connector via company-specific Identification, Authentication and Authorisation (IAA) mechanisms, e.g., EU Login, eID, etc. The core component responsible for these functions is the Tier 1 Authentication Provider, which stores user and role information. It uses an extended version of Keycloak, an open-source OIDC Identity Provider. Role-Based Access Control (RBAC)[55] policies determine which actions each end user is allowed to perform on specific agent resources. This is implemented via an API gateway (Spring Cloud Gateway). Therefore, participants must store credentials as OIDC Access Tokens, specifically JSON Web Tokens (JWTs).

The Tier 2 identity management, managed by the Dataspace Governance Authority, ensures secure, encrypted communication between participants' connectors and is realised through both centralised and decentralised components. The centralised Identity Provider Federation creates, validates, and manages Tier 2 certificates. When a new participant is onboarded, a Tier 2 certificate is designed and installed in the participant's connector. It also manages the Security Attribute Provider Federation, which creates and assigns identity attributes for ABAC and provides them as signed ephemeral proofs. The decentralised Tier 2 Authentication Provider stores the Tier 2 certificate and validates certificates and ephemeral proofs from other agents during mutual TLS (mTLS) authentication. It also checks Tier 1 certificates against the ephemeral proofs and requests new proofs from the Security Attribute Provider Federation when necessary. Authorisation at the Tier 2 level is implemented via an API gateway that enforces ABAC policies based on authentication information to control access to resources. The Tier 2 certificate is an X. 509 certificate issued by the certificate authority of the Identity Provider Federation. The Data Space Governance Authority assigns identity attributes and shapes the interaction rules between participants.

4.1.1.2 Local catalogue publication

Local catalogue publication refers to the publication of metadata of the respective participant's data products in the connector. Local catalogue publication is therefore to be clearly distinguished from federated catalogues, because the data offerings are in the participant's local catalog.

[48] SIOPv2: https://openid.net/specs/openid-connect-self-issued-v2-1_0.html#name-cross-device-self-issued-op
[49] OIDC4VP: https://openid.net/specs/openid-4-verifiable-presentations-1_0.html#request_scope
[50] Keyrock: https://github.com/ging/fiware-idm
[51] OIDC: https://openid.net/developers/how-connect-works/
[52] OPA: https://www.openpolicyagent.org/docs
[53] ODRL: https://www.w3.org/TR/odrl-model/
[54] Wilma: https://fiware-pep-proxy.readthedocs.io/en/latest/
[55] RBAC: https://csrc.nist.gov/projects/role-based-access-control

In EDC, catalogs are technically realised by enabling data providers to publish their data product descriptions (assets) through their so-called control plane, which other participants in the data space can access via their connector using HTTP POST requests. The catalogs are dynamically generated JSON-LD.[56] schemes adhering to DCAT[57] and ODRL[58] specifications, containing datasets that represent the offered data. Each dataset includes a usage policy defined with ODRL. This policy specifies conditions for accessing the data. The datasets also include one or more distribution channels, each describing the wire protocol (e.g., HTTP pull, S3 push) used to access the data. In addition, access services are included, providing endpoints for negotiating data access contracts. To avoid conflicts, EDC uses namespaces when using JSON-LD. This enables extensibility so that catalogs can also be customised based on the identity of the data consumer and the login credentials. This ensures access control and dynamic enforcement of policies in accordance with Dataspace Protocol (DSP) standards.

In FIWARE, local catalog publication can be implemented through the NGSI-LD API[59], which enables providers to expose and describe data assets as linked data entities. The FIWARE Context Broker manages the publication of these entities, facilitating semantic interoperability and discoverability across the data space. Asset metadata can be expressed using DCAT- and ODRL-based vocabularies, aligned with the DSBA Technical Convergence Recommendations. This allows data offerings to be queried based on their context, attributes, and relationships. The NGSI-LD data model also enables event-driven updates through subscriptions, supporting real-time synchronisation of asset availability and status between providers and consumers within the FIWARE ecosystem.

In SIMPL, the Local Assets Catalogue represents the component of the SIMPL connector where data providers register information about their published assets. This catalogue contains the minimal required metadata and supports the DSP. When a provider registers an asset, a unique asset ID is created to identify it, and the asset is associated with the relevant policies and contract definitions. The Local Assets Catalog ensures that all the offered services and usage conditions of a data provider are available, allowing data consumers to discover the provided assets and access them in accordance with established policies.

4.1.1.3 Contract negotiation

Contract Negotiation is the part of the connector where access and usage policies are enforced. After publication of the data product, the data provider's and the data consumer's connectors initiate contract negotiation and align on the policies of the two participants.

In EDC, contract negotiation is realised through asynchronous messaging using the DSP. When a data consumer requests access to a dataset, it sends a contract negotiation request with the dataset offer via the Management API[60]. The negotiation progresses through a series of defined states, with both data consumer and data provider control planes exchanging DSP messages to transition states. EDC ensures reliable message exchange by implementing transactions in which state transitions are committed only upon successful acknowledgement from the counterparty. Messages are idempotent and include unique IDs. If not acknowledged, they are resentful, and the receiver handles de-duplication. The EDC's eventing system allows developers to subscribe to events, such as the finalisation of a contract negotiation, using the EventRouter, with support for both asynchronous and synchronous transactional notifications.

[56] JSON-LD: https://json-ld.org/
[57] DCAT: https://www.w3.org/TR/vocab-dcat-3/
[58] ODRL: https://www.w3.org/TR/odrl-model/
[59] NGSI-LD API: https://www.etsi.org/deliver/etsi_gs/CIM/001_099/009/01.02.01_60/gs_CIM009v010201p.pdf
[60] Eclipse EDC Management API: https://eclipse-edc.github.io/Connector/openapi/management-api/

Reliability is maintained across restarts by persisting interaction states in transactional stores, like Postgres, ensuring consistent and dependable contract negotiations within the data space.

In FIWARE, contract negotiation is handled through the TM Forum APIs[61], which manages the lifecycle of data sharing agreements between providers and consumers. These APIs align with the DSP framework to ensure interoperability with other data space implementations. Policy enforcement and negotiation parameters are defined using the ODRL, and decisions are enforced through the Wilma PEP Proxy and Keyrock components. The integration of these APIs allows automatic policy validation, status tracking, and contract updates, ensuring traceability and compliance within decentralised environments.

In SIMPL, contract negotiation refers to the same process as in EDC. Nevertheless, the Contract Negotiation Adapter component is crucial to this process. This component acts as an intermediate link between the Catalogue Client application and the connector. The Contract Negotiation Adapter is implemented as a Java backend application that sends a request for an offering to the provider, which returns the offering along with its unique Offering ID and the associated usage and access policies. Once the user reviews and accepts these conditions, the Contract Negotiation Adapter constructs a request to initiate contract negotiation with the provider's connector and retrieves the negotiation status. This ensures that both the data provider and the data consumer have a shared understanding and agreement on data usage policies.

4.1.1.4 Transfer process

The transfer process becomes available as soon as contract negotiation is completed and the contract is executed via the data plane.

In EDC, the transfer process manages data sharing between the data provider and the data consumer after the contract is finalised. Initiated via the Management API, transfers can be finite (e.g., a file transfer) or ongoing (e.g., a continuous data stream). EDC supports two modes: first, a data consumer pull, where the data consumer retrieves data from the data provider; and second, a data provider push, where the data provider sends data to the data consumer. The process is orchestrated by a shared state machine between the control planes of both parties, which ensures synchronised and efficient data transfer. This separation of control and data planes enables scalability. Furthermore, policy monitoring maintains compliance with contractual terms throughout the transfer.

In FIWARE, the transfer process leverages the NGSI-LD interface for data exchange, supporting both synchronous queries and asynchronous event subscriptions. Depending on the negotiated contract, data can be exchanged through direct API calls or context-based updates managed by the Orion Context Broker[62]. Communications are secured via HTTPS, and authentication and authorisation are enforced through Keyrock (OIDC/OAuth2) and the Wilma PEP Proxy, ensuring that all data transfers comply with agreed contractual and policy conditions.

In the SIMPL-Open architecture, data transfer is straightforward and supports two special types: bulk transfer and data streaming. The data transfer component enables access to various data resources. It facilitates exchange between participants, efficiently managing the process by implementing data orchestration and simple data transfer building blocks. Technically, it accesses data resources and transfers copies to consumers via the EDC connector, with the consumer's data space connector storing the copy for access. This ensures

[61] TM Forum APIs: https://www.tmforum.org/oda/open-apis/directory
[62] Orion Context Broker: https://fiware-orion.readthedocs.io/en/master/

seamless, secure data exchange within the data space by utilising standardised connectors and protocols tailored to different data types and transfer requirements.

Currently, SIMPL implements two data transfer building blocks: the data orchestrator and simple data transfer. The data orchestrator leverages existing plugins from the EDC connector to manage data transfers, specifically enabling consumer pull and provider push. It translates contractual agreements into tangible actions for data exchange between the source and destination. Simple data transfer is used to exchange small- to medium-sized datasets (a few megabytes to 100 megabytes) between participants. This approach ensures efficient, secure, and standardised data exchange within the data space, accommodating various data transfer needs.

4.1.1.5 Data plane

While most of the previously presented services of the connector are handled via the so-called control plane, the actual data products are exchanged between the data provider and the data consumer via the data plane.

The Data Plane of the Eclipse Dataspace Connector (EDC) is responsible for transmitting data between participants, utilising various wire protocols such as HTTP, Kafka or cloud object storage. It operates under the direction of the Control Plane and communicates with it via the Data Plane Signalling API. Typically, the Data Plane is deployed as an independent component in a separate environment, such as a Kubernetes cluster, enabling independent scaling and management. During registration, the Data Plane reports its capabilities, including supported protocols and transfer types, to the Control Plane. The Control Plane uses this information to determine available data transfer types and to select the appropriate Data Plane for transfer processes. EDC provides the Data Plane Framework (DPF), a platform for building custom Data Planes. The DPF supports end-to-end streaming transfers for scalability, both pull- and push-style transfers, and provides extension points for various data sources and sinks, enabling direct streaming between different types. In SIMPL, the data transfer is similar to EDC, as it utilises the EDC data plane.

In FIWARE, there is no separate data plane component, unlike in EDC or SIMPL. However, equivalent functionality is provided by the Context Broker, which manages the exchange of context data between participants through the NGSI-LD API. Therefore, while the FIWARE architecture integrates control and data exchange into a unified layer rather than distinct planes, it effectively fulfils the data-plane role by ensuring secure, interoperable, and event-driven data sharing, fully aligned with the DSP and DSBA interoperability principles.

4.1.2 Federation Services

Federation services are fundamental in supporting the interplay between participants in a data space. These services operate in accordance with the policies and rules specified in the Rulebook by the data space authority.

It is important to note that data spaces are typically distributed. This means there is no central platform where all data is stored. In most cases, participants in a data space manage their own data and can decide whether to share it with other participants, sometimes across multiple data spaces.

The distributed nature of data spaces offers participants great flexibility and autonomy, allowing them to maintain control over their own data. However, this distribution can also pose challenges for coordination and collaboration among participants.

For this reason, federation services are essential. These services facilitate interaction and cooperation among participants, ensuring that the established policies and rules are followed

and that data transfer is carried out securely and efficiently. Additionally, federation services can include tools and technologies that help participants manage their data, share information, and collaborate on joint projects, all within the framework of the data space's rules and policies. In summary, although data spaces are inherently distributed and participants have the freedom to manage their own data, federation services play a crucial role in facilitating interaction and cooperation among them, ensuring that the data space functions harmoniously and effectively.

There are six main categories of federation services:

- Data Space registry
- Validation and Verification services
- Policy information Point services
- Catalogue services
- Vocabulary services
- Observability services

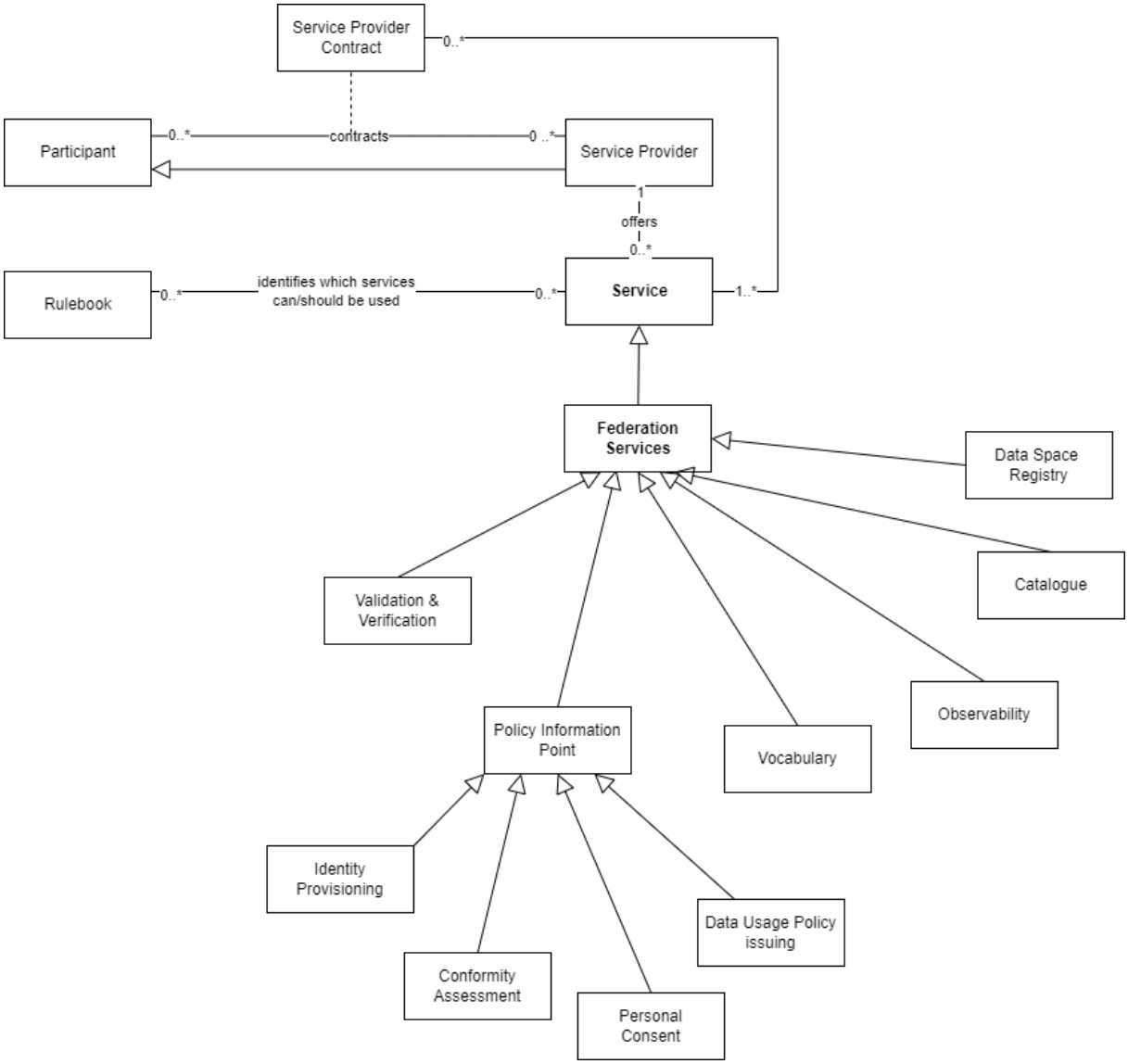

Figure 8 Federated Services diagram.

4.1.2.1 Data Space Registry

According to DSSC, the Data Space Registry is a kind of configuration file, a machine-readable interpretation of the Data Space rulebook. According to DSSC, this is a new service and therefore immature.

In EDC, no Data Space Registry could be found. As it will be an important service in the future, current developments are continuously being evaluated. EDC does not plan to implement this in the future because the Data Space Registry is very data-space-specific.

In FIWARE, registry-like functionality is provided through the FIWARE Data Space Connector, which integrates identity and onboarding capabilities aligned with the DSBA Technical Convergence recommendations. The Keyrock Identity Manager supports participant registration and credential validation, enabling interoperability with external governance authorities or federated registries when required.

In SIMPL, the Data Space Registry is defined as the Governance Authority Agent, whose primary goal is to establish the onboarding process and manage the participant registry. This involves several components: the Onboarding component (central to managing onboarding requests from applicants), the Identity Provider component (responsible for generating credentials and storing them in the Credentials Database), the Security Attributes Provider component (which registers the participant's security identity attributes), and the Authentication Provider (which manages the authentication process).

4.1.2.2 Validation and Verification Services

Validation and Verification services issue credentials, verify credentials, and optionally allow delegation of trust, which technically also involves issuing a credential.

The services are closely related to the connector's credential store and have already been described there in section 4.1.1.

4.1.2.3 Policy Information Point services

The Policy Information Point (PIP) provides policy information to help participants make decisions, such as granting access or issuing credentials. PIP services include Identity Provisioning (providing identity details), Personal Consent (indicating data-sharing consent), Conformity Assessment (checking compliance with policies), and Data Usage Policy Issuing (providing standardised policies). These connect to policy decision and execution points in participant agents to implement access and usage policies.

Specific points in this regard have also been described in section 4.1.1.

4.1.2.4 Catalogue services

Catalogue services provide an overview of registered data products in the data space and link to their respective participant agents. This enables participants to search for and discover assets in the data space. These services implement the Publication and Discovery building block and use the DCAT specification to express metadata of data products.

EDC offers a federated catalog as an extension of the software stack[63].

In FIWARE, catalog type functionalities are provided by the Orion-LD Context Broker, which manages metadata and contextual information through the NGSI-LD API. This API enables data providers to register, update, and publish assets, while consumers can query and subscribe to context changes in real-time, supporting both pull and push discovery models. While Orion-LD does not implement a fully federated catalogue in the strict sense, its

[63] Eclipse EDC Federated Catalog module: https://eclipse-edc.github.io/documentation/autodoc/federated-catalog/

capabilities can be used to simulate federated behaviour by enabling interoperable publication and discovery of data assets across different domains.

In SIMPL, the Federated Catalogue component implements the Resource Catalogue building block and part of the Search Engine building block, enabling providers to publish their resources and consumers to discover them. Rather than embedding search functionality within the Federated Catalogue, the Search component is a distinct part of the consumer agent that connects to the Federated Catalogue within the governance authority agent. This design supports the two-tier IAA approach, where the consumer end-user connects to the Search component via Tier 1, and the Search component connects to the Federated Catalogue via Tier 2.

SIMPL uses the XFSC Federated Catalogue[64] as a catalogue for data, apps, and infrastructure, the Federated Catalogue is not monolithic; it consists of multiple components to reuse existing technology and allow for scalability, and these components can be deployed individually.

4.1.2.5 Vocabulary services

Vocabulary Services provide an overview of available data models in the data space, enabling participants to select common models for specific applications. This ensures semantic interoperability between participants, especially when certain data models are mandated. They also link these data models to APIs or technical interfaces for data exchange, offering both semantics and syntax. This affects the metadata to describe a data product offering.

Each data space must host its own vocabulary or access existing ones. EDC does not offer its own developments and relies on existing vocabularies.

Similarly, FIWARE does not implement a standalone Vocabulary Service. Instead, semantic interoperability is built into the NGSI-LD information model, which uses Linked Data principles (URIs and JSON-LD contexts) to consistently represent entities and relationships. This design eliminates the need for a separate vocabulary layer.

In SIMPL, the Vocabulary Management component is part of the Metadata Description building block. It serves to harmonise vocabularies within the data space by providing definitions for metadata representation and, if necessary, data representation standards. The governance authority uses this component to define vocabularies. The Vocabulary Datastore contains the loaded ontologies and schemas used for semantic validation. The Vocabulary Management component is implemented as a file system, and its user interface is an Angular front-end application.

4.1.2.6 Observability services

Observability Services record specific data about data sharing within the data space to enable auditing, provenance, and traceability. Depending on the use case and relevant legal or contractual obligations, auditing data sharing might be necessary. These services help to ensure that data sharing complies with required standards and regulations.

[64] XFSC Federated Catalogue: https://gitlab.eclipse.org/eclipse/xfsc/cat

EDC has several extensions for this. These are based, for example, on Micrometre[65], JDK logger[66] or Events Cloud[67] and thus offer solutions for monitoring, logging, and event stream management.

FIWARE does not provide a single dedicated Observability Service; instead, it is designed to integrate seamlessly with widely used open-source monitoring and logging tools. Through the FIWARE Monitoring Generic Enabler (GEri)[68], monitoring data can be collected from heterogeneous sources, normalised, and exposed via NGSI APIs through the Orion Context Broker. This enables comprehensive monitoring, logging, and traceability of system and data performance across distributed environments.

In SIMPL, the so-called Observability component implements the Logging building block and part of the Monitoring building block, providing functionalities to collect and monitor logs and metrics from all other components of the SIMPL-Open agent. Although it interacts with every element. The key functions of the Observability component are monitoring technical logs of the SIMPL-Open agent infrastructure, automating the deployment of a preconfigured monitoring dashboard and monitoring business logs by logging all business actions in a central repository. Furthermore, it logs infrastructure metrics and stores technical logs of both the infrastructure and software components in a log repository. Additionally, a preconfigured monitoring dashboard for infrastructure metrics monitoring, facilitating comprehensive oversight of the agent's performance and activities, is offered.

4.2 Analysis of related Data Spaces and initiatives

When analysing other DS initiatives relevant to the project, we need to consider their design choices to ensure alignment, interoperability, and potential reuse within the architecture of the European Tourism Data Space (Annexe II).

