Co-funded by the European Union

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			
POLITENICO DE 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	INDUSTRY INNOVATION CLUSTER SLOVAKIA	BEN - ICC
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	AE-ADQUIVER DATA & ADVANCED ANALYTICS, SOCIEDAD LIMITADA	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		

Co-funded by the European Union

D2.4 ETDS Architecture

Document Identification			
Status	Final	**Due Date**	31/05/2025
Version	1.0	**Submission Date**	28/05/2025

Related WP	WP2	**Document Reference**	D2.4
Related Deliverable(s)	D2.1	**Dissemination Level (*)**	PU
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

Document Information

List of Contributors	
Name	Partner
Dr. Andreas Eisenrauch	Amadeus Germany GmbH
Anastasia Koufaki	ADP
Mario Bravo Candel	NTTDES
Eduardo Martin Crespo	NTTDES
Carme Moreu Alfos	NTTDES
Rebeca Barcena Orero	NTTDES
Peio Oiz Arruti	ANYSOL
Victor Barrientos	ANYSOL
Dr Dolores Ordóñez	ANYSOL
Tayrne Butler	ANYSOL
Jonathan Huffstutler	EONA-X
Marie Texier	EONA-X
Jesús Santamaria	TECNALIA
Jesús Herrero	TECNALIA
Valentin Sanchez	TECNALIA
Flavie de Bueil	CITYDNA
Beatrice Dorenti	INTELLERA
Alessio Sidoti	INTELLERA
Vesna Kobal	ARCTUR
Joan Escamilla	ITI
Jordi Arjona Aroca	ITI
Antoni Gimeno	ITI
Fabián Avilés Martínez	GMV
Rubén Alconada	GMV
Pablo Pérez	GMV
Antoine Isaac	EF
Yago González Rozas	PLEXUS TECH
Laura Sande Alonso	PLEXUS TECH
Maik Mannsfeld	FRAUNHOFER
Blanca Adiego	HIBERUSTEC
Maria Pahoula	PLEIAD
Nicolò Carletti	DATA APPEAL
Federica Amati	DATA APPEAL
Anssi Tarkiainen	LAPLAND
Nuno Antonio	UNL
Américo Rio	UNL
Juan Francisco Inglés	LIBELIUM LAB

Document History			
Version	Date	Change editors	Changes
0.1	16/01/2025	Eduardo Martin	Initial version
0.2	19/05/2025	Partners involved in the WP activities	Overall contributions
0.3	21/05/2025	Eduardo Martin	Final version before correcting and formatting
1.0	27/05/2025	Tayrne Butler	Final version to submit

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	NTTDES	21/05/2025
Project Coordinator	AnySol	22/05/2025

Table of Contents

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	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

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 Reference Architecture provides a technical infrastructure of 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, mainly relying on the SIMPL decision.

The Consortium also pointed out key considerations for the definition of 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, or correctly understanding private and public-sector data usage is 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 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 DSSC design principles.

The Consortium ("partners") is in charge of the development of the ETDS sectoral data space, which results in the proposition of DEPLOYTOUR and its minimal viable data space. Among the partners, coordinators from the two preparatory actions (DATES/DSFT Blueprint) participate and guarantee that there is continuity during the deployment of the ETDS.

This second deliverable sets the principles of the DEPLOYTOUR architecture. This document not only considers the preparatory actions of DATES/DSFT Blueprint on the recommendations of the reference architecture but also includes the analysis of the first deliverable ("ETDS Interoperability & Data Sharing"). Among the proposed work packages (WP1 to WP6), WP2 ("TOURISM DATA SPACE BUILDING BLOCKS AND OPERATIONALIZATION.") and WP4 ("REAL-WORLD DEPLOYMENT OF ETDS THROUGH USE CASES BASED ON THE VARIOUS TYPES OF DATA IN THE TOURISM SECTOR") serve to elaborate the strategic decisions for shaping this deliverable structure and its content.

The final document covers the foundations of the technical infrastructure of the ETDS in alignment with existing building blocks and sets the basis on which the use cases will be implemented and how this implementation will be tested.

This document is divided in seven broad sections:

- Section 1 covers the Project Executive Summary;
- Section 2 introduces the first deliverable and the objectives;
- Section 3 covers the state-of-the-art of the data space initiatives and architectures;
- Section 4 describes the technical stack, building blocks and the minimum viable data space of ETDS (DEPLOYTOUR);
- Section 5 synthesises the high level data space architecture;
- Section 6 and Section 7 provide the conclusions and next steps in the deployment of the ETDS.