4.2.1 Austrian Data Space

The Austrian Tourism Data Space[69] is a national initiative focused on enhancing interoperability and driving innovation in Austria's tourism sector. This data space initiative is designed in alignment with both the IDSA and the Gaia-X Federated X (Split) Model to support secure, sovereign, and interoperable data sharing. They implement an IDS RAM-like architecture to handle the technical aspects of the data exchange. A key element of this setup is the Eclipse Dataspace Connector (EDC) from Nexyo (an Austrian IT company), which facilitates secure data sharing and consumption while enforcing usage policies and ensuring traceability. By aligning with the X split model of Gaia-X, the data space further promotes technical compliance and fosters trust at the ecosystem level, while preserving data sovereignty for all participating actors.

[65] Eclipse EDC Micrometer: https://github.com/eclipse-edc/Connector/tree/main/extensions/common/metrics/micrometer-core
[66] Eclipse EDC Extension JDK logger: https://github.com/eclipse-edc/Connector/tree/main/extensions/common/monitor/monitor-jdk-logger
[67] Eclipse EDC CloudEvents Specification: https://github.com/eclipse-edc/Connector/tree/main/extensions/common/events/events-cloud-http

[68] GEri: https://app.readthedocs.org/projects/fiware-monitoring/downloads/pdf/develop/
[69] Austrian Tourism Data Space: https://www.tourism-dataspace.com/en

Within this framework, Austria Tourism (Austria's national tourism organisation) plays a pivotal role, acting as a Trust Anchor and Governance body, ensuring the data space operates in accordance with Gaia-X principles (see Figure 9).

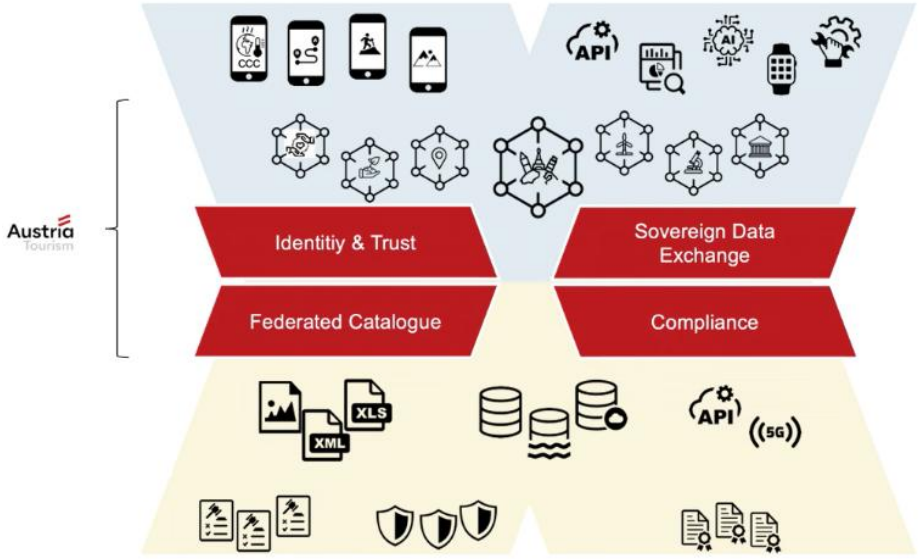

Figure 9 Austrian Tourism operating according to Gaia-X principles.

Similarly to the European landscape, the Austrian tourism sector is largely made up of SMEs with basic or limited technical expertise. To address this, the data space is designed as a B2B solution with a major motivation of creating simple, intuitive tools that lower entry barriers and actively encourage data sharing across the sector. Although this data space is intended to connect a wide range of businesses, stakeholders, and actors within the tourism sector, it is currently made up primarily of federal states' tourism organisations in its early stage of implementation (9 hubs in the federal states and one for Austria Tourism were implemented) .

The onboarding process concludes with the creation of a dedicated DataHub (SaaS) for each participant in the data space. This hub serves as the participant's interface to the ecosystem. For data providers, it is where data assets and usage policies are defined and managed. For data consumers, once a data offer is accepted, the resulting contractual agreements and access terms are stored and enforced. The identity of participants is ensured through the use of Decentralized Identifiers (DIDs) to foster compatibility, and each participant's DataHub manages the decentralised identity of the organisation which is part of. This setup ensures clarity, traceability, and full control over data sharing and usage within the trusted environment.

Most of the data shared by these organisations adhere to open data principles and, only in some cases, include additional defined access and usage policies. These policies are defined based on the ODRL model, in alignment with the standards established by the W3C. Access to the data is governed through an Attribute-Based Access Control (ABAC) mechanism. Sensitive data have not yet been shared within the data space, not due to technical limitations, but because there is no clear consensus on how to meet the legal and contractual obligations among the participant parties. This framework aims to provide full access control to the participants, so that they can only share data for which the interested party is eligible and nothing in addition. For those who wish to share highly sensitive data, vector embeddings, etc. it is foreseen that anonymisation, and/or any required pre-processing will take place on the data provider's own infrastructure and will be offered to the data space in the same way as any other data asset.

Looking ahead, the goal is to implement a fully decentralised, federated catalogue. This setup is shaped by the current maturity level of related EDC components, which limit immediate realisation. In parallel, the roadmap includes developing a marketplace and billing capabilities, alongside the integration of more advanced identity management standards, such as Verifiable Credentials (VCs), EU digital wallets, and full compliance with decentralised identity claims protocols. Additionally, the team is closely following the evolution of the SIMPL framework and remains open to a potential migration if requested by its customers.

4.2.2 EONA-X

EONA-X is a European data space for Mobility, Transport, and Tourism with the key objective of enhancing user experiences in mobility and tourism by providing seamless integration of travel and tourism data across various modes of transportation. To achieve that, the aim is to address the industry's key challenges by ensuring data sovereignty, guaranteeing privacy, and nurturing trade.

This section provides an overview of the key architecture principles and the high-level design, including descriptions of the main functional scenarios encountered in a data space.

Architecture principles

EONA-X's technical architecture aims to be interoperable and modular, while enabling self-sovereign and trustworthy data exchanges between actors. This is enabled by adhering to a set of principles detailed below.

Overall, EONA-X architecture principles are closely aligned with the Data Mesh concepts, which emphasise:

- A Distributed and Domain-Driven Architecture, where data is not centrally owned in a data lake or data platform but hosted and clearly owned by a business domain owner. This helps to avoid unnecessary duplication and ensure a clearly identified Source of Truth.
- To apply Product Thinking to Data, which means to make sure data is easily discoverable and addressable, of good quality, self-describing, interoperable and governed by standards, secured, and governed by global access control policies.
- A self-serve platform hiding all the underlying complexity and providing quick access to data in a self-service manner, with capabilities such as connecting once to reach many data sources, data publication and discovery, data versioning, unified data access control and logging, monitoring/alerting… to name just a few.

Exchange protocol & standards

Usage of strong protocols is essential for compatibility and interoperability of EONA-X technical solution within the larger data space landscape: Eona-X supports the IDSA protocol (now called "Dataspace Protocol", or "DSP": technical specification) for data space communication protocol (message types and API bindings). This is achieved by relying on the Eclipse Data Space Components (EDC), which implement this protocol as the default within the framework and thus provide ready-to-use extensions. In addition, the EDC follows the latest version of the IDSA rulebook regarding concepts and the organisation of data spaces. IDSA's principles aim for decentralisation as the default solution architecture, with centralised components where applicable and useful (feature-wise or to support business models).

The Dataspace Protocol (DSP) builds on well-established industry standards, such as the W3C DCAT V3 catalogue vocabulary and the W3C ODRL policy expression language, which enable interoperability with other data spaces.

Self-Sovereign Identity (SSI) management

The Identity and Access Management (IAM) strategy to be enforced for exchanges between components is configured by EONA-X when the data space is instantiated. As mentioned earlier, the EDC components are extensible and accommodate the data space IAM requirements.

The EDC provides out-of-the-box support for the OAuth2 industry-standard protocol for authorisation (relying on a centralised authorisation server to authorise access to the resources).

The EDC also provides support for decentralised identity management, as specified by W3C. This decentralised approach is based on the concept of Verifiable Credentials (VCs), which are a cryptographically signed set of attributes describing an entity (e.g., a person, a company...) that owns them. These VCs are granted by entities called VC issuers hereafter. A VC issuer can be an organisation, a government entity, or a data space ... Each data space can define a list of trusted and relevant VC issuers in its context.

This decentralised identity approach enables each participant to retain control over their identity and credentials. It removes the need for a centralised authorisation server that could become a single point of failure for the data space. Hereafter, we will focus on this decentralised identity management approach.

High-level design

The following high-level design diagram depicts the architecture's components. Solid bold lines represent mandatory components, and optional components are shown by dashed bold lines. All these components fall into five categories:

- **Data services** which cover the discovery of the datasets, the management of a common semantic throughout the data space, the contract negotiation and agreement process, and the data transfer.
- **Access control & trust services** which encompass the compliance with the trust framework defined for the data space (e.g., Gaia-X Trust Framework...) and the access control to the datasets.
- **Administration & governance services** which cover the management of the data space participant (on-boarding/exclusion of a participant), the auditing and billing.
- **Observability & alerting services** for the operational, functional, and environmental monitoring of the components.
- **User-facing services** which cover the portals =/dashboards used by the participant or data space operator to operate and monitor their components.

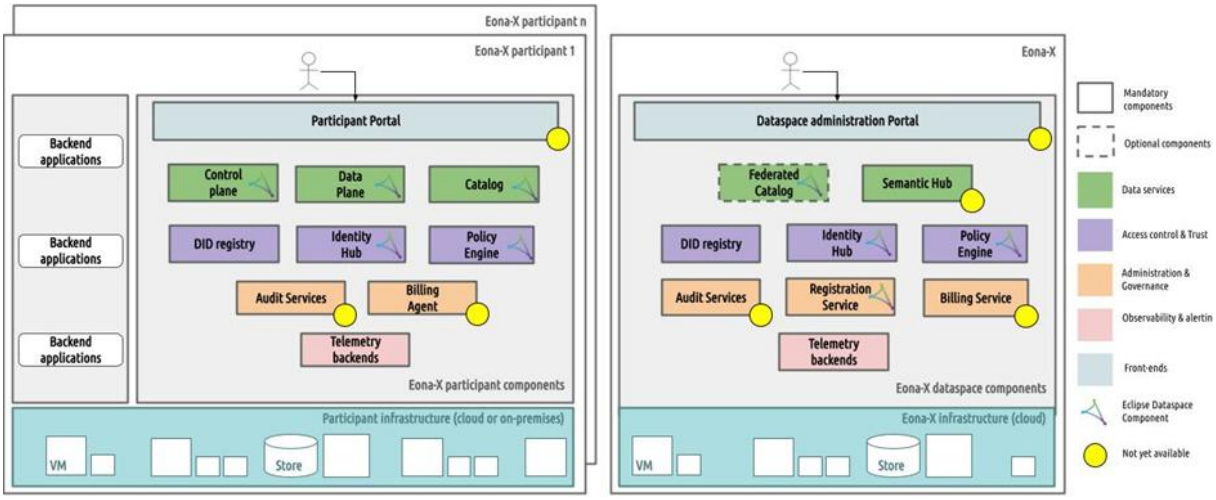

Figure 10 High-level design of the architecture.

The bottom blue layer of the diagram represents the infrastructure on which the EDC components are deployed. It is worth emphasising that the EDC components are cloud-agnostic by design and can be customised to work at scale in any environment (on-premises bare-metal, different cloud vendors, hybrid).

Components description

- **Control Plane:** The Control Plane is the core participant component responsible for managing the dataset offering (provider), negotiating access to the datasets (consumer), and orchestrating the data transfer. It utilises EDC technology and is currently available as a participant component.

- **Data Plane:** The Data Plane handles the actual data transfer once a contract has been established. It supports SIMPL data transfers, particularly via the REST API, and will support bulk data transfers (e.g., large-file transfers) and event streaming in the future. This component also uses EDC technology and is available as a participant component.
- **Catalogue:** The Catalogue component allows participants to expose offers configured in the Control Plane. It also enables crawling other participants' catalogues to discover datasets available within the data space. It embeds a search engine to facilitate the identification of relevant assets. This component uses EDC/DCAT technology and is available as a participant component.
- **Federated Catalogue:** The Federated Catalogue serves as the central entry point, crawling through all participant catalogues to discover datasets available within the data space. It embeds a search engine to facilitate the identification of relevant assets. This component uses EDC/DCAT technology and is available as an optional data space component.
- **Semantic Hub:** The Semantic Hub provides the semantic models of the datasets exposed by the data providers. The technology selection for this component has not yet been completed, and it is currently not available as a data space component.
- **DID Registry:** The DID Registry hosts the DID document of each entity, supporting the W3C specification. It operates as a standard HTTP server/DID-Web and is available for both participants and the data space.
- **Identity Hub:** The Identity Hub is a digital, decentralised wallet where each data space participant stores its Verifiable Credentials (VC) as per the W3C specification. This

component uses EDC/VCs technology and is available for both participants and the data space.

- **Policy Engine:** The Policy Engine enforces access and usage control based on the trusted attributes of the participants. It utilises EDC/ODRL technology and is available for both participants and the data space.
- **Billing Services:** Billing Services and Agents support various billing flows involved in a data space. The technology selection for this component has not yet been completed, and it is currently unavailable to participants or the data space.
- **Audit Services:** Audit Services are used for auditing purposes. They contain a log that records all actions performed by participants immutably. EONA-X can inspect participants through the data space Audit Services to ensure compliant behaviour and, if needed, undertake organisational or legal measures. The technology selection for this component has not yet been completed, and it is currently unavailable to participants or the data space.
- **Registration Service:** The Registration Service maintains an up-to-date list of participants. It serves as the entry point for onboarding new participants and for delivering the Verifiable Credential (VC) attesting that an entity is part of EONA-X. This component uses EDC technology and is available as a data space component.
- **Telemetry Backends:** Telemetry Backends collect, persist, and serve back telemetry data (metrics, logs, traces). They cover operational, functional, and environmental KPIs and can be used to enable alerting and enactment. This component uses OpenTelemetry technology and is available for both participants and the data space.

Functionality overview

This section provides a high-level description of the core functionality required for EONA-X to function as a data space.

- **Identity and Trust Management:** Self-Sovereign Identity (SSI) allows entities to share their identity while retaining ownership of their credentials and personal data. It uses Decentralised Identifiers (DIDs) to enable verifiable, decentralised digital identity. A DID can be resolved into a DID document, which describes the subject and how to interact with it. EONA-X architecture uses the DID: web method for DID resolution via an HTTP web server. DIDs can also enable Identity and Access Management (IAM) by introducing an Identity Hub, where subjects store their Verifiable Credentials (VCs). Trusted entities issue VCs, and EONA-X will act as a VC issuer during the onboarding process.
- **Asset management configuration / Control plane:** To expose a new dataset to other data space participants, the provider creates a Contract Offer, which includes an asset description, access policy, usage policy, and contract duration. If the data consumer meets the criteria and accepts the terms, a contract is generated. The data provider manages assets, policies, and contract offers through APIs exposed by the Control Plane component, either programmatically or via a participant portal.

Note that assets, policies, and contracts persist in a local database, whose technology is up to the participant as long as there is a suitable EDC extension for that technology. Newly created contract offers are then visible to other participants through the mechanism described in the following section.

- **Catalogue & Asset discovery:** Participants in the EONA-X data space can discover available assets provided by EONA-X providers through their local Catalogue component. The Catalogue regularly queries the data space Registration Service and

Control Plane to fetch and cache contract offers from all participants. Participants can then use the search API or Portal to find relevant assets, with access policies ensuring that only available offers are displayed.

- It is worth noting that even if the Catalogue is depicted as a participant component, it can also be deployed as a centralised data space component (*Federated Catalogue* in the HLD diagram above).
- **Policy engine:** The Policy Engine is an EDC component that supports onboarding and access control enforcement. It can be used as a library within other components or deployed as a standalone component callable through an API. The Policy Engine evaluates policies expressed in the W3C ODRL vocabulary against claims extracted from the caller's verified VCs. It returns true if the policy is fulfilled and false otherwise. Policies are bound to specific scopes, indicating when they should be evaluated during the process. Access is allowed only if all policies bound to the current scope are satisfied.
- **Data access request & contract management:** Based on the available contract offers returned by its Catalogue, a data consumer can identify relevant assets from the available contract offers in the Catalogue and initiate the negotiation process with the EONA-X provider through the Control Plane. The provider validates the caller's Verifiable Credentials (VCs) and access policy. It also ensures that the caller is an EONA-X participant.
- If validated, the negotiation process begins until an agreement is reached or cancelled. Upon agreement, both parties generate and store a digitally signed contract. The negotiation can be automatic or involve manual acceptance. The provider can revoke the contract if the terms are violated, resulting in the consumer losing access to the data.
- **Data plane:** After establishing a contract, the consumer can initiate data transfer through its Control Plane. The provider Control Plane validates the consumer's Verifiable Credentials (VCs) and policies before starting the transfer. Two transfer modes are supported within the EDC:
- *Consumer Pull*, where the consumer queries data from the provider using its Data Plane component.
- *Provider Push,* where the consumer specifies a sink for the data.
    - The data space operator provides credentials for secure querying in a connector-as-a-service setup. Future developments will support bulk data transfer by chunking and parallelising the data.

4.2.3 deployEMDS

This section describes the deployEMDS[70] reference implementation:

Within the technical section of the deployEMDS project, an analysis was conducted on the various technological stacks present across Europe for data spaces, EDC, and FIWARE. Since SIMPL was released in January 2025, it was not included in this technical analysis. After completing a series of tests, it was determined that, given the project requirements and the comparison between the two technologies, the Eclipse technology was chosen to support the use cases.

Although the EDC stack's capabilities outperformed those of the FIWARE stack, this does not imply that EDC is a fully developed, ready-to-use software stack for building a data space. In reality, EDC views itself more as a versatile toolbox that requires adaptation and extension to meet the specific needs of a data space.

[70] deployEMDS (EMDS): https://deployemds.eu/

In terms of architecture, the project follows the DSSC guidelines with the building blocks architecture mode (Figure 11).

The objectives of the architecture are as follows:

- Discoverability: Ensure harmonised discoverability of local and regional data offers at the European level.
- Entry Points: Facilitate access to the deployEMDS data space for local implementation sites and stakeholders to promote offers, negotiate digital contracts, and exchange data within use cases under agreed terms and conditions.
- Interlinking: Support the harmonised interlinking of existing data space identity schemas at the European level to enhance cross-data space interoperability.

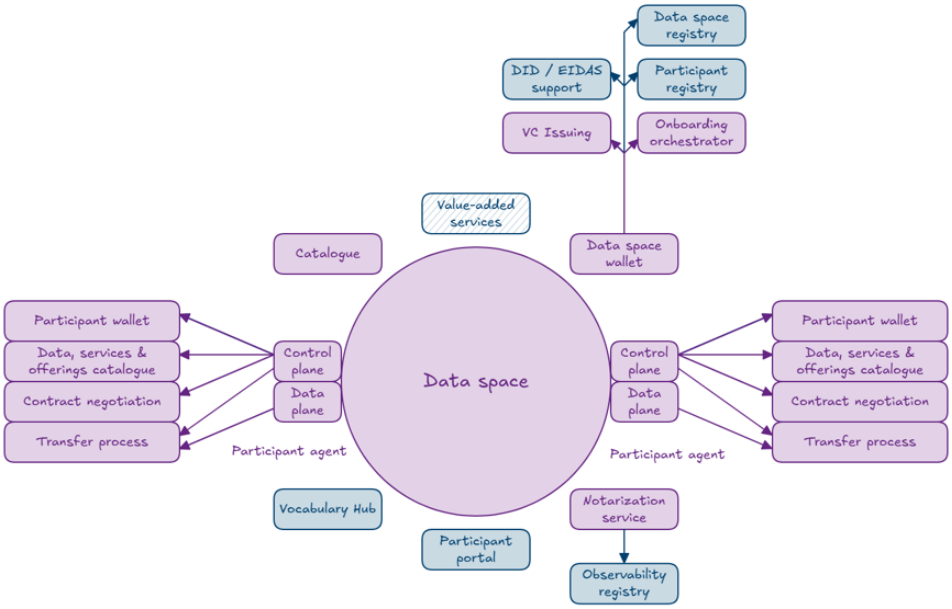

Figure 11 deployEMDS architecture overview.

The overall deployEMDS architecture must account for the fact that some implementation sites are already connected to an existing data space or have begun building their own, while others are starting from scratch. These existing data infrastructures vary significantly, as they were developed at different times and are based on diverse data space architectures or implementations. Figure 12 illustrates the various scenarios that the EMDS architecture encounters:

- Scenario A: EMDS participants with no relationship to an existing data space.
- Scenario B: The data space consists solely of participants connected to each other, for example, to implement one or more use cases. Central components, such as a catalogue, are either not operational or operational only for internal purposes, with minimal features, as in the Flanders Smart Data Space.
- Scenario C: A fully-fledged data space architecture with most central data space services in place, such as a participant portal, a catalogue, a participant registry, or a logging service. These data spaces are designed to be large data ecosystems or marketplaces that support a wide variety of use cases, such as Eona-X or the German Mobility Data Space[71].

[71] German Mobility Data Space: https://bmdv.bund.de/SharedDocs/EN/Articles/DG/mobility-data-space.html

- Scenario D: Similar to Scenario C, but where participants are more loosely coupled and no single data space operator exists to manage central services. Instead, the functionality of central services is distributed within the architecture, either operated by individual participants responsible for specific services or fully distributed among all participants using distributed ledger technologies.