1.1 Objectives

The scope of this document is limited to those components considered part of the target solution architecture underpinning the ETDS project, departing from the functionalities that DATES delivered. The following objectives are tackled in this deliverable:

- Identify the main technical issues and challenges for the minimum viable data space;
- Provide the high-level building blocks based on the use cases (pilots);
- Reshape the mandatory and optional building blocks needed for the deployment of the ETDS;
- Identify the technical stack that already exists on the market.

2 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.

2.1 Analysis of the preparatory action blueprint

The preparatory action DATES/DSFT Blueprint[1] sets guidelines to reuse and deploy a reference architecture for the ETDS. The blueprint builds on the OpenDEI Design principles[2] (position-paper) document, the DSSC Glossary[3], and the IDS Rulebook 2.0[4], as well as considering other relevant programs, i.e., GAIA-X, EONA-X, TDH022, among others.

The blueprint emphasises on 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 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[5] (DGA), Data Act[6] (DA) and General Data Protection Regulation[7] (GDPR). The document mentions several technologies (i.e., SOLID, MyData, EU Wallet) having 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 data models and interoperability of the ETDS. While the Smart Data Models[8] standard is promoted as the ideal solution, the Consortium must also consider other initiatives conducted by local SMEs or national boards, such as EONA-X[9] or TDH022[10]. The results from the pilot canvas sessions are essential for gaining a clear understanding of data sources and, consequently, how the data product offerings will be shaped.

2.2 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[11]). 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

[1] 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

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

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

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

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

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

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

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

[9] EONA-X: https://transition-pathways.europa.eu/learning-resources/eona-x-mobility-data-sharing-transport

[10] TDH022: https://docs.italia.it/italia/mitur/gl-tourism-digital-hub-interoperabilita-docs/it/main/index.html

[11] SIMPL: https://simpl-programme.ec.europa.eu/

Communications Networks, Content and Technology is implementing the SIMPL architecture in multiple phases (Annex I).

2.2.1 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[12]) and aims to consolidate with other initiatives (i.e., IDSA, Gaia-X) to establish a sovereign, interoperable, and trustworthy data-sharing environment[13]. The architecture includes crucial components like the Data Plane and Control Plane, ensuring 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 according to defined policies and agreements. Governance frameworks ensure that data access and usage comply with regulations, including the Data Act.

SIMPL complements DSSC by focusing on the interoperability of public and legal data platforms. While DSSC concentrates on the technical and organizational layers of data spaces, SIMPL facilitates seamless interactions between public data platforms, ensuring they comply with EU regulations. Both DSSC and SIMPL place a strong emphasis on data sovereignty and trust, ensuring reliable systems for secure data access and exchange.

The synergy between DSSC and SIMPL is evident in their shared objectives of ensuring interoperability and regulatory compliance. While DSSC provides the concepts and specifications of the necessary technical infrastructure for data spaces, SIMPL ensures smooth and compliant data exchange within public and legal platforms providing 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.

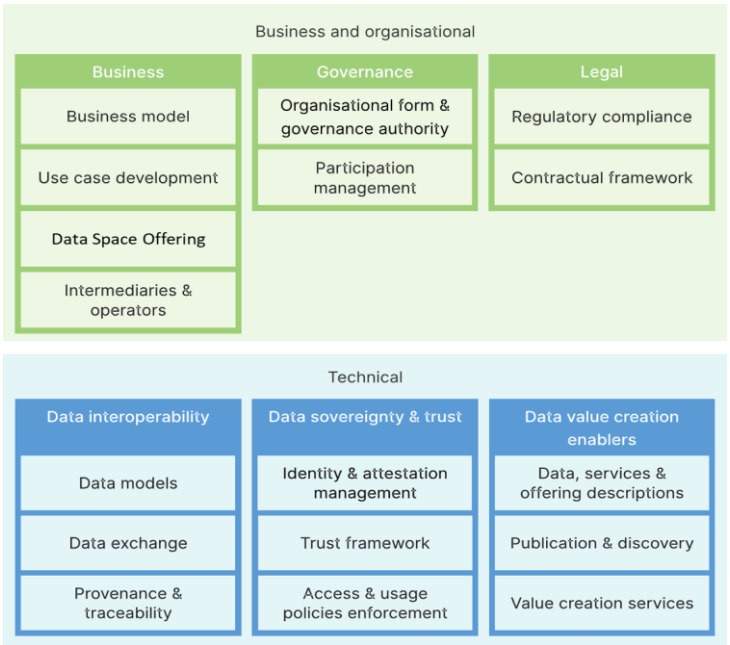

Figure 1 DSSC Building Blocks.

[12] Data Spaces Toolbox: https://toolbox.dssc.eu/

[13] "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

2.2.2 IDSA reference architecture model (RAM)

The International Data Spaces Reference Architecture Model[14] 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 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)[15]. 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"[16] emphasises its significance as a step towards standardising data space interoperability, 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[17]. It ensures that components and organizations 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[18] 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 Dataspace Protocol 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 Data Act and the General Data Protection Regulation (GDPR). 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.