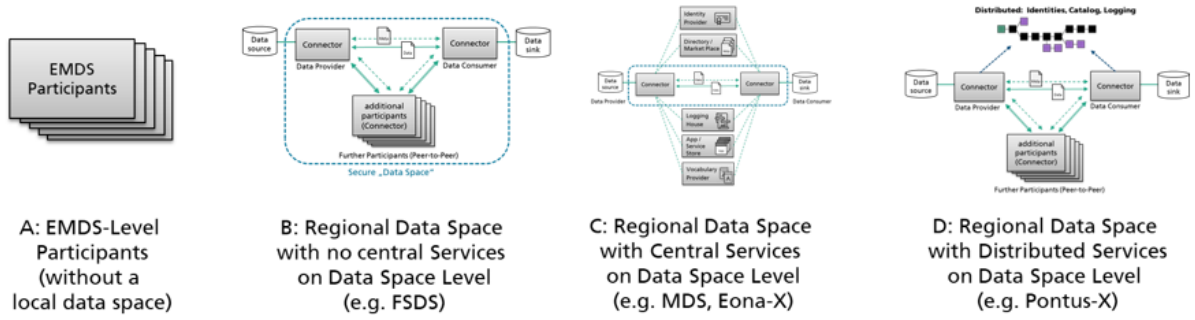

Figure 12 EMDS different architectural scenarios.

The deployEMDS architecture includes a central data catalogue for efficient data discovery across Europe, using harvesting mechanisms to synchronise existing data catalogues. The web-based interface allows users to search and filter data assets based on various criteria, ensuring effective data analysis and use. Additionally, the architecture aims to interlink participant identity and trust information through a central EMDS Federated Identity Registry. This registry collects and harmonises identity information, typically in the form of Decentralized Identifiers (DIDs), from various entities within different data spaces.

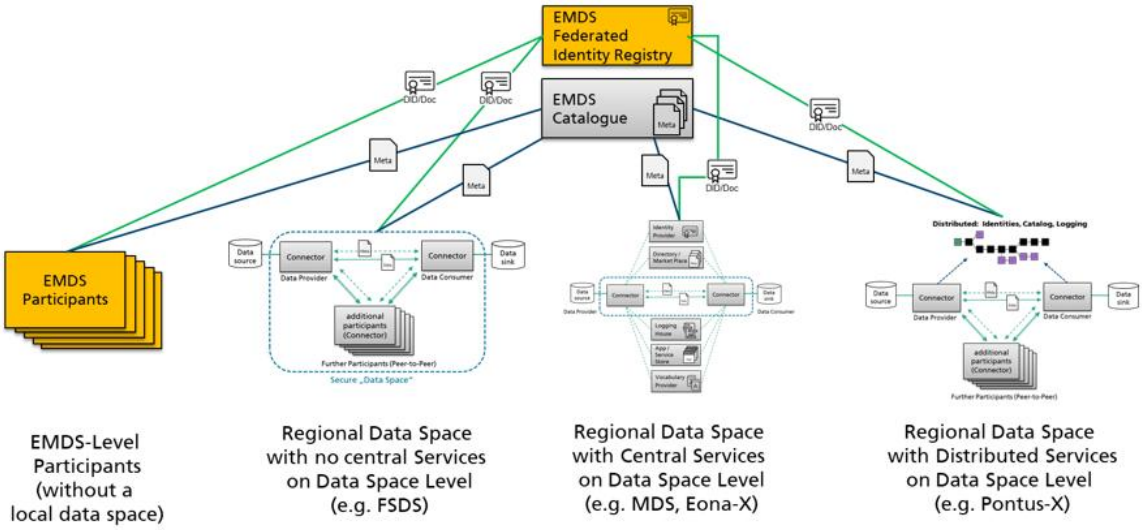

Figure 13 EMDS Decentralised Identifiers.

4.2.4 Cultural Heritage Data Space

This section aims to introduce the infrastructure underlying the Europeana platform[72], as well as the future basic architectures of the Cultural Heritage Data Space and the European Collaborative Cloud for Cultural Heritage (ECCCH) and their mapping.

[72]Cultural Heritage Data Space and Europeana platform: https://pro.europeana.eu/page/common-european-data-space-for-cultural-heritage

The Europeana Platform is the European Union's leading digital platform for cultural heritage, designed to support the digital transformation of the cultural sector across Europe. It aggregates and provides access to millions of cultural heritage items from museums, libraries, archives, and galleries, enabling users to explore, access, and reuse a vast amount of digitised cultural content.

It operates on a **c**entralised aggregation model, in which metadata from cultural institutions flows through trusted intermediaries, known as aggregators, into a centrally managed infrastructure. These aggregators ensure high data quality, legal compliance, and metadata standardisation.

The key layers of the platform, depicted in Figure 14, are:

- Europeana Portal**.** The public-facing platform where users can search and explore cultural heritage collections available on the platform. Each item includes metadata and links to the actual digital content, typically hosted on the provider's own site, and often some low-resolution representation or preview of the actual content. Access and usage policies are also provided for each asset, ensuring secure and compliant data sharing.
- Europeana APIs. A suite of programmatic interfaces that provide access to structured cultural metadata and content. They allow both Europeana Portal and external applications to query, retrieve, and reuse metadata from Europeana's central repository.
- Indexing and storage Layer, including such components.
- Europeana Pro complements the public portal by serving as the professional interface of the platform. It offers a comprehensive knowledge base for cultural heritage professionals, including documentation, standards, guidelines, case studies, and updates on policy and funding opportunities.
- Aggregation includes components from METIS, Europeana's metadata ingestion system, responsible for the ingestion and processing of metadata. METIS validates incoming metadata submissions, enriches them through services like multilingual label generation and linked data entity recognition, and publishes them in line with Europeana's quality standards. This system is essential for ensuring that the data shared through Europeana is clean, consistent, and ready for discovery and reuse.

Additionally, the Europeana Data Model (EDM) is the semantic framework that ensures metadata is standardised and interoperable across institutions. It provides an RDF-based framework for describing cultural heritage objects and their contextual relationships. EDM enables rich, interoperable metadata by capturing information about the object itself, its digital representations, its creators, subjects, associated places, and much more. The model supports multilingualism and the linked open data principles, and aligns with major cultural heritage standards such as Dublin Core, LIDO, and CIDOC CRM.

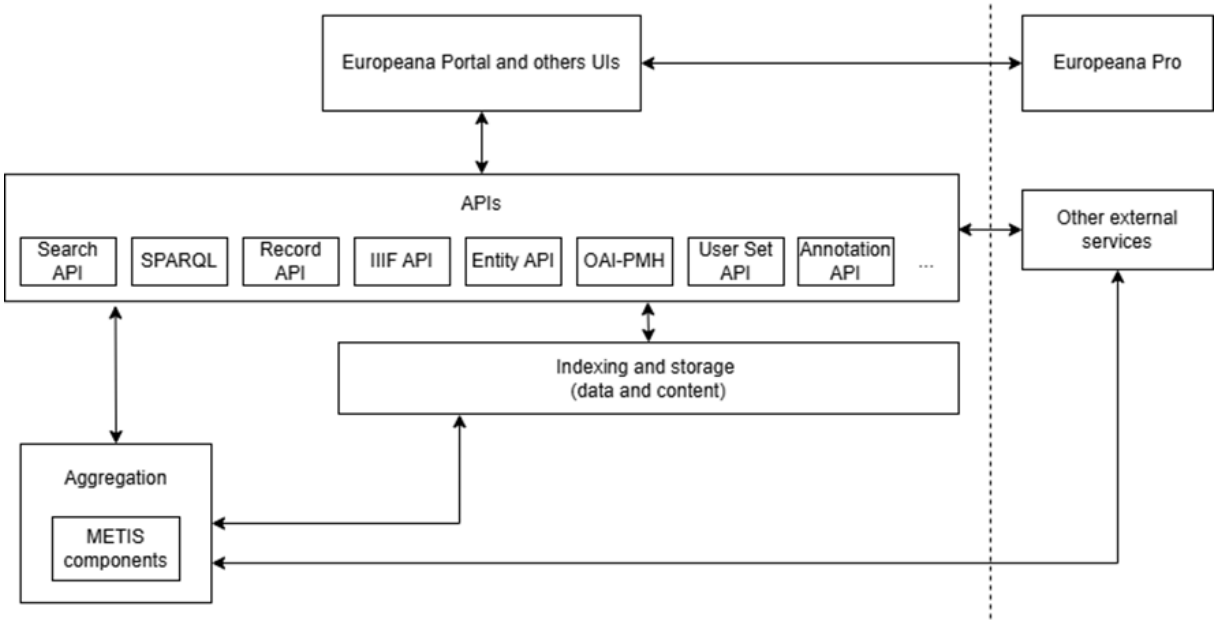

Figure 14 Key layers from Europeana Platform.

Regarding asset publication, Europeana follows a centralised process in which cultural institutions, mostly via aggregators, submit metadata for their digital objects. Once validated and ingested through Europeana's Metis system, these records are made accessible through standardised APIs, allowing third-party systems to query, filter, and reuse cultural heritage metadata at scale. Unlike federated data spaces, where metadata remains distributed and is accessed via decentralised, peer-to-peer API frameworks, Europeana aggregates and indexes data centrally, offering a unified, optimised API layer.

While the metadata flow is centralised, the federated aspect is supported by the distribution of the actual content across the data providers' own repositories. Most of the organisations participating in this initiative adhere to open data principles, as the Europeana initiative strongly encourages sharing the data as openly as possible to boost the reuse of digitalised cultural data. For the few who may not, efforts have been made to avoid the inclusion of overly complex mechanisms for data acquisition or related negotiations.

Usage policies are translated into standardised rights statements. These machine-readable declarations indicate the copyright status of a digital object and clarify whether it can be reused and, if so, under what conditions. These statements, provided by the content owners, accompany each digital asset and serve as both legal and technical indicators to help users understand how the content may be reused. However, the actual enforcement of access and usage policies is the responsibility of the content providers themselves, carried out through their own legal terms and technical measures. While rights statements are essential for ensuring transparency and enabling content filtering, it is ultimately up to each provider to implement and enforce the appropriate policies. Each data provider retains full control over access to their digital assets.

Following that, the Common European Data Space for Cultural Heritage builds on the existing functionalities and services of the Europeana Platform, which already provides access to millions of digitised cultural heritage items from across Europe. As mentioned, the platform offers mature tools for metadata ingestion, semantic enrichment, multilingual discovery, and

API-based reuse. Their goal is to move away from the centralised Europeana approach and implement and provide access to these additional services in a decentralised manner.

This data space initiative aims to expand the functionalities of the existing infrastructure to increase the availability, quality, and interoperability of cultural heritage data, with a special focus on 3D content, open licensing, and reuse in education, tourism, research, and creative sectors. Major efforts are being invested in identifying and implementing additional data services that may be useful within the cultural heritage domain, as well as in improving the quality and availability of cultural data by investing in data annotation and enrichment services with a focus on completeness, semantic enrichment, and multilingualism.

To summarise, while several principles of the CHDS, such as data sovereignty and metadata interoperability, are aligned with the IDSA framework, the initiative does not fully adhere to it. IDSA, along with initiatives such as Gaia-X, promotes a decentralised, federated approach to data sharing, where both data and metadata remain distributed and are accessed through secure, transparent peer-to-peer mechanisms. In contrast, this initiative lacks a basic data catalogue (e.g., DCAT) and instead relies on built-in functionalities that allow direct interaction with the data. It uses a centralised metadata aggregation model, with metadata stored and accessed via a central infrastructure. Furthermore, the absence of essential components such as connectors, identity and trust services, and usage control mechanisms highlights a significant departure from IDSA-like architectures.

Finally, the European Collaborative Cloud for Cultural Heritage (ECCCH) is a Horizon Europe initiative running from June 2024 to May 2029, designed to create a digital collaborative workspace for cultural heritage professionals and researchers. The ECHOES project[73] is responsible for building the core infrastructure, governance model, and virtual environment that will form the backbone of the ECCCH. Anchored in Open Science principles, ECHOES will enable the secure flow of data between the Cultural Heritage Data Space and the Cloud, promoting reuse and the creation of semantically rich Digital Commons. Projects funded under ECCCH-related calls are expected to integrate with ECHOES by implementing modular, API-accessible services and aligning their data models with the platform's evolving architecture. Interoperability with common data formats (e.g., RDF), open metadata models, and open-access APIs is essential, and ECHOES will provide detailed integration guidelines. Funded projects must dedicate resources to ensure technical compatibility, flexible design, and effective collaboration within the ECCCH ecosystem.

4.3 Establishing the Minimum Viable Data Space

A Minimum Viable Data Space (MVDS) is an integration of components that enable the creation of a Data Space, with elemental features that support a usable, secure process for sovereign data exchange.

The main intention is to facilitate processes so the development team can deliver a first version, which is iterated to respond to the requirements of the Data Space.

Here, we take into account that the participant will use a connector delivered as CaaS (Connector as a Service) by the ETDS, meaning this data space hosts the connector, while

[73] https://www.echoes-eccch.eu/

each participant receives access to their own dedicated connector domain (i.e., requiring specific configuration and extensions as needed).

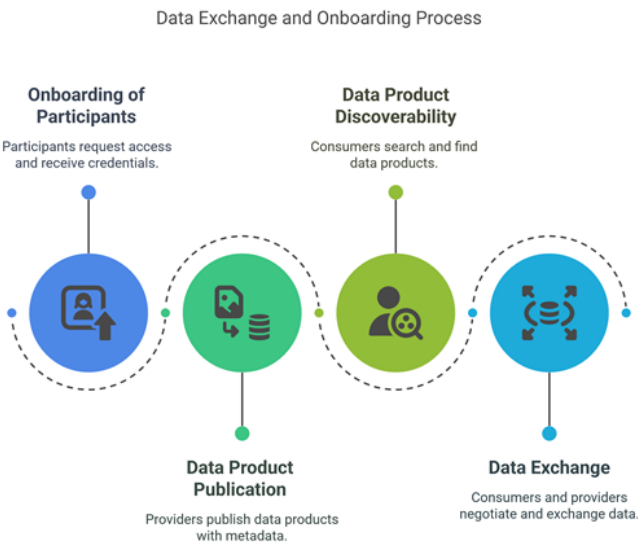

Figure 15 Data Exchange and Onboarding Process.

4.3.1 Onboarding of participants

This section describes how participant onboarding will be implemented. As a starting point, three key agents are involved in the process: the data space authority, the data provider, the data consumer and participants.

- The data space governance authority is the entity responsible for the governance.
- Data provider is the entity responsible for providing and supplying data to the Data Space Portal. On the other hand, a data consumer is the entity that consumes data.
- A participant is either a data space authority, a data provider or a data consumer who joins the data space.

The onboarding process involves five main steps:

4.3.1.1 DS pre-onboarding

The participant completes a request, which is the formal petition to access the ETDS via the Data Space Portal. The request requires identification attributes to proceed with the registration.

4.3.1.2 Registration

Through the Data Space Portal, and once the participant has sent the petition, a new entry in the Data Space Registry is generated.

The Data Space Registry requires that the data space be described and that the data space governance authority define Data Space rules and policies, and that these be machine-readable to automate the process. Based on these data space rules and policies, the Data Space Registry manages participant registration, which can occur in two phases: onboarding

or offboarding. Hence, a list of trust anchors is obtainable, representing the external entities responsible for validating specific claims about participants. These validations serve as the basis for issuing internal Verifiable Credentials (VCs), which ultimately identify and establish the list of trusted participants. Lastly, the Data Space Registry permits issuing and storing, through protocols, a verifiable credential (VC) that identifies each participant.

4.3.1.3 Management of the registration

The next step is to conduct an assessment, during which the Data Space Governance Authority manages the participant's request. Two scenarios diverge from this point: if the request is accepted, the process will proceed; if it is rejected, the participant must submit a new request.

4.3.1.4 VC issuing

Supported by the Data Space Registry, a verifiable credential (VC) is issued and eventually integrated into a wallet, serving as the digital identifier throughout the Data Space.

4.3.1.5 Participant VC

Given the conclusion of the previous steps, the participant is notified of the access, tries the VC, and their role is converted to data provider or data consumer within the Data Space.

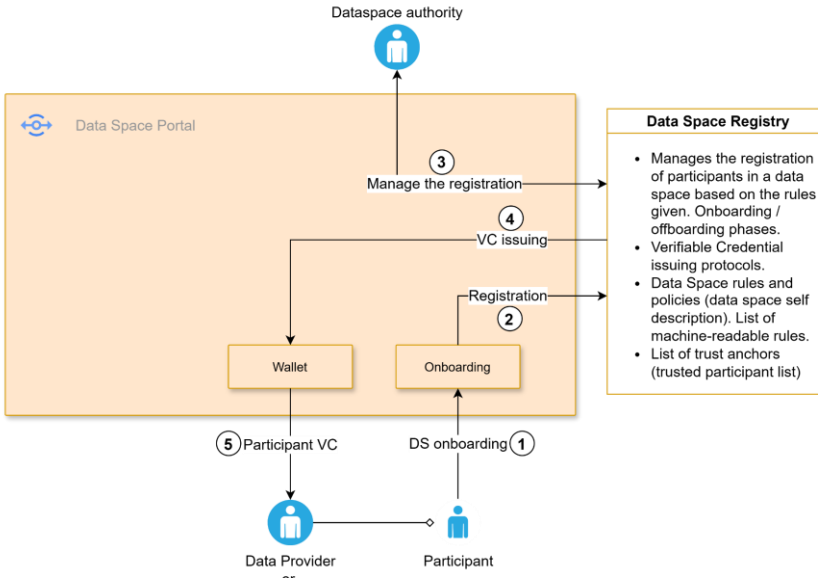

Figure 16 Onboarding of participants diagram.

4.3.2 Data product publication

Once the participant is registered in the Data Space with the role of data provider, they are allowed to publish datasets throughout the resource catalogue.

The data product publication process involves seven main steps:

4.3.2.1 DS authentication

The data provider undergoes identification, using the provided VC through Data Space Portal and stored in the wallet.

4.3.2.2 Authorisation

The Data Space Portal ensures the authentication, connected to the Data Space Registry, determining the data provider is allowed to publish new datasets.

4.3.2.3 Provide data product metadata

On previous data provider authentication and authorisation, next the data provider selects the dataset publication, describes the metadata and policies of the offering.

4.3.2.4 Get data model

The published datasets require to be described following standards to ensure the overall platform is meeting vocabulary standards, providing semantic interoperability. In order to enhance the metadata description, the vocabulary service supplies tools to manage and organise semantic resources, granting coherence and interoperability. It includes resources in terms of vocabulary, ontologies, application profiles and data schemes.

4.3.2.5 Data space connector

The information regarding the dataset and their metadata is then validated through the cataloguing function of the ETDS.

4.3.2.6 Catalogue publication

Eventually, the offering is published to the catalogue of resources.

4.3.2.7 Returns the status

The status of the publication returns to the Data Space Catalogue and the Portal, which is shown to the data provider.

The process of updating an offering alludes to the metadata of the offering, modified by the data provider in a similar process to data product publications. Given the nature of the process, it shall not have a critical impact on signed contracts.

Removing an offering implies an intermediate status of the publication: unpublish. On unpublished status, all data consumers are notified, subsequently, the contract extinction is formalised. From that point forward, deletion can be allowed.

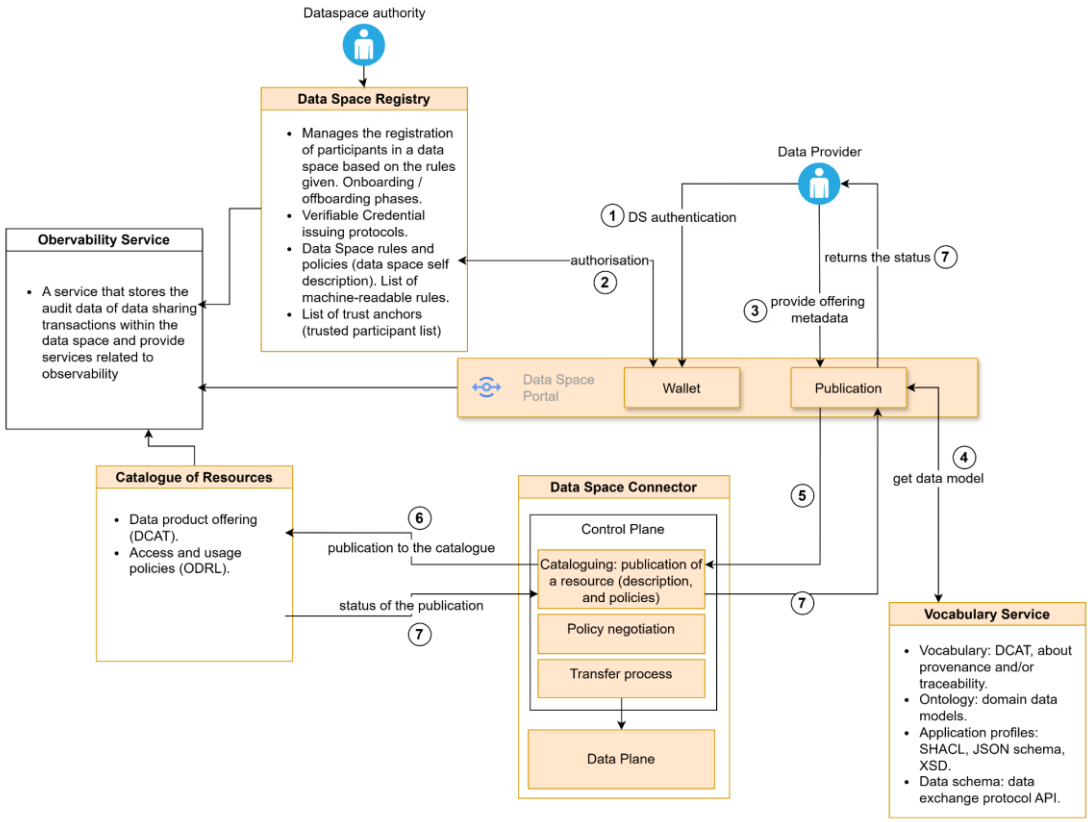

Figure 17 Data product publication diagram.

4.3.3 Data product discoverability

Discovery of data products within the resource catalogue allows the data consumer to query datasets, view what they contain, and review their use policies.

4.3.3.1 DS authentication

The data consumer undergoes identification using the provided VC from the Data Space Portal, which is stored in the wallet.

4.3.3.2 Authorisation

The Data Space Portal ensures authentication, connected to the Data Space Registry, and determines whether the data consumer is allowed to search for datasets.

4.3.3.3 Search for an offering

Once the data consumer is authenticated and authorised, the data consumer queries an offering through simple or advanced search, filters, categories aligned to controlled vocabularies. Queries are executed in the resource catalogue through the Data Space Connector.

4.3.3.4 Return of the offerings

Lastly, the resource catalogue retrieves the available offering list that is suitable based on the filtered searches. As a consequence, the information is returned to the data consumer.

Every transaction is monitored by the Observability Service, which stores and audits the actions within the Data Space. Overall, the focus is to trace datasets plus ensure the provenance.

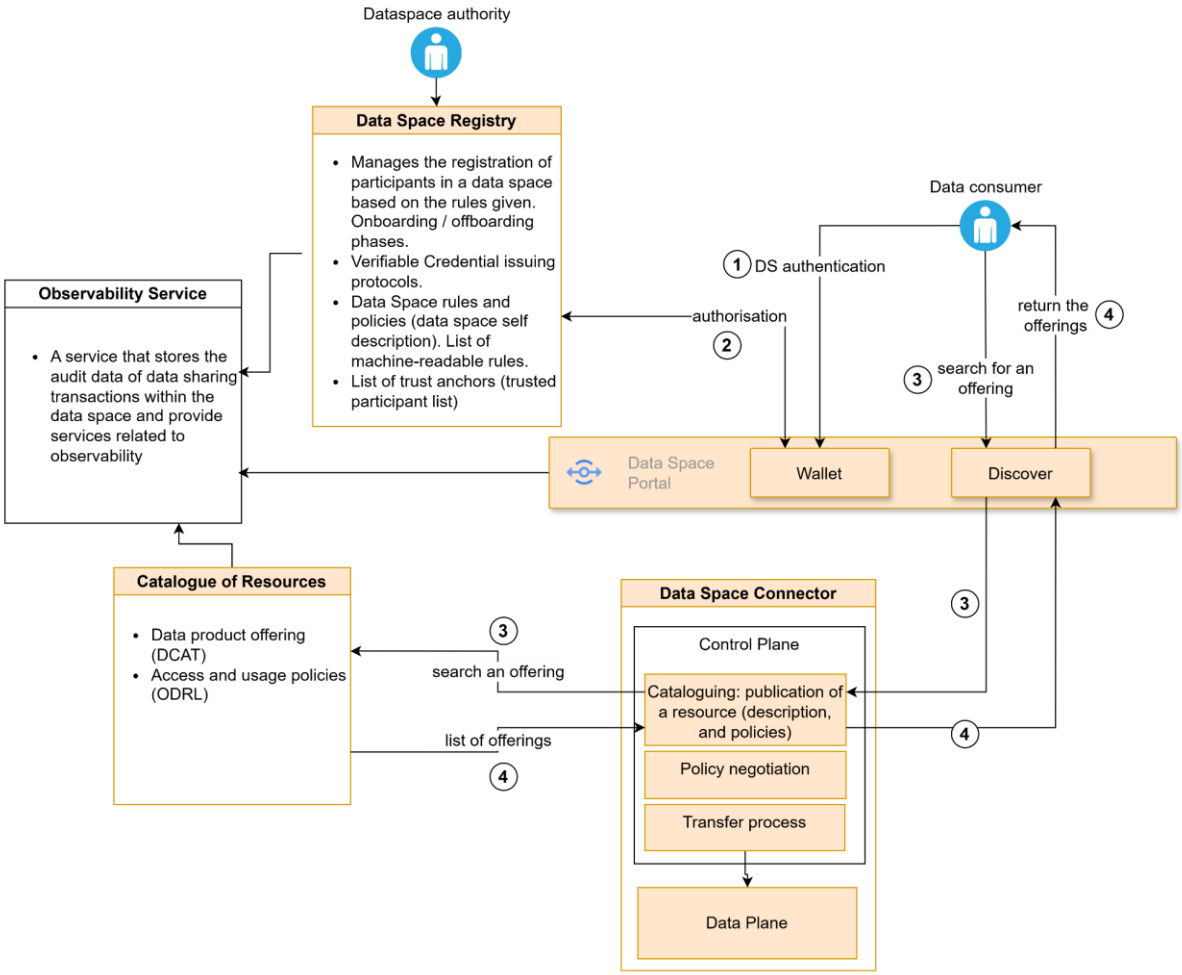

Figure 18 Data product discoverability diagram.

4.3.4 Contract negotiation

The Contract negotiation phase is central to establishing an agreement between the data provider and the data consumer. This phase occurs in the Control Plane, where both parties agree on the conditions for data use, ensuring the data provider retains ownership and control over their dataset. The negotiation process is essential for determining the terms of use, access rights, and obligations before data exchange can occur.

4.3.5 Data exchange

Data exchange relies on a centralised ecosystem that allows potential data sharing between different organisations or companies. This process occurs in the Data Plane, which enables actual data transactions to take place once a contract has been formally agreed upon. Data exchange is conducted after the contract negotiation phase, and transaction details are documented in a machine-readable format for transparency and traceability.

4.3.5.1 Request a contract for an offer

The data consumer requests a contract for a dataset, which is sent to the Data Space Connector's policy negotiator.

4.3.5.2 Negotiation protocol

The data consumer runs a negotiation through the data provider connector.

4.3.5.3 Agreement/rejection of the offer

The data provider connector shares the offer with the data provider, who decides whether to accept or reject it. Given the scenario of a rejection, the negotiation concludes.

4.3.5.4 Persist agreement

Given an agreement, both agents sign the contract, which is stored on each Data Space Connector.

The Observability Service monitors every transaction, storing and auditing actions within the Data Space, enabling further data transactions.

Data transactions imply that every agent is authenticated and authorised beforehand to ensure the process complies with privacy and security requirements.

The data consumer is the agent that initiates the data transaction, regardless of the transaction features. The core intention is to facilitate the transaction in accordance with the previous contract negotiations.

- Initiate request: The data consumer requests the dataset transaction through the access token given at the negotiating process.
- Data transferring: The data consumer connector transmits the request to the data provider connector.
- Verification: PEP (Policy Enforcement Point) receives the request, verifies the token access and authorises the request. It is then transferred to the PDP (Policy Decision Point), where the policies are evaluated. To ensure the transaction, PDP inquires the agreement to PAP (Policy Administration Point), which verifies the policy agreement.
- Data exchange: Assuming that the Policy Decision Point (PDP) authorises the request, the data exchange proceeds through the data plane of both connectors. On completion, data consumers can visualise the datasets.

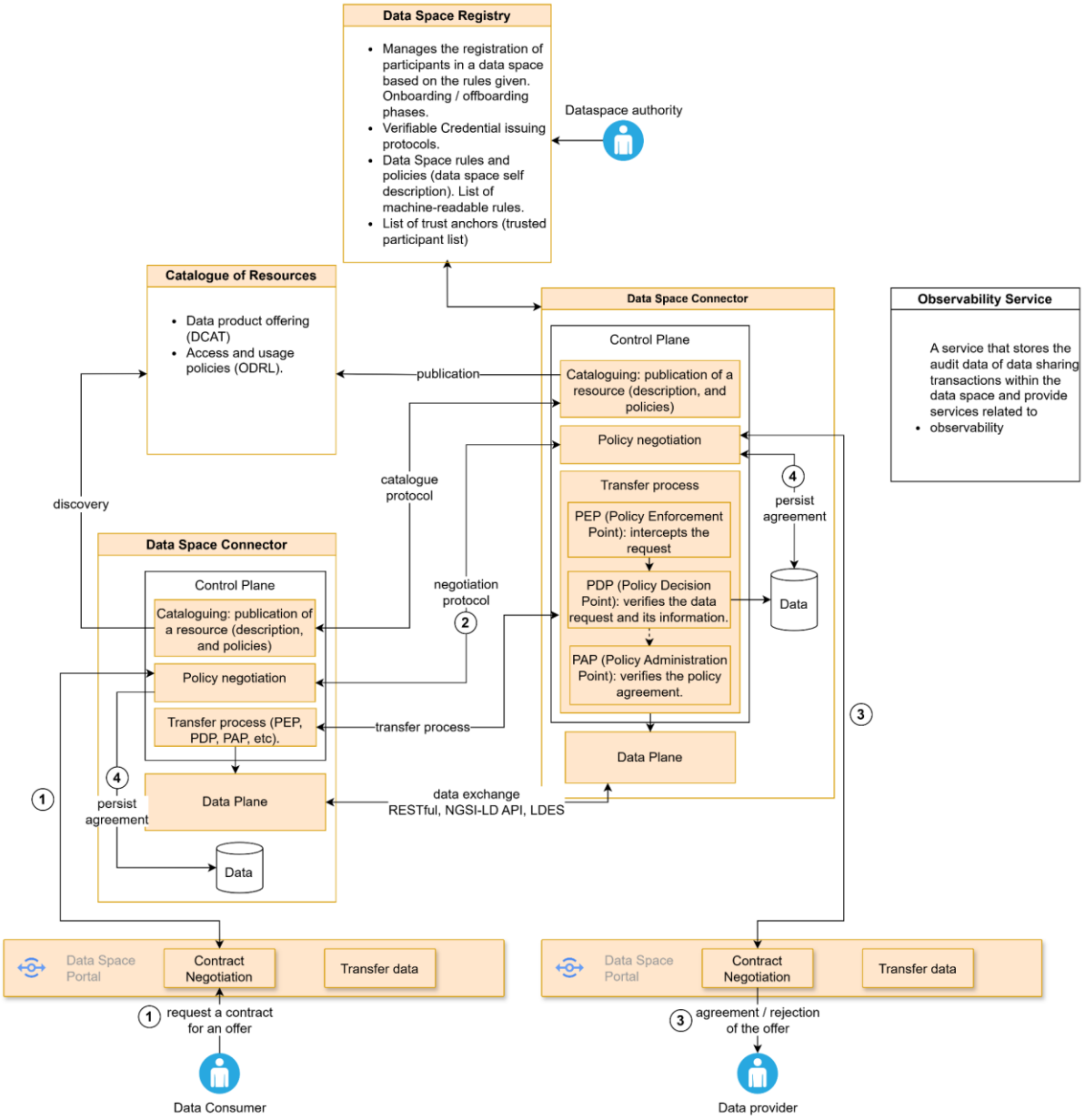

Figure 19 Data product exchange diagram.

4.4 Technological Stack decision

The technological stack should be the most suitable to build a federated data space architecture. During the assessment of existing technological stacks, the EDC emerged as a flexible and extensible option, though it requires additional configuration to meet specific use-case requirements. Notably, EDC is being progressively embedded into the SIMPL middleware, reinforcing its relevance as a European-ready technological stack within data space initiatives and, by extension, the ETDS.

Decisions regarding stack adoption should be based on the maturity of solutions assessed during prior use-case development. These considerations must reflect not only what pilots are eliciting but also the evolving ecosystem of data space-related initiatives, such as Europeana, CHDS, deployEMDS, and Eona-X, which depict a hybrid landscape where centralised and

decentralised services coexist. Additionally, alignment with the DSP should be ensured to guarantee interoperability and compliance across the data space ecosystem.

Disclaimer: This section is incomplete. A primary analysis of data space-related initiatives showcases the varied architectures used for data sharing and access across different platforms and databases. The technological stack for the ETDS and the related decisions on the total or partial use of existing solutions (e.g., SIMPL) will not be finalised until the conclusion of the use case analysis.

Furthermore, during the assessment of stacks, some initiatives illustrated that distributed systems and their federation have become architectural imperatives. However, simultaneously, centralised portals will continue to play essential roles in functions like data enrichment and discoverability; or, even more supportive middleware technology will have to be provided to leverage deficiencies among EU data space standards, such as IDSA and Gaia-X, where missing components undermine the overall operating system and prevent the deployment of MVDS. By requiring participants to go through the onboarding process and use compatible technologies (such as connectors and trust frameworks), the ETDS ensures that, regardless of how they manage their data internally (centrally or in a decentralised manner), their external behaviour within the data space respects data sovereignty and the network's decentralised rules.

This assessment also reveals key limitations that should be addressed in subsequent iterations to confirm the identification of requirements, their grouping, and the scalability and interoperability of either stack in the context of the ETDS.

5 European Tourism Data Space Architecture

This section depicts the architecture of the ETDS with a focus on federated services and catalogues. Additionally, the design of a high-level architecture for this sectoral data space is also foreseen.

5.1 DEPLOYTOUR as a Federated Data Space Architecture

This section lists the minimum components of the ETDS enabling the federation of different data spaces. Because the ETDS is intended to act as a future-proof, overarching infrastructure for tourism data sharing, these components must ensure interoperability with other European sectoral data spaces. These data spaces are the Cultural Heritage Data Space, deployEMDS, and others such as EONA-X and the Austrian Data Space.

The requirements elicited from the deliverable “ETDS Interoperability & Data Sharing” are not explicit in the definition of the ETDS as a federated data space and will need to continue refining in successive iterations.

Eclipse EDC has already proposed implementations[74] of the GAIA-X architecture, specifically for federation of catalogues, consisting of multiple components and reusing existing technology and allowing scaling (among them, authentication, verification of credentials and registry of participants)[75].

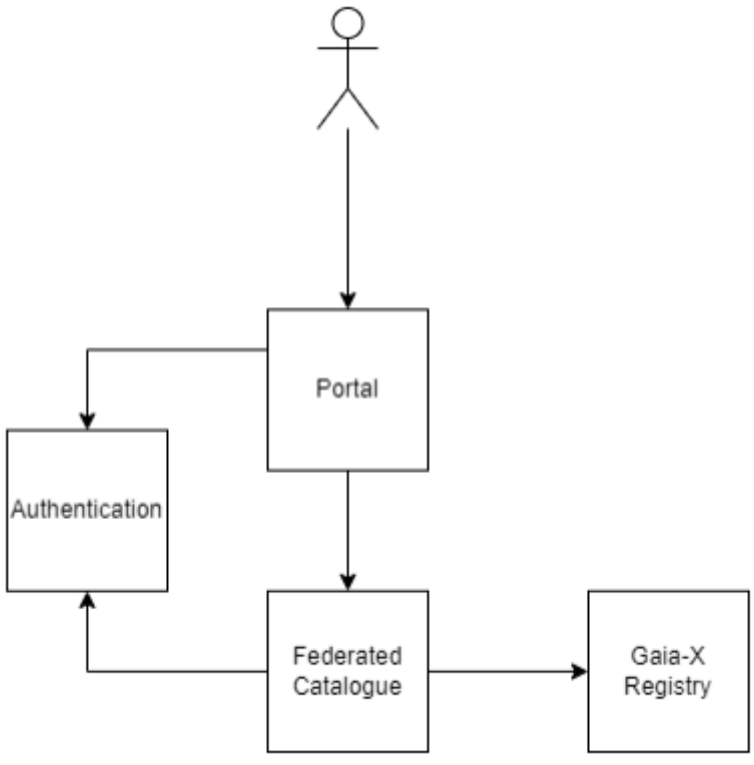

Figure 20 Overview of the architecture of the Federated Catalogue, according to GAIA-X.

[74] Architecture document for the GXFS Catalogue: https://gitlab.eclipse.org/eclipse/xfsc/cat/architecture-document

[75] Some of the EDC implementations proposes Keycloak for authentication by means of JWT, the verification of Verifiable Credentials (self-descriptions) and the registry where trust providers allow the certification of those credentials.

5.1.1 First approach to the final architecture: implementing Self-Sovereign Identity (SSI)

This proposal recommends that the Tourism Data Space adopt a Self-Sovereign Identity (SSI) framework based on the W3C Decentralised Identifier (DID) standard. This approach enables decentralised identity and verifiable credential exchange using standard web protocols, offering enhanced user control, data protection, and interoperability. The proposal aligns with implementations already underway in leading data space initiatives, such as EONA-X and the Austrian Tourism Data Space, both of which utilise a similar architecture with secure data exchange mechanisms based on the Eclipse Dataspace Components (EDC).

In a data space environment, Identity and Access Management (IAM) should be decentralised, interoperable, and privacy-preserving. SSI provides a foundation for achieving this by empowering each actor to control its own identity and access policies. In the tourism domain, this includes travel providers, businesses, service platforms, and regulatory bodies.

Understanding the did: web method.

The did: web method allows organisations and individuals to create decentralised identifiers. Each identifier links to a DID document that contains metadata, such as public keys and authentication methods. This offers a standards-based mechanism for trust. Organisations retain full control of their digital identities and can make their metadata publicly verifiable, ensuring trustworthy interactions between parties.

A DID refers to a unique entity, called the subject, and is designed so it can be decoupled from centralised registries, identity providers, and certificate authorities.

A DID can be resolved into a DID document, which is a set of data describing the subject and how to interact with it in a trustworthy way. It typically contains the endpoints (services) exposed by the subject, along with verification methods and cryptographic material.

The process that takes a DID as input and returns a DID document is called DID resolution. The DID includes a method that refers to a dedicated specification explaining how the DID document can be resolved, depending on the nature of the registry in which the DID document persists.

Specifically, the architecture relies on the DID: web method, which exposes the DID registry via an HTTP server.

DID can be leveraged to enable IAM by also introducing an Identity Hub (or Decentralised Web Node[76]), which is a data storage where each subject stores its VCs. The endpoint for the subject's Identity Hub is made public via the subject's DID document. Thus, when two subjects interact with each other in such an ecosystem, the caller provides its DID in the request (step 1), enabling the callee to:

- Resolve the caller's DID into a DID document (step 2),
- Retrieve the Caller's Identity Hub endpoint from the DID document (step 3),
- Request the caller's Verifiable Credentials to its Identity Hub (step 4).

[76] Decentralized Web Node: https://identity.foundation/decentralized-web-node/spec/

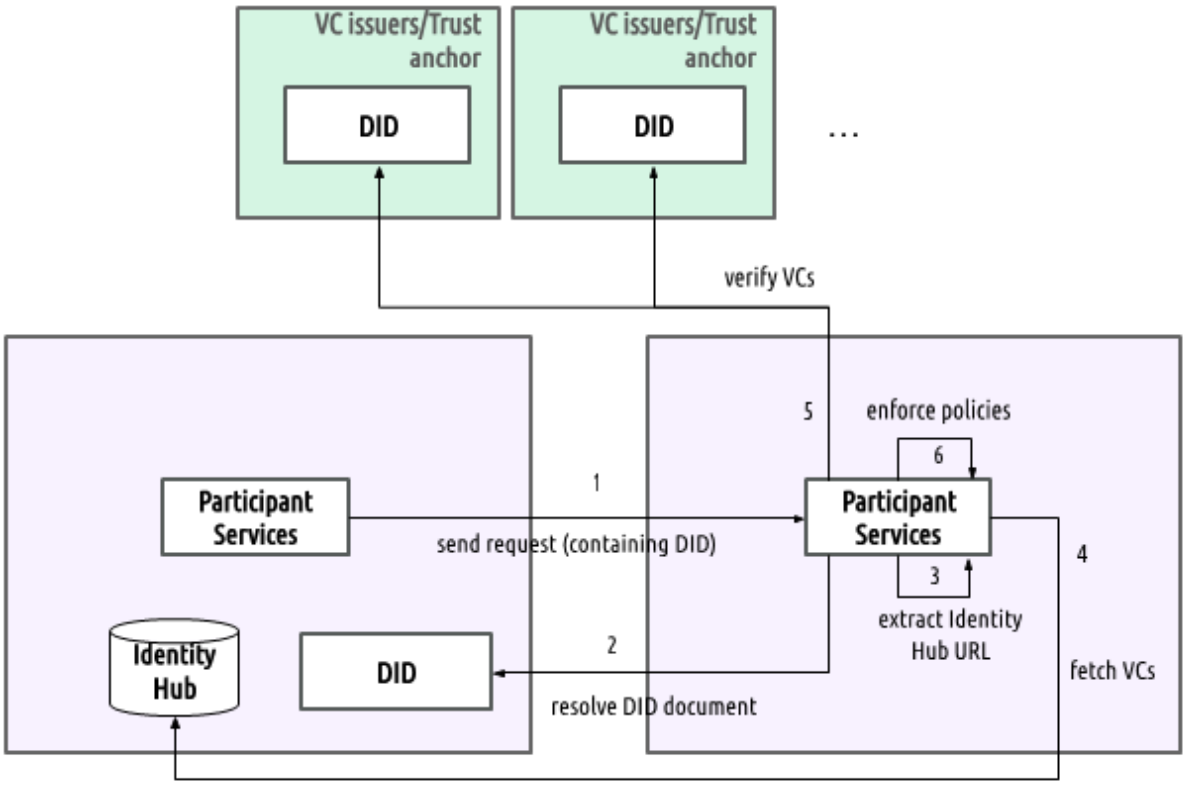

Figure 21 Participant authentication and access control in a SSI context.

Once the caller's VCs have been retrieved, the callee verifies them (check digital signature, step 5) and uses its Policy Engine to evaluate the underlying claims against the policies which are defined in the current context (step 6).

The VCs of each subject are granted by external entities called VC Issuers hereafter. A VC Issuer can be a government or an organisation. Each data space typically defines a list of trustworthy and relevant VC Issuers in its context, called the Trust Anchors. The following diagram illustrates the complete IAM process described above.

As an important consideration, implementing Attribute-Based Access Control (ABAC) to leverage VC and dynamically evaluate access conditions will enable more contextual, role-specific access control, extending beyond simple role-based schemes.

5.1.2 Conclusion

This model fosters secure, trusted data exchange while ensuring that identity management is decentralised, standards-based, and aligned with European digital sovereignty objectives. It enables alignment with other pioneering efforts such as EONA-X and the Austrian Tourism Data Space, paving the way for a broader, interoperable European tourism ecosystem that prioritises trust, autonomy, and data protection.