[14] 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.

[15] Dataspace Protocol: https://eclipse-dataspace-protocol-base.github.io/DataspaceProtocol/2025-1-RC1/

[16] 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

[17] IDSA Certification & Trust Framework: https://internationaldataspaces.org/offers/certification/

[18] IDSA Rulebook: https://internationaldataspaces.org/idsa-rulebook/

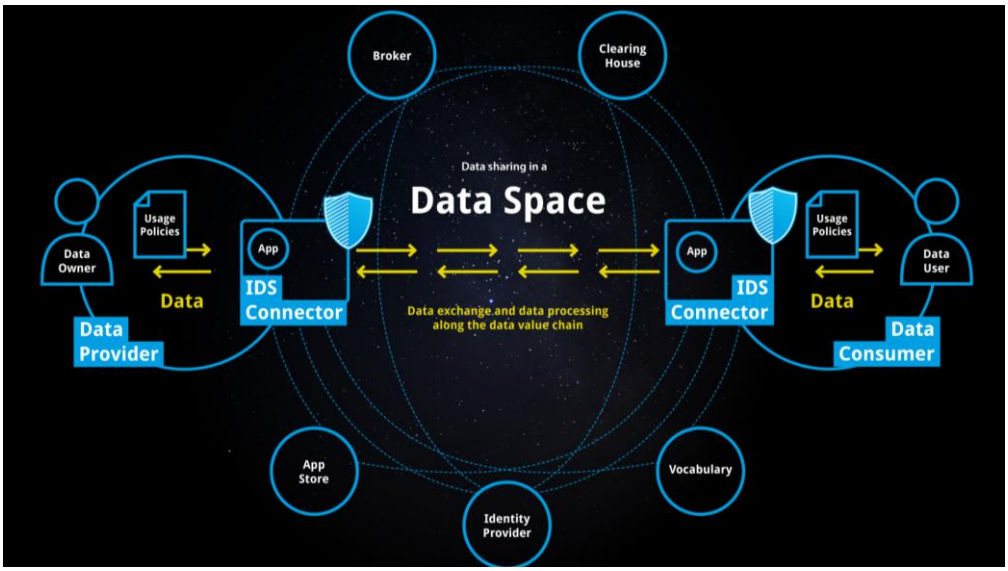

Figure 2 IDS-RAM

2.2.3 Gaia-X

The Gaia-X Architecture Document[19] 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 and secure data infrastructure based on 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.

[19] 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 that its architecture supports secure and sovereign data exchange, facilitating the creation of a robust and trustworthy data-sharing ecosystem.