5.2 High level Architecture design

This section aims to provide a first look at the high-level architecture of the ETDS. The proposed high-level architecture is not intended to describe the various layers of the ETDS reference architecture but rather to provide a general perspective on how the data space should be structured.

5.2.1 Recommendations

The Consortium considers using a standardised language to describe the different capabilities defined in the requirements collection. These languages are the Business Process Model and Notation[77] (BPMN), the Unified Modelling Language[78] (UML) and the ArchiMate specification[79]. The Object Management Group maintains these three languages.[80] (OMG) and can be used in open-access tools such as Modelio[81] or Archi[82]. According to the Open Group website[83], among the main benefits of using these languages are:

- ensure clarity in communication across stakeholders;
- modelling of capabilities and strategic goals;
- representation of services and interfaces that are distinct from the modelling language implementation;
- customisable viewpoints for the stakeholders' perspectives;
- modelling of executable workflows, tasks, processes, among others;
- provides means for documenting, using diagrams, component relationships, etc.;
- representation of behavioural aspects, and given the case actors and use cases.

Although BPMN is proposed by the DATES/DSFT Blueprint, the most suitable modelling standard for this initial stage of the ETDS reference architecture is ArchiMate. While UML uses a formal language for designing any type of software component or system, BPMN is more appropriate for modelling workflows and processes. The ArchiMate language is particularly well-suited for a higher modelling level. In terms of practicality, only ArchiMate is used as the modelling language that sticks to an architecture framework at the EU level.

The latter is probably less suited compared to BPMN for providing details on the different architecture layers, but offers a simpler means to represent the data space components from an enterprise architecture viewpoint. Besides, the main benefit of using ArchiMate is the possibility to adopt reference architectures at the EU level, such as the EIRA/eGovERA Business Agnostic Reference Architecture[84] 6.1.0, which is modelled through the Cartography Tool (CarTool©) via the Archi plug-in for EIRA[85].

5.2.2 ETDS high-level architecture

As analysed in section 3.2.6.1, the EIRA approach enables the analysis of requirements in an existing reference architecture, or the design of a target solution use case in an agnostic manner. This flexibility allows different problems or requirements to be addressed independently and without a specific sequence. For example, APIs can be analysed and designed from abstract Architecture Building Blocks (ABBs) to concrete Solution Building Blocks (SBBs) such as OpenAPI specifications, even if the data model or vocabulary for describing data offerings has not yet been fully resolved. This approach supports varying levels

[77] BPMN: https://www.omg.org/spec/BPMN
[78] UML: https://www.omg.org/spec/UML/2.5.1/About-UML/
[79] ArchiMate: https://pubs.opengroup.org/architecture/archimate32-doc/_archimate_3_2_specification.html
[80] OMG: https://www.omg.org/
[81] Modelio: https://www.modelio.org/index.htm
[82] Archi: https://www.archimatetool.com/download/
[83] "Relationship to Other Standards, Specifications, and Guidance Documents", found in Appendix D of the *ArchiMate® 3.1 Specification* documentation (The Open Group): https://pubs.opengroup.org/architecture/archimate31-doc/apdxd.html
[84] eGovERA Business Agnostic RA: https://cartool-ec.github.io/eGovERA_BA_RA/index.html?view=id-41fe8a5febed4b4ba2e2c3d45a2772ad
[85] EIRA Archi plug-ins: https://interoperable-europe.ec.europa.eu/collection/european-interoperability-reference-architecture-eira/solution/cartography-tool; Archi plug-ins list in: https://www.archimatetool.com/plugins/

of granularity across different views or even within the same view, ensuring adaptability to the specific needs of each pilot.

Building upon this foundation, the eGoveERA framework provides a structured methodology particularly suited to the modelling of Data Spaces, ensuring consistency with the European Interoperability Framework (EIF) and alignment with initiatives such as Gaia-X. Within this approach, interoperability is addressed through four complementary layers: Organisational, Legal, Semantic and Technical enablers of the ETDS.

The following subsections present the ETDS high-level architecture across these four interoperability layers. Each layer is described and depicted using ArchiMate© notation, including the Interoperability Architecture Solutions constraints, notation, and building blocks, oriented to the development of solutions.

5.2.2.1 Legal Layer

The Legal layer ensures that all interactions within the ETDS comply with relevant European and national legislation, including the General Data Protection Regulation (GDPR), the Data Act, and the eIDAS 2.0 Regulation. It provides the framework for data-sharing agreements, contractual trust, liability allocation, and enforcement of consent and access conditions. This layer plays a key role in ensuring legal compliance while supporting data sovereignty and ethical principles within the governance of the data space.

To further illustrate this, Figure 22 below presents the Legal view, structured across two main groupings: Legal Governance Content and Legal Functional Content, which distinguish the strategic dimension of legal interoperability from its operational implementation.

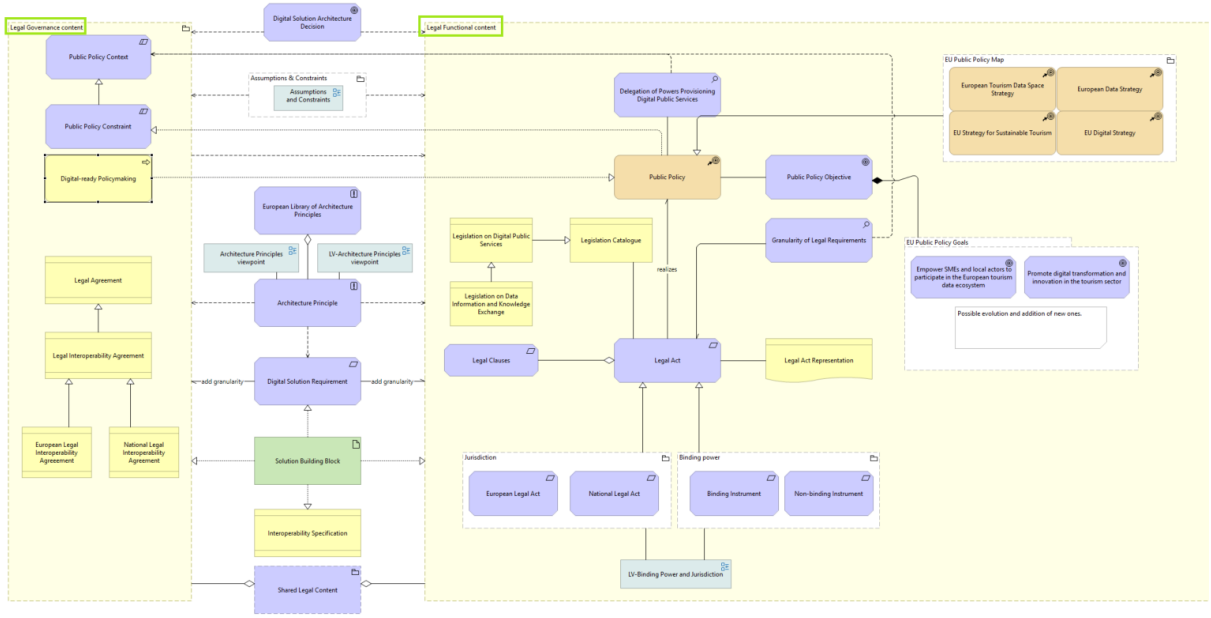

Figure 22 Legal view for ETDS (EIRA/eGovERA -based).

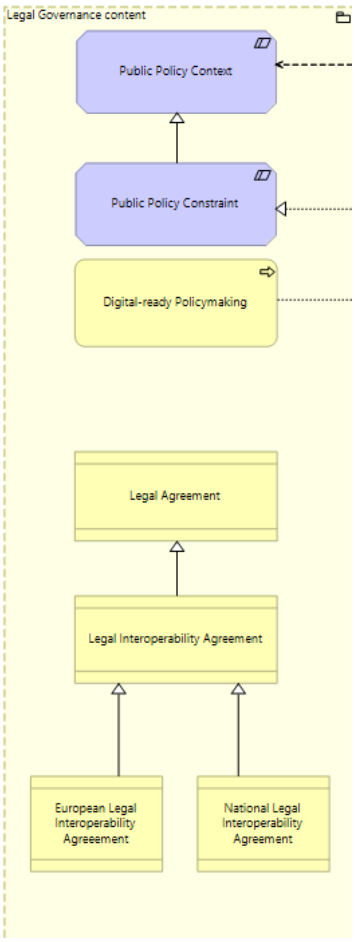

Figure 23 Legal Governance content for ETDS (eGovERA-based).

The Legal Governance content refers to the broader rules, constraints and policymaking processes that frame legal interoperability. It includes:

- Public Policy Context, describing the environment in which policies are formulated and decisions are made.
- Public Policy Constraint, defining the regulatory or legal constraints on how policy can be applied.
- Digital-ready Policymaking, which ensures digital aspects are considered early in the policy cycle, promoting future-proof and interoperable regulations.
- A hierarchy of legal agreements enabling collaboration across jurisdictions, including:
  - Legal Interoperability Agreements, both at European and National levels, which formalise governance rules between administrations.
  - These feed into broader Legal Agreements that govern collaborations across digital public services.

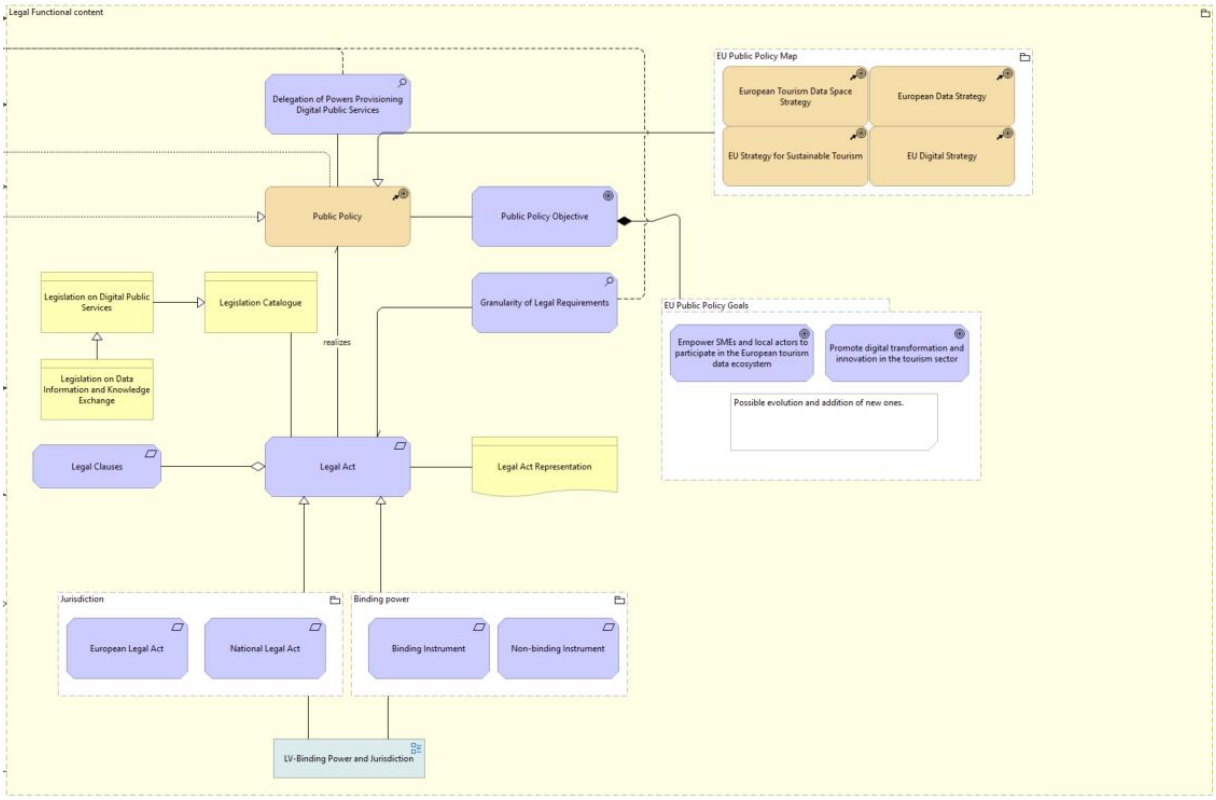

Figure 24 Legal Functional content for ETDS (eGovERA-based).

The Legal Functional Content focuses on how policies are implemented in practice, through legal instruments and specific requirements. This includes:

- Public Policy Objectives and the associated Granularity of Legal Requirements, ensuring traceability from high-level goals to enforceable actions.
- Legal Act and Legal Clauses, which operationalise policy decisions and set the legal basis for digital service delivery.
- Supporting structures such as the Legislation Catalogue, encompassing domains like digital public services and data exchange, and the Delegation of Powers for provisioning digital public services.

Building upon this foundation, the eGovERA also offers a detailed view of legal acts (binding/non-binding and jurisdiction-related, such as national-European). This serves as a catalogue of legislations where to pick the specific legal text that apply to the solution being designed, the ETDS architecture in this case.

As illustrated in the figures below, the LV-Binding Power and Jurisdiction view presents how policy intentions are translated into concrete legal instruments, forming the backbone of interoperable digital public services within the European Union. At the top level, European and National Legal Acts define the regulatory basis for implementing interoperability across and within Member States. These acts are grouped into categories that reflect their purpose and influence: European Binding Instruments, European Non-Binding Instruments, National Binding Instruments, and National Non-Binding Instruments, each covering aspects of structural, behavioural, and governance interoperability.

It is important to note that the applicability and configuration of these legal instruments may vary across pilots, depending on their domain, context, and stakeholders. The Legal View serves as a reference model, supported by resources such as the *Rulebook (Still under development by WP3), Rolebook (Developed by WP3) and Blueprint*, which guide the

governance setup for each data space. As the ecosystem evolves, this legal framework is expected to adapt gradually, incorporating new regulations, use case requirements, and lessons learned from implementation.

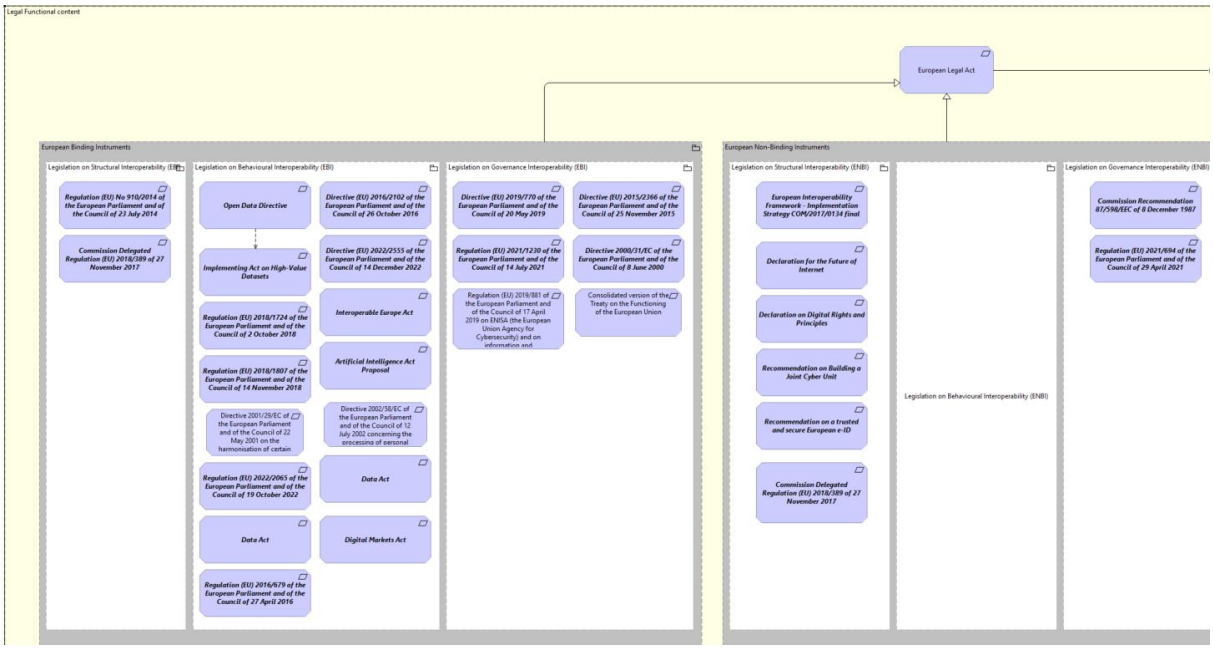

Figure 25 LV-Binding Power and Jurisdiction within Legal Functional content for ETDS (eGovERA-based).

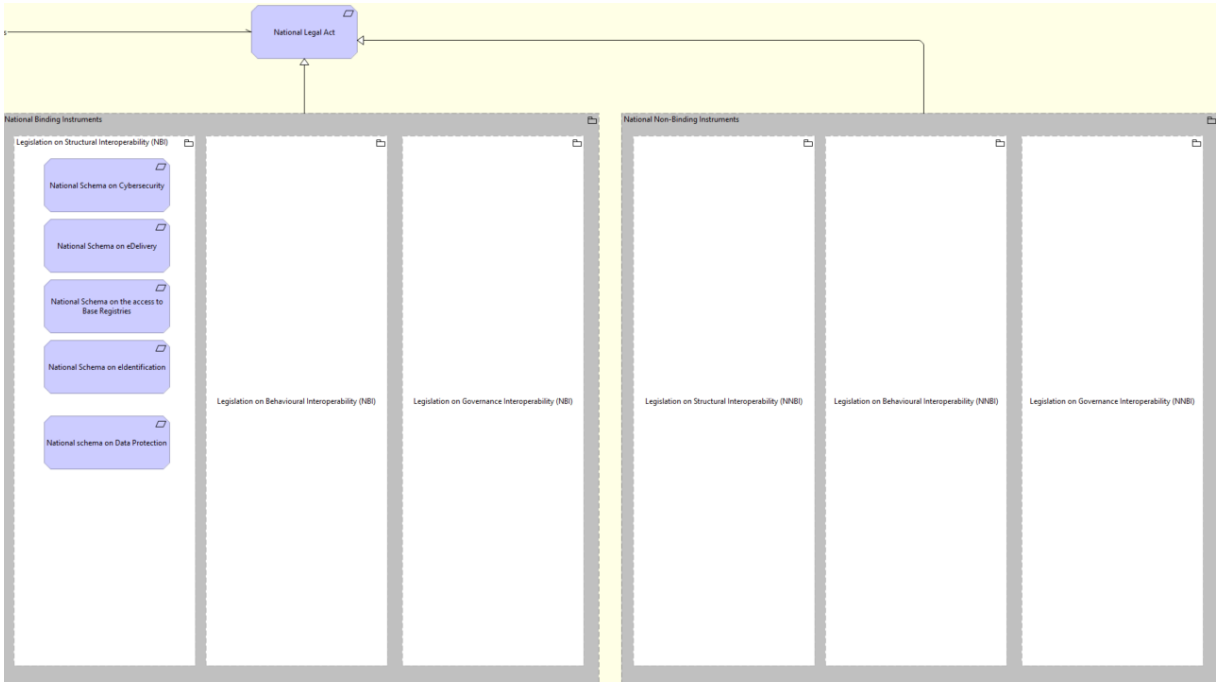

Figure 26 LV-Binding Power and Jurisdiction within Legal Functional content for ETDS (eGovERA-based).

As illustrated in the Figure 27 below, between Legal Governance Content and Legal Functional Content, the ETDS architecture introduces an architecture alignment layer that bridges policy intentions with operational legal implementation. It begins with Digital Solution Architecture Decisions, supported by contextual assumptions and constraints and guided by principles from

the European Library of Architecture Principles (ELAP)[86]. From these principles, Digital Solution Requirements are derived and translated into Solution Building Blocks, each governed by an Interoperability Specification. These components are legally grounded through Shared Legal Content, ensuring reusability and cross-border compliance across ETDS implementation.

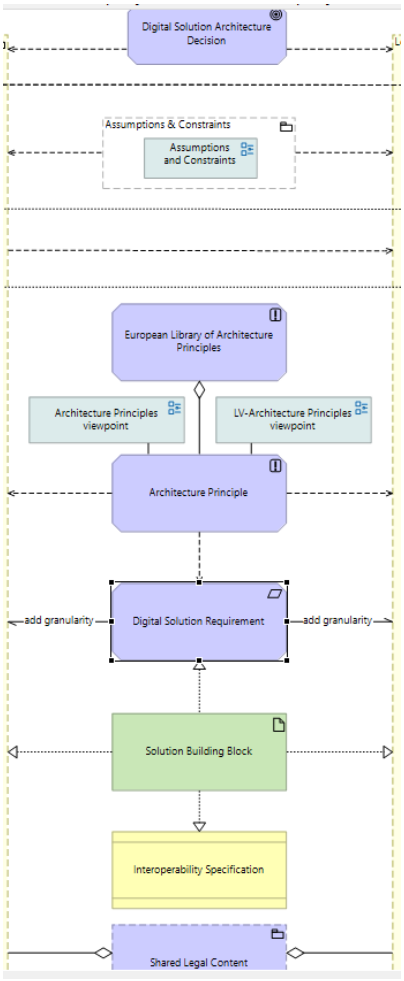

Figure 27 Legal Layer for ETDS (eGovERA-based).

The Assumptions and Constraints view captures the contextual foundation on which the ETDS is architected. It distinguishes two key elements: Assumptions, which represent expected conditions, and Constraints, which define limitations and obligations. As shown in the figure below, these elements are tailored to the specific use case addressed by ETDS pilots. It is important to note that this is an initial version that will be refined and evolved throughout the project as pilots mature and new requirements emerge.

[86] ELAP: https://interoperable-europe.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/solution/elap

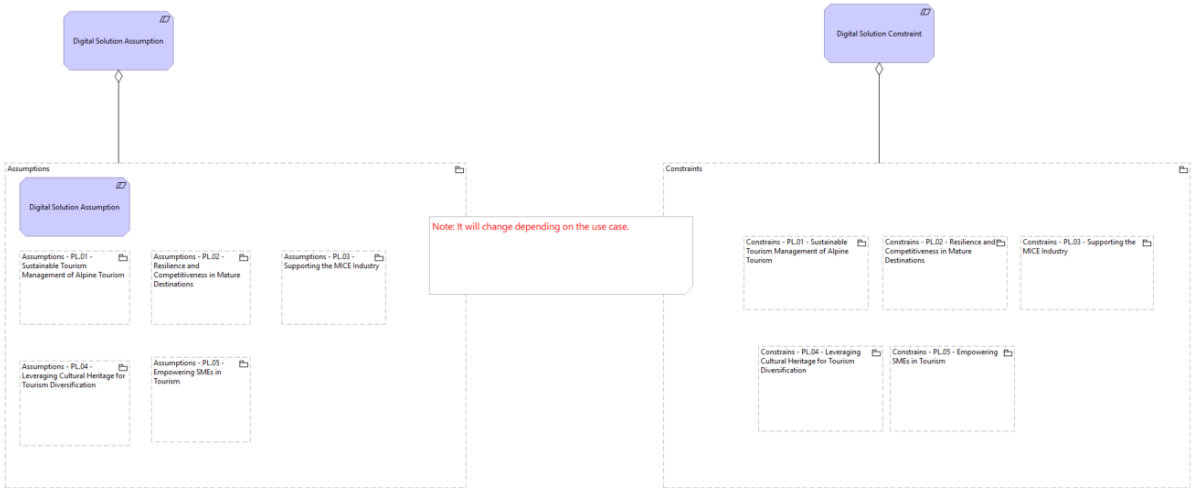

Figure 28 Assumptions and Constraints within Legal Layer for ETDS (eGovERA-based).

The Architecture Principles Viewpoint, based on the ELAP principles mentioned above, presents the set of design principles that guide the development and governance of digital public services within the ETDS. Grouped into strategic categories, the principles define how digital solutions should be conceived, implemented, and governed, emphasising core values such as openness, transparency, user-centricity, security, multilingualism, and reusability, which together foster interoperability and trust across Member States.

As illustrated in Figure 29, the view displays the complete set of principles applied within the ETDS. While Privacy is part of the reference model, it is not directly applicable in the ETDS context, as no processing of personal data related to identifiable individuals is foreseen.

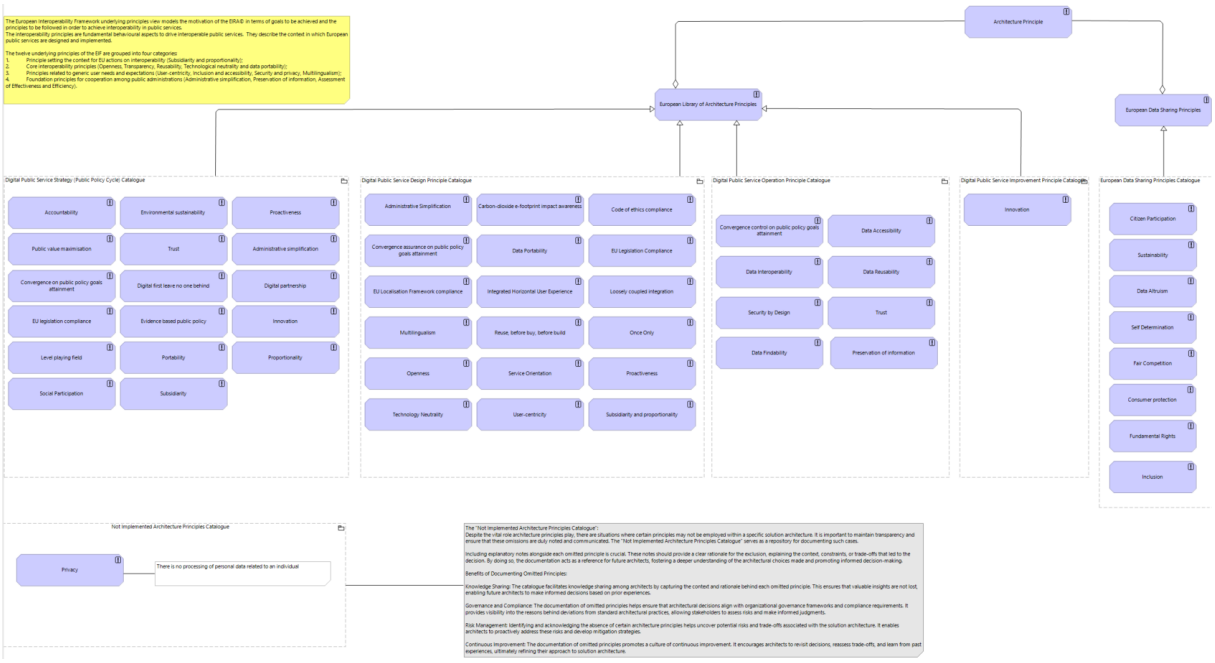

Figure 29 Architecture Principles within Legal Layer for ETDS (eGovERA-based).

5.2.2.2 Organisational Layer

The Organisational layer defines the governance and collaboration structures within the ETDS. It identifies the key roles and relationships among participants, including data providers, data consumers, intermediaries, and governance authorities. It clarifies how responsibilities,

interactions, and coordination mechanisms are distributed across the ecosystem. This layer supports the establishment of trust and accountability among participants, in line with the EIF principles of organisational interoperability.

To further illustrate this, Figure 30 presents the Organisational Layer, structured across two main groupings. The Organisational Governance Content and Organisational Functional Content, which distinguish the strategic dimension of organisational interoperability from its operational implementation within the ETDS.

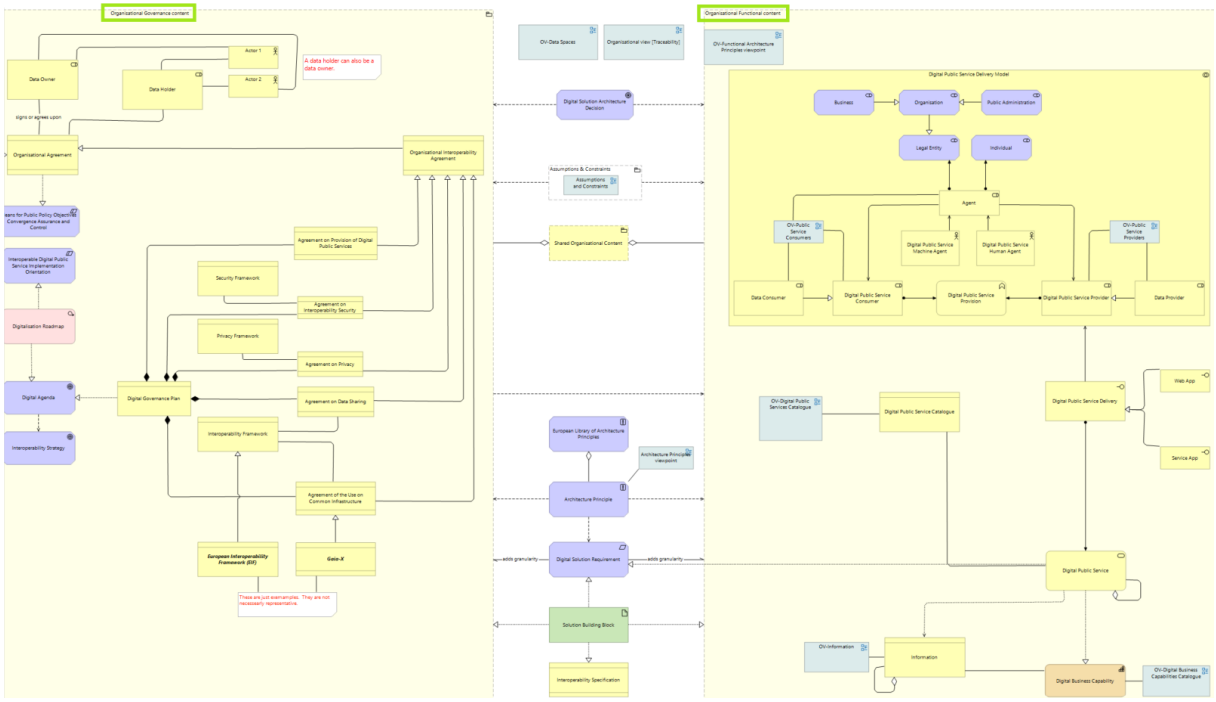

Figure 30 Organisational view for ETDS (eGovERA-based).

The Organisational Governance Content group provides a comprehensive representation of the coordination structures and agreements that underpin collaborative service provision in the ETDS. It captures the strategic governance mechanisms that enable trust, accountability, and structured cooperation among data providers, data holders and other relevant actors.

At the centre of this group lies the Digital Governance Plan, which consolidates key frameworks and contractual instruments to ensure coherent and secure interactions within the ecosystem. These include interoperability, privacy, security and data sharing, all of which align with broader strategic instruments such as the Interoperability Strategy and Digital Agenda.

This governance architecture is operationalised through a set of formal agreements that define how data space services are delivered, protected, and sustained. These agreements establish the necessary conditions for service provision, data exchange, identity and access management, and the use of infrastructure. Together, they support the implementation of the EIF's organisational interoperability principles, ensuring that all participating entities can collaborate effectively across domains and borders.

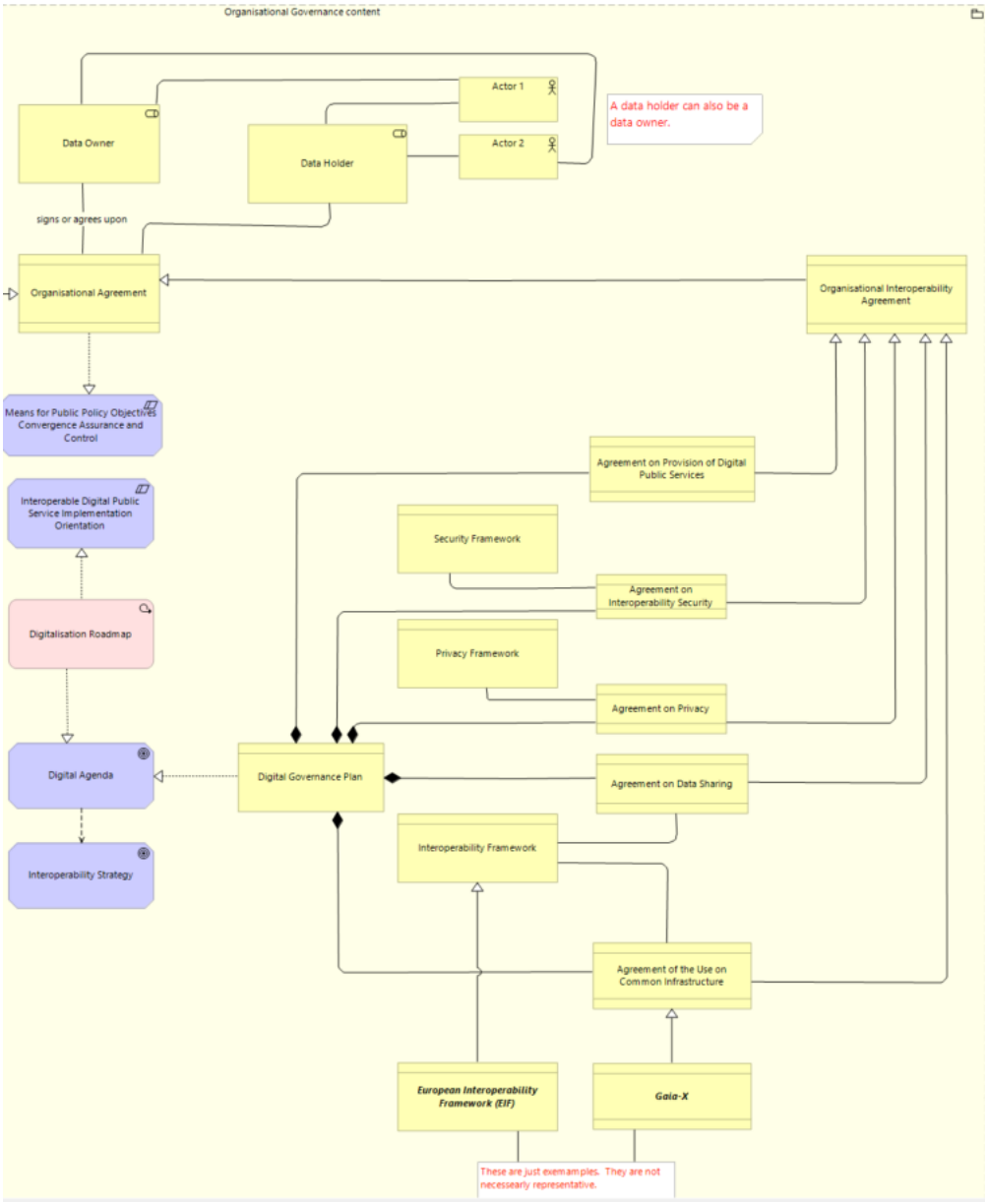

Figure 31 Organisational Governance content for ETDS (eGovERA-based).

The Organisational Functional Content group describes how data-sharing capabilities are structured, orchestrated, and consumed within the ETDS. It provides a functional view of the roles, responsibilities, and interactions between the different participants involved in the provision, exchange, and consumption of data.

Within the context of the ETDS, the Digital Public Service Delivery Model describes how different stakeholders interact and operate in the data space. An agent represents the execution of functions, assuming roles such as data provider or data consumer, depending on assigned responsibilities and contextual needs. This model shows how data products are exposed and accessed, and ensures that data delivery meets stakeholder requirements.

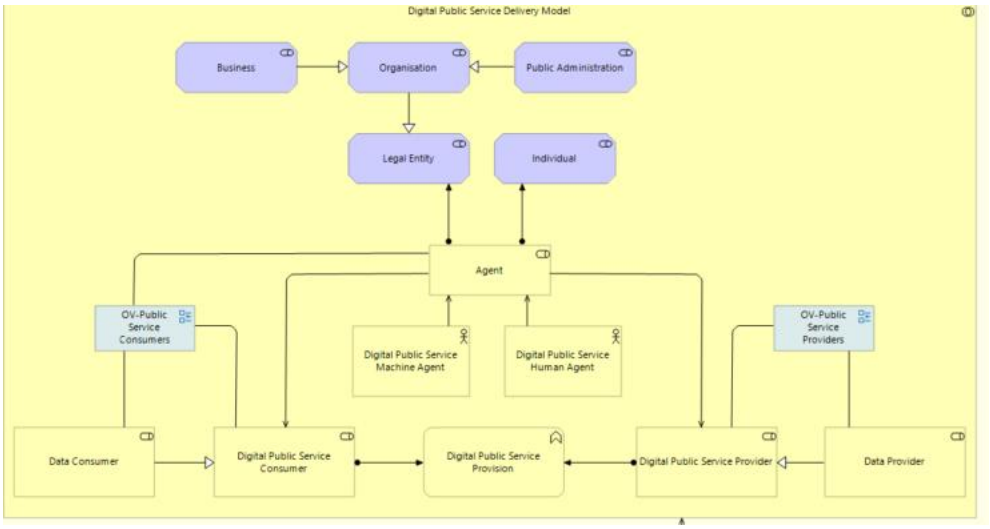

Figure 32 Digital Service Delivery Model within Organisational Functional content for ETDS (eGovERA-based)I.

As part of the Digital Public Service Delivery Model, the following views illustrate how data provision and consumption roles are distributed across the five pilot areas of the ETDS. These views serve to operationalise the abstract model by identifying concrete actors and stakeholders relevant to each pilot context. Each role allocation is subject to evolution, reflecting the ETDS architecture's adaptive, iterative nature.

The first OV-Public Service Consumers view captures the allocation of public service consumers per pilot. It shows the types of stakeholders expected to consume data services, including research institutions, SMEs, local authorities, DMOs (Destination Management Organisations) and individual tourists. These actors reflect the diversity of tourism-related needs across the five pilots. This allocation helps clarify who the beneficiaries of the data space are and informs the requirements for data accessibility, user experience, and service design.

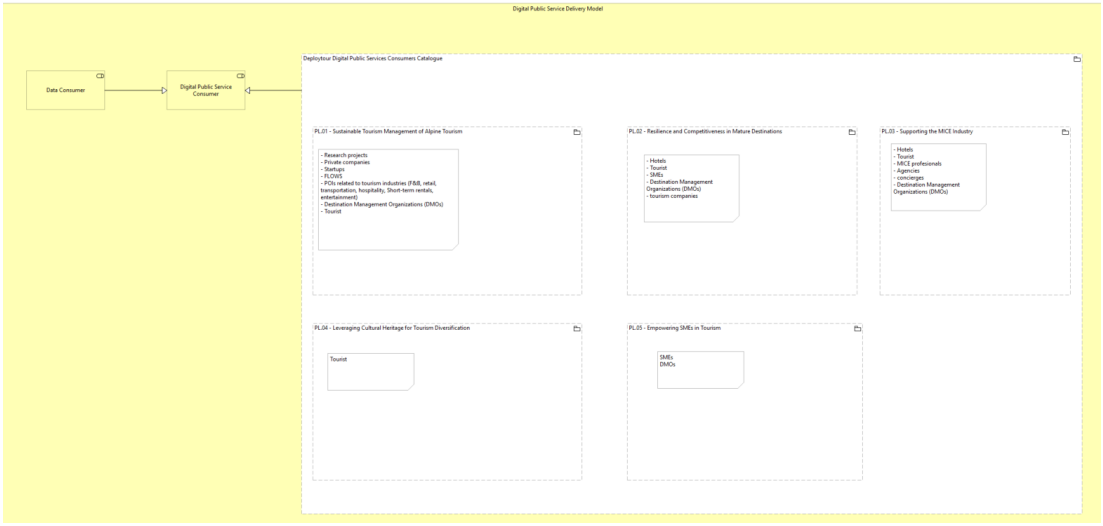

Figure 33 OV-Public Service Consumers within Organisational Functional content for ETDS (eGovERA-based).

The second OV-Public Service Providers view complements the previous one by outlining the roles of public service providers within each pilot. It defines which entities are responsible for exposing or delivering tourism data services. These may include DMOs, public administrations, tourism platforms and other relevant organisations. The distinction between providers and consumers helps identify dependencies, responsibilities, and potential governance models for

cross-pilot data interactions. It also reinforces transparency and accountability across the ecosystem.

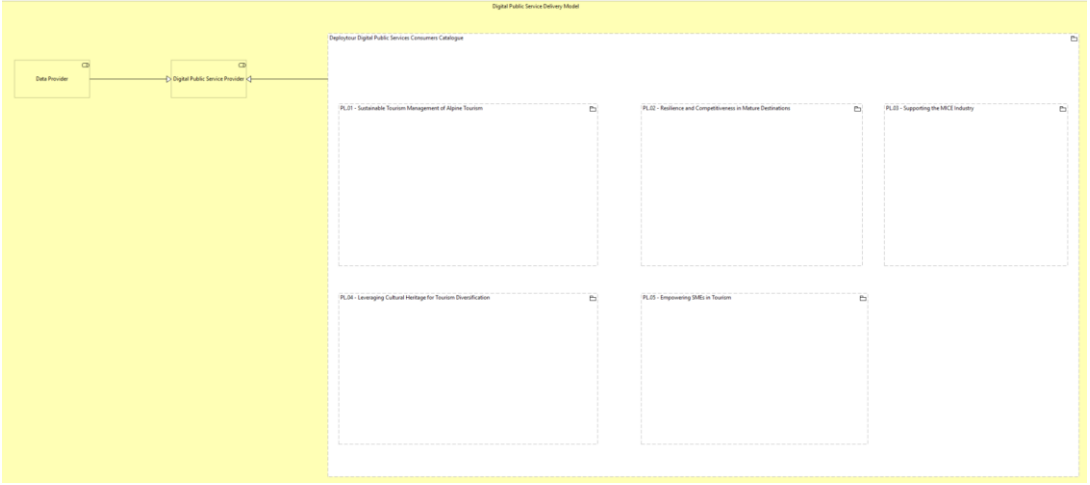

Figure 34 OV-Public Service Providers within Organisational Functional content for ETDS (eGovERA-based).

The Organisational Functional Content also includes three key architectural viewpoints that support the delivery and accessibility of data services within the ETDS: OV-Digital Public Services Catalogue, OV-Information and OV-Digital Business Capabilities Catalogue.

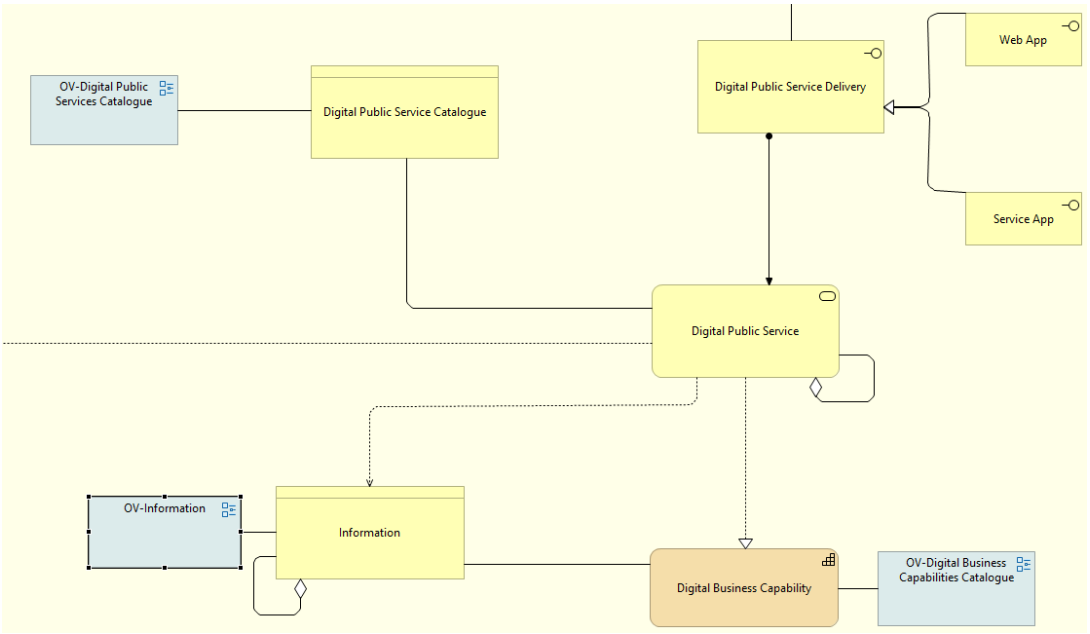

Figure 35 Organisational Functional content for ETDS (eGovERA-based).

The OV-Digital Public Services Catalogue provides a structured inventory of the business services that the data space will solve. These services encapsulate functionalities such as “Exchange data in a context of a Data Space” or “Secure access to data”, reflecting the core operations expected within the ETDS. These services will evolve as the project grows, and new needs are identified. Also, they will evolve based on pilot needs and maturity, ensuring continued alignment with stakeholder expectations.

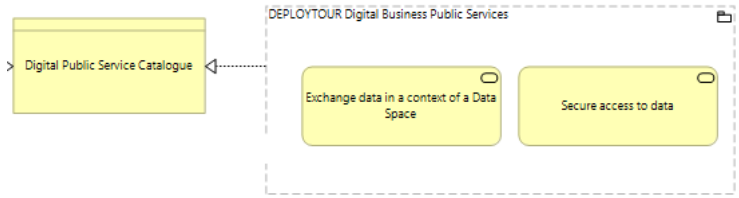

Figure 36 OV-Digital Public Services Catalogue within Organisational Functional content for ETDS (eGovERA-based).

The OV–Information viewpoint represents the set of data products that are exchanged within the ETDS. The catalogue is structured to accommodate the specific information needs of each pilot, meaning that the actual data products may vary depending on the context and objectives of each use case. As the project progresses, pilots will refine and expand these information assets to reflect evolving requirements, ensuring that the ETDS remains responsive and aligned with stakeholder priorities.

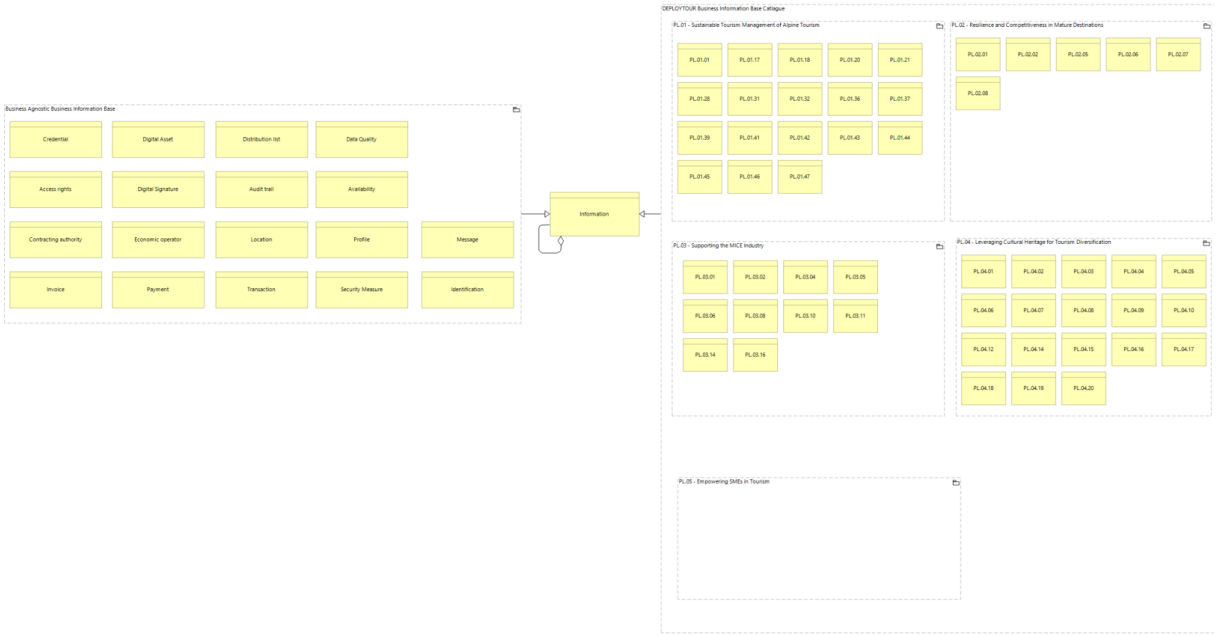

Figure 37 OV–Information within Organisational Functional content for ETDS (eGovERA-based)I.

The OV–Digital Business Capabilities Catalogue provides a view of the business capabilities required to implement and sustain digital services in the ETDS. The capabilities specific to this data space will continue to be identified and refined as the project and pilot use cases evolve. This iterative approach enables the identification of new functional needs as they arise. In some cases, the existing capabilities defined by frameworks such as eGovERA may already provide sufficient coverage. However, the catalogue remains adaptable to support emerging requirements and ensure the ETDS is equipped to meet its functional and operational objectives.

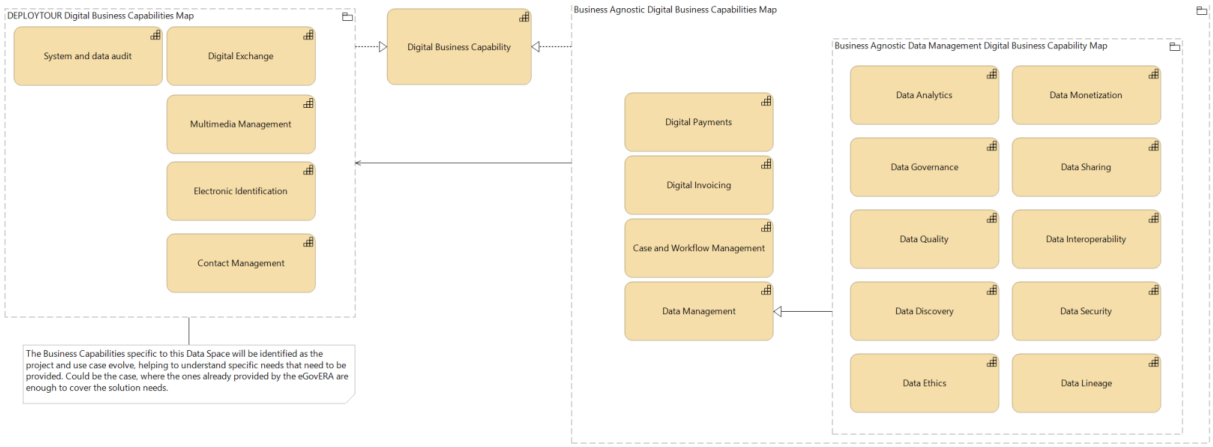

Figure 38 OV – Digital Business Capabilities within the Organisational Functional Content grouping for ETDS (eGovERA-based).

Together, these architectural viewpoints provide the backbone of the ETDS organisational functionality, enabling the efficient discovery, execution, and alignment of data services with the ecosystem's strategic and operational goals.

5.2.2.3 Semantic Layer

The Semantic Layer provides support for designing end-to-end, interoperable products and services in the ETDS. The building blocks under this layer primarily model the representation and serialisation of data, and related services, in line with the EIF principles of semantic interoperability.

Semantic agreements are essential for harmonising disparate terminologies and enabling interoperability across distributed systems. These agreements govern the management and use of data within organisations and ecosystems and formalise policies and contracts. This dual structure provides a framework for collaboration among diverse participants in a data space.

Data policies define the rules and guidelines for data and metadata management, including data collection, storage, processing, distribution, and disposal. Semantic agreements ensure, therefore, data quality, accessibility, and protection in accordance with regulatory and ethical standards. On the other hand, data contracts formalise the terms and conditions for data sharing between parties, including rights, responsibilities, security measures, and the purpose of data use.

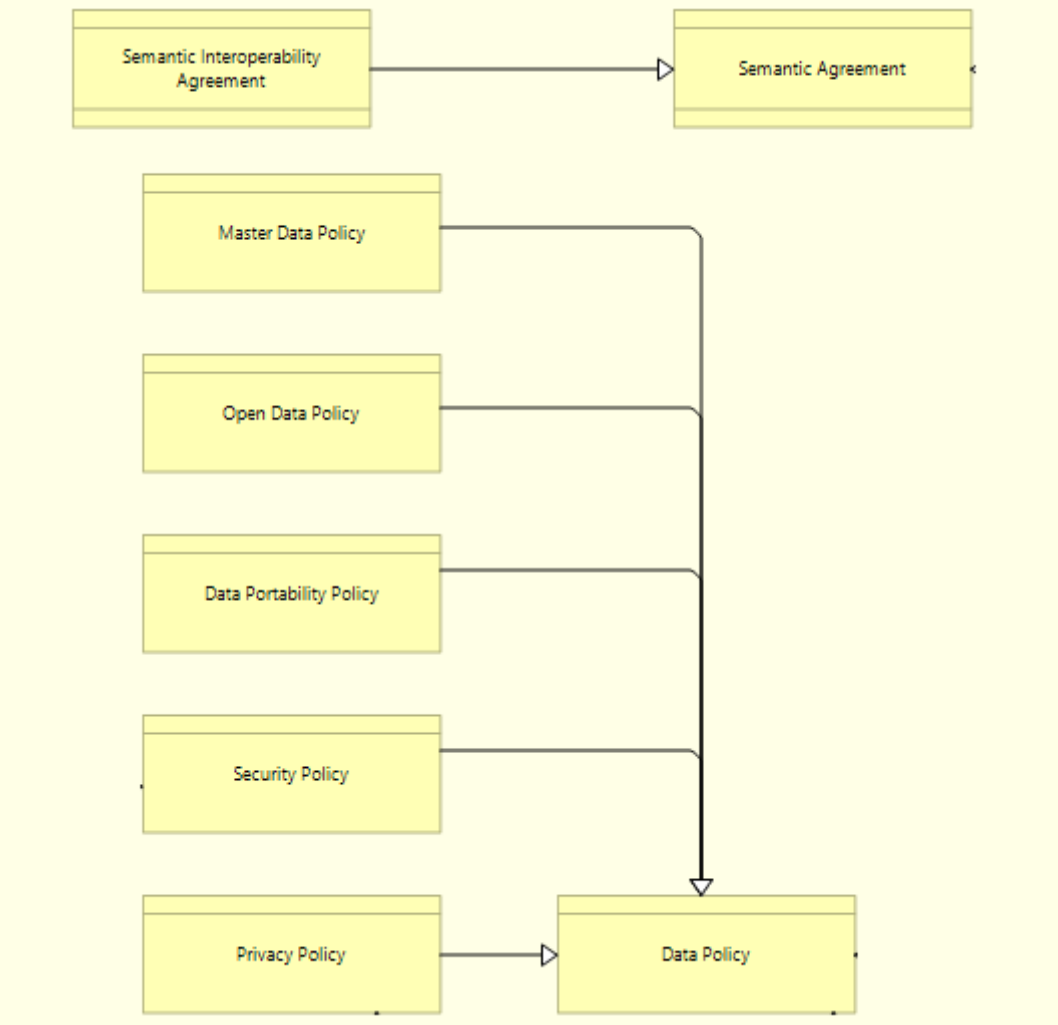

Figure 39 39 Semantic Governance content for ETDS (eGovERA-based).

At the core of these agreements, policies, and contracts are data objects, precisely datasets and ontologies. A dataset is a structured collection of related data, organised for ease of use, exchange, and analysis, and enriched with metadata. An ontology defines a set of artefacts to model a specific domain, enabling the representation of data sources (that is, in a given data format, using reference data) and interoperability within the ecosystem. This is relevant to the extent of semantic reasoning and data validation. Additionally, semantic interoperability boosts cross-industry integration by organising the necessary metadata and models to represent exchanges in a machine-readable manner, following standards and complying with regulatory frameworks.

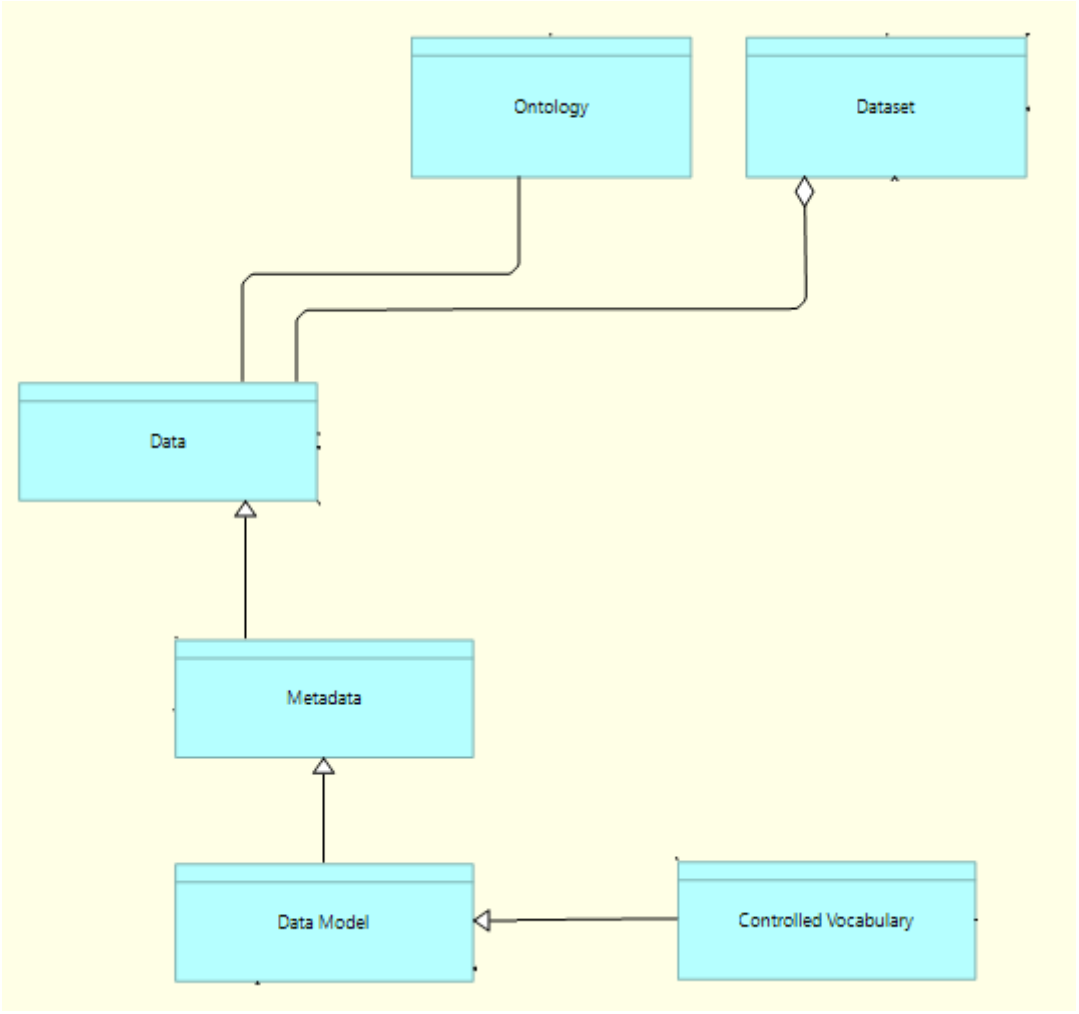

Figure 40 (Simplified) Semantic Functional content for ETDS (eGovERA-based).

It is important to distinguish between Data and Metadata: while Data captures the actual content, Metadata describes that content. For this reason, it is often more precise to refer to an explicit metadata model when representing or standardising metadata, ensuring clarity and consistency across the ecosystem. In practice, an ontology will cover an underlying data model and a controlled vocabulary

5.2.2.4 Technical Layer

The definition of the Dataspace Enablers (within the context of eGovERA, specifically the EIRA approach for Data Spaces) refers to a specific grouping of technical services required to establish, manage, and facilitate an MVDS. The EIRA approach emphasises a decentralised model where data is maintained and managed by participants. The Dataspace Enablers group is an Architecture Building Block (ABB) grouping that contains the fundamental services required to operationalise a data space.[87]. The services include:

- The Dataspace grouping is the core service representing the ecosystem.
- The Trust grouping includes the functionalities related to storing, securing, anonymising, pseudonymising, rectifying, and erasing personal data.
- The Identity Provider grouping, the services to manage and control user identities and access rights.

[87] See Annex IV to zoom on the different parts of the data space enabler,

- The Contract Negotiation grouping, the services to manage data contracts, policies and governance services for the availability, usability, integrity and security of data.
- The Data Catalogue Management grouping, the services to manage the dataset catalogue and the federated data catalogue for the management of metadata about data assets.
- The Vocabulary Management grouping is the vocabulary hub service for managing and providing access to a wide range of vocabularies or terminologies.
- The Connector Registry and App Store grouping, which facilitates data integration and data processing.
- The Catalogue grouping is the service of organising and discovering metadata about data assets.
- The Data Transfer grouping is the service supporting data exchange.

In the centre of the diagram in Figure 41, the data space connector is depicted, showing both the connector provider and consumer (i.e., the data space participants) and their association with a data-related building block.

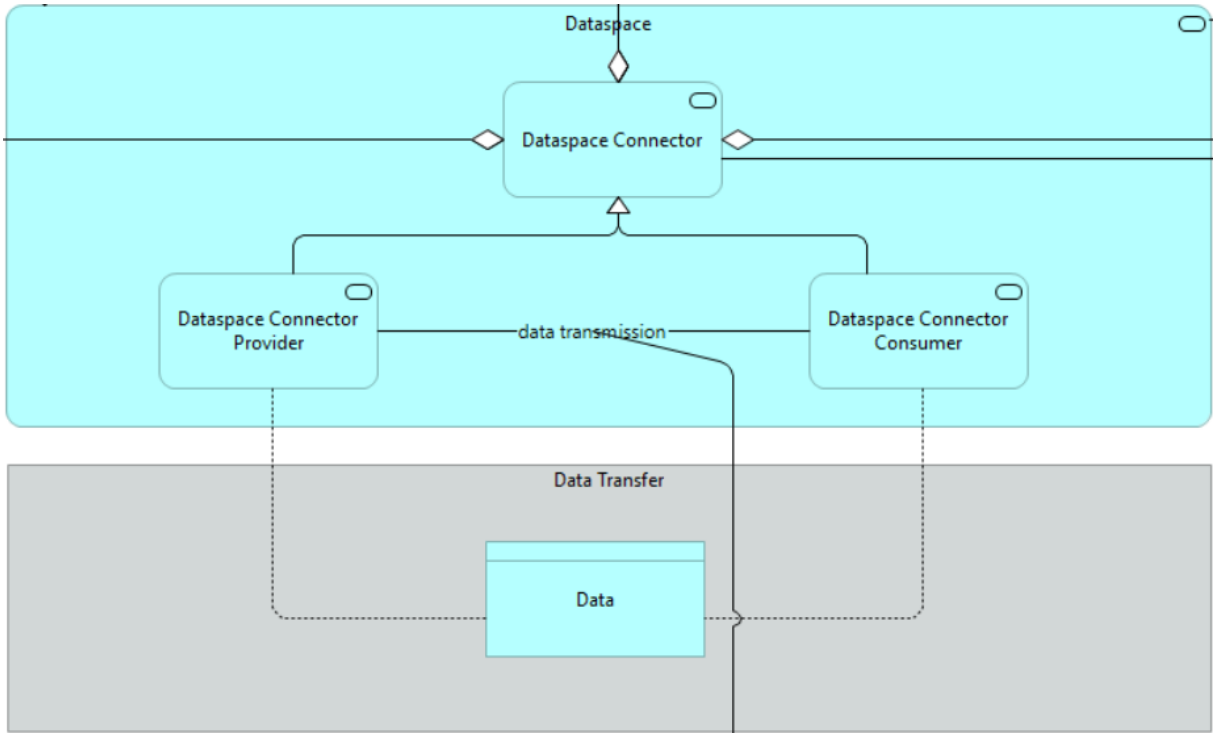

Figure 41 TVA-Data Space Enablers within Technical Functional content for ETDS (eGovERA-based).

Following the top side of the diagram in Figure 42, the Identity Provider package includes building blocks for Identity Management, both in a decentralised and a centralised approach, that model the processes, policies and technologies that manage and secure digital identities (of participants, systems or applications). The building blocks for identification and access conceptually aggregate into the Dataspace Connector building block, a relationship that is replicated for Vocabulary Hub and expanded to other building blocks that are not in the scope of this first iteration (the Observability, Privacy, and Message Broker building blocks).

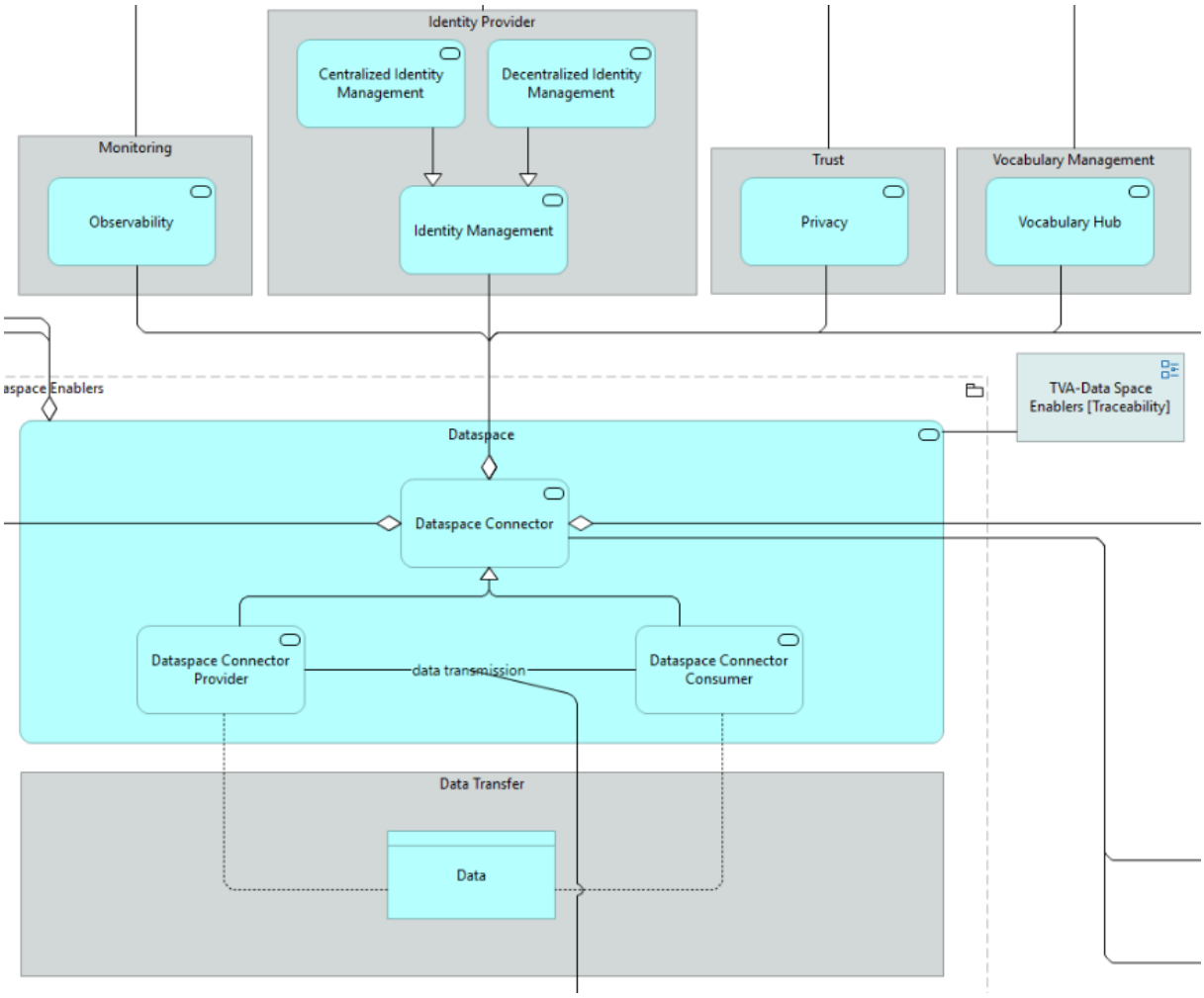

Figure 42 TVA-Observability and Monitoring, Indentification and Access, Privacy, Knowledge Discovery, and Messaging Enablers within the Technical Functional Content for ETDS (eGovERA-based).

Following the left side of the diagram in Figure 43, the Connectors Registry and App Store package includes the building blocks Service Registry and Service Discovery and Registry, which support the discoverability of services and connectors. At this first stage, the Consortium considers providing a Dataspace Portal from which participants can obtain the connector and find products and services from a centralised perspective; however, the idea of giving decentralised portals will be on the loop in future iterations. On the bottom of the Connectors Registry and App Store package, the Catalogue package and the Contract Negotiation package respectively contains the building blocks that manages metadata and facilitates participants to describe and share their data assets in a standardised way across the data space (Dataset Catalogue, Federated Data Catalogue Management, and Data Catalogue Management), and the handling of contractual and policy-related aspects of data sharing. Both packages aggregate to the Dataspace Connector building block, facilitating federated data discovery and indexing, and ensuring that all participants agree on usage rules, as well as on compliance and data governance principles, before engaging in the data exchange.

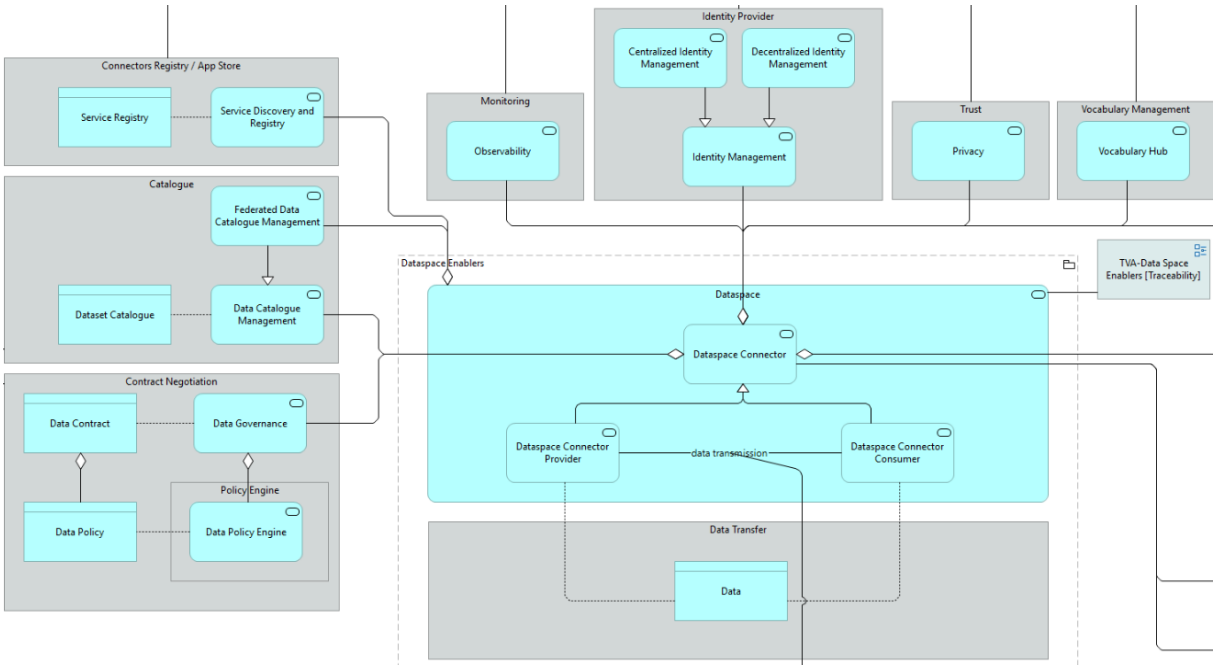

Figure 43 TVA-API, and Data Management Enablers within the Technical Functional Content for ETDS (eGovERA-based).

Finally, on the bottom right of Figure 44, the Data Analytics and Quality package comprises the Data Quality building block, ensuring that the shared and integrated data is fit-for-purpose across the ecosystem and optimising business processes. However, at this MVP stage, Data Analytics should not be included.

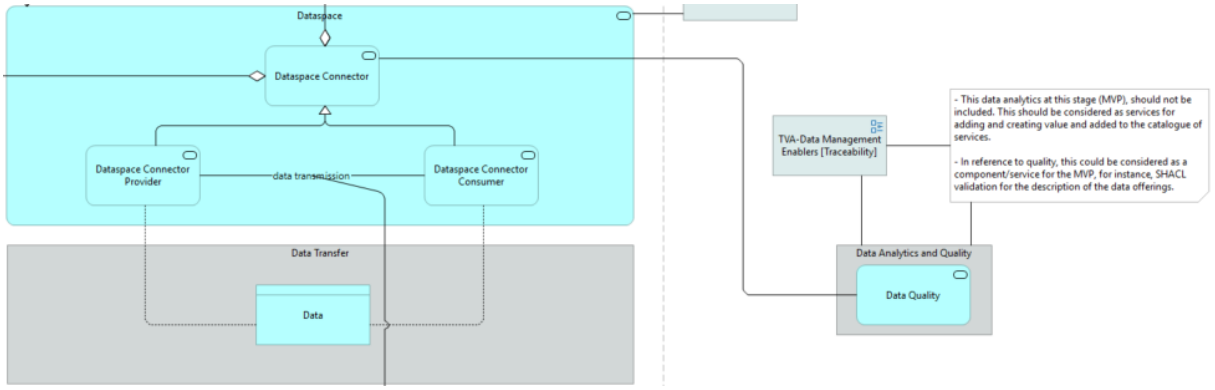

Figure 44 TVA-Data Management Enablers within the Technical Functional Content for ETDS (eGovERA-based).

6 Conclusions

The proposal for an ETDS architecture faces technical challenges that the Consortium will continue to tackle in the context of use case development. A common agreement on a precise understanding of the end-user product is paramount to enabling the operationalisation and scalability of the ETDS. This does not imply the absence of a concrete data product; rather, it acknowledges that the nature of the end-user products may vary significantly across pilots, based on the specific needs of each context. Nonetheless, a first deployment of a Minimum Viable Data Space (MVDS) is provided based on the assessment of the technological stack within the context of data space initiatives.

Regarding the creation of the data space, the MVDS has been defined as the integration of elemental architectural features which enable a usable and secure process for sovereign data exchange. Those features include the following: participant onboarding, data product publication, data product discoverability, and data exchange. This first deployment will be subsequently refined together with the ETDS Rulebook and the maturity of the use cases: based on the pilot results, the technological stack will decide the precise control and data planes that are integrated to the connector; the local catalogues refinement including the possibility to offer a tourism DCAT-AP, in line with the mobility (deployEMDS) and the language (LDS) DCAT-AP; and a consolidated governance mechanism to adapt to different stakeholders on the onboarding processes and contract negotiations.

All in all, the pilots have helped validate which technical building blocks are essential and which can be optional and progressively introduced. In this line, the proposal of a high-level architecture based on EIRA/eGovERA Business Agnostic RA allowed the Consortium to prioritise time investment: EIRA/eGovERA aligns with the architecture principles adopted in SIMPL and helps manage complexity during the early stage of deployment.

When examining the available technological stack, the EDC, SIMPL, and FIWARE middleware emerge as the most relevant options. EDC offers a modular, standardised foundation for identity management, data transfer, and policy enforcement. In turn, SIMPL, which builds on EDC, adds more sophisticated capabilities, including a dedicated onboarding and governance framework and integration with common federation services, which are ideal for meeting future-specific requirements. Meanwhile, FIWARE contributes with an open-source ecosystem of interoperable components compatible with data-space paradigms (for example, context brokers, identity management and policy enforcement modules) and thus represents an important alternative or complementary layer in the stack. As more components mature and interoperability standards evolve, specifically those of the EUDI Wallet RA or EDC (e.g., Identity Hub and Data Space Registry are EDC services in progress), the ETDS can progressively expand towards a real-case data space.

7 Annex

7.1 Annex I: Comparative table of reference architectures and frameworks of EDTS

The rapid development of the European Data Strategy has led to multiple architectural frameworks and reference models to support secure, interoperable, and sovereign data spaces. These initiatives aim to foster collaboration across sectors while ensuring trust, transparency, and compliance with European values and regulations.

This comparative table provides an overview of six key frameworks and reference models that are relevant to the implementation of the European Tourism Data Space (ETDS). Each of these initiatives contributes different perspectives—technical, organisational, legal, and policy-driven—towards the realisation of interoperable data ecosystems.

The comparison focuses on the core purpose, key components, areas of focus, and notable standards or principles associated with each framework. This overview is intended to guide stakeholders in understanding the complementarities and potential synergies among these initiatives as they work to implement sustainable, future-proof data spaces in Europe.

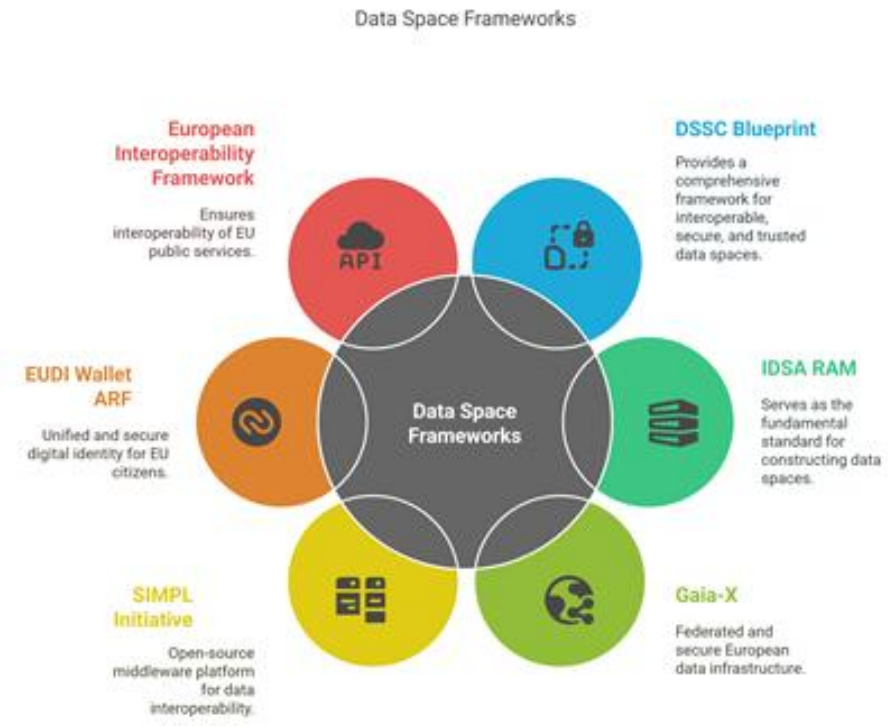

Figure 45 Data Space Frameworks according to the European Data Strategy.

Framework	Purpose	Key Components	Focus	Notable Standards or Concepts

DSSC Blueprint	Provides a comprehensive framework for interoperable, secure, and trusted data spaces	Data Plane, Control Plane, Verifiable Credentials, Dataspace Protocol (DSP), Governance frameworks	Technical & organisational infrastructure for data spaces	DCAT v3, ODRL, Verifiable Credentials, DSP, Data Act compliance
IDSA RAM	Serves as the fundamental standard for constructing data spaces	Five-layer modular architecture, Dataspace Protocol (DSP), IDS Certification, IDSA Rulebook	Trustworthy and self-determined data exchange	ISO/IEC 27001, IEC 62443, IDS-specific standards, RAM 5
Gaia-X	Federated and secure European data infrastructure	Conceptual Model, GXDCH, Federation Services, Compliance Document	Data sovereignty, transparency, and trust	Gaia-X compliant credentials, alignment with IDSA RAM principles
SIMPL Initiative	Open-source middleware platform for data interoperability	SIMPL-Open, SIMPL-Labs, SIMPL-Live; Modular and scalable architecture	EU-funded support for interoperability across public data spaces	Open-source, modular approach, SIMPL community events
EUDI Wallet ARF	Unified and secure digital identity for EU citizens	Architecture & Reference Framework (ARF), Reference Implementation, Legal alignment with eIDAS 2.0	Digital identity, authentication, and electronic signatures	Common technical and legal standards across Member States
European Interoperability Framework (EIF)	Ensures interoperability of EU public services	EIF principles, European Interoperability Reference Architecture (EIRA), Interoperable Europe Board	Interoperability in public service delivery	Legal, organisational, semantic, and technical interoperability

Table 1 Comparative table of reference architectures and frameworks of EDTS.

7.2 Annex II: Comparative analysis of selected data space initiatives

The following table presents a comparative analysis of selected data space initiatives relevant to the European Tourism Data Space (ETDS). These initiatives showcase diverse architectural models, governance structures, and implementation strategies, yet all contribute valuable insights and building blocks towards achieving interoperable, trustworthy, and sustainable data ecosystems in Europe. Each initiative addresses different domains such as tourism, mobility, or cultural heritage, and reflects varying levels of maturity and technical design choices. This overview supports the identification of best practices, technical patterns, and synergies for the development of cross-sectoral data spaces.

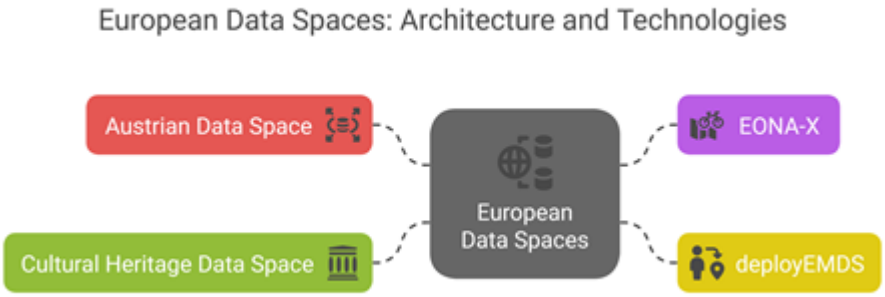

Figure 46 Data Space initiatives relevant to the ETDS.

Initiative	Purpose	Architecture	Key Features	Standards / Technologies
Austrian Data Space	National data space for tourism interoperability and innovation	Based on IDSA RAM and Gaia-X Federated X (Split Model), uses Eclipse Dataspace Connector (EDC)	Trust anchor by Austria Tourism; intuitive B2B tools; 10 hubs across federal states	Decentralised Identifiers (DIDs), ODRL, Attribute-Based Access Control (ABAC), W3C standards
EONA-X	European data space for Mobility, Transport, and Tourism	Distributed, modular, aligned with Data Mesh and IDSA; uses EDC and Dataspace Protocol (DSP)	Self-sovereign identity (SSI); catalog discovery; control & data planes; verifiable credentials	W3C DCAT v3, ODRL, OAuth2, DIDs, Verifiable Credentials, IDSA DSP
deployEMDS	harmonised discoverability and interoperability for regional tourism data	DSSC-based building block model; flexible for various implementation scenarios	Central catalogue, contract negotiation, decentralised identity registry	Eclipse Dataspace Connector (EDC), DSSC architecture guidelines, DIDs
Cultural Heritage Data Space	Access and reuse of digital cultural heritage across Europe	Built on the Europeana platform; centralised metadata, distributed content	Focus on metadata quality, multilingualism, 3D content, legal clarity, and data reuse	Europeana Data Model (EDM), RDF, Dublin Core, LIDO, CIDOC CRM, Europeana APIs
Green Deal Dataspace (SAGE)	Operational Green Deal Data Space focused on the access, integration and use of green as well as environmental data across Europe	Based on IDSA Architecture, certifiable standards from IDSA and GAIA-X; uses Eclipse Dataspace Connector (EDC)	Leverages outcomes from the European Strategy for Data, enriching data quality, validation and interoperable metadata.	TBD
TEMS	Data-driven ecosystem in the media sector, allowing media	TBD by TEMS	Data access, sharing, and sovereignty that comply with data	TBD by TEMS

	organisations to combat fake news and misinformation.		protection legislation.	
European Language Data Space (LDS)	A secure and efficient platform for the exchange, monetisation, and reuse of multilingual and multimodal language data.	A distributed, decentralised, peer-to-peer infrastructure (META-SHARE, ELRC-SHARE, ELG Cloud Platform, among others) that uses mappers from these platforms and the EDC and Dataspace Protocol (DSP).	Catalog discovery; Identity & Access Management; registry of participants and S/W components.	W3C DCAT v3, ODRL, DSP, KeyCloak, Language DCAT-AP,self-descriptions (based on DCAT model).
European Data Space for Smart Communities (DS4SSCC)	Establishing a federated and innovative data space for smart and sustainable cities and communities.	DSSC-based building block model; Gaia-X; future adaptation to IDSA RAM and EUDI Wallet. The DS4SSCC architecture seeks to make the evolution of Smart Solutions/Data Platform to a data space, rather than the creation of a data space from scratch.	Data broker; Identity Management and Authorisation; Data API (); Data Publication; Universal Trust Registry	W3C VC; XACML; ABAC, RBAC; JSON REST API; iSHARE; i4Trust; DSP; DOME.

Table 2 Comparative analysis of data space initiatives related to ETDS.

7.3 Annex III: EIRA/eGovERA Business Agnostic RA 6.1.0

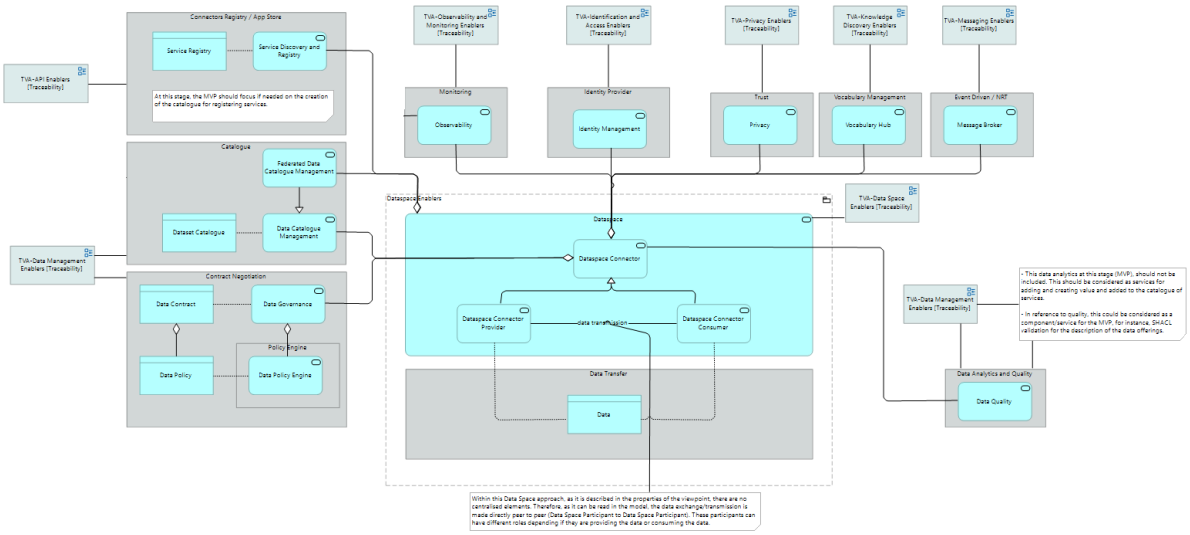

Figure 47 EIRA/eGovERA Business Agnostic RA 6.1.0.