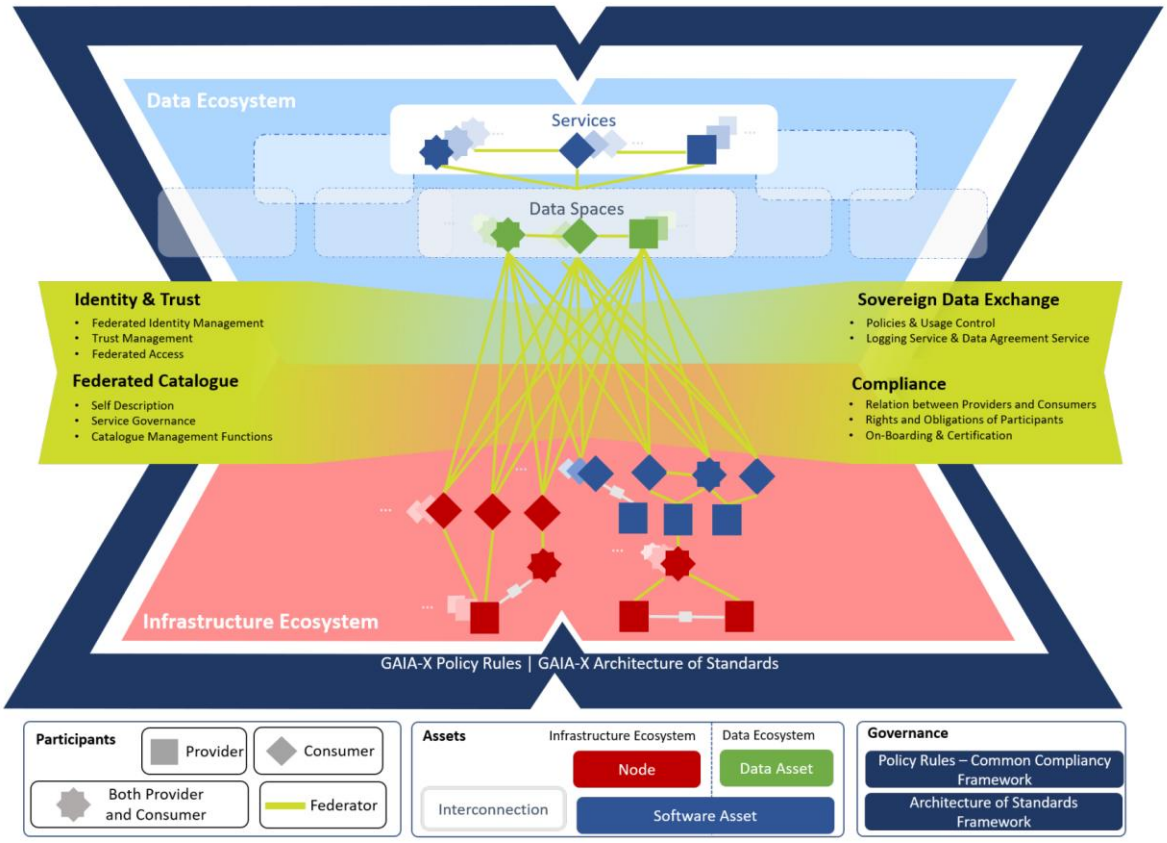

Figure 3 Gaia-X Ecosystem

2.2.4 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.

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 the data spaces and open-source community, facilitating the integration and development of interoperable solutions. This intelligent middleware brings together various components essential for operating data spaces, allowing data providers to have full control over 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 that analyse the feasibility of implementing the SIMPL-Open software stack in 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

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.

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.

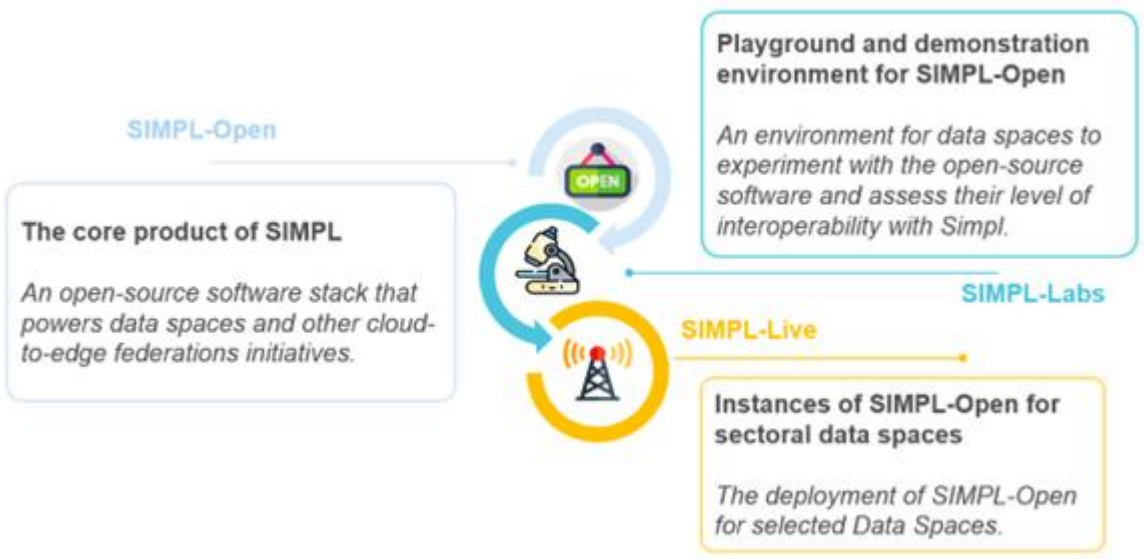

Figure 4 SIMPL Products

2.2.5 EUDI Wallet ARF

The EUDI Wallet[20] is an innovative project aimed at providing European Union citizens with a secure and unified digital identity for various activities, such as traveling, working, accessing public services, making payments, and signing documents. This project is closely linked to the eIDAS Regulation and its update, eIDAS 2.0, 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, establishing a common framework that facilitates 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.

2.2.6 European Interoperability Framework

The European Interoperability Framework[21] (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 account for the progress of its implementation via the IOPEI Monitoring Observatory[22]. A new governance structure, the Interoperable Europe Board (the 'Board'), resulting from the Interoperable Europe Act[23] (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,

[20] 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/

[21] EIF: https://ec.europa.eu/isa2/eif_en/

[22] IOPEI monitoring: https://interoperable-europe.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory

[23] IEA: https://eur-lex.europa.eu/eli/reg/2024/903/oj

meaning that the adoption of the framework should be considered for the deployment of the ETDS.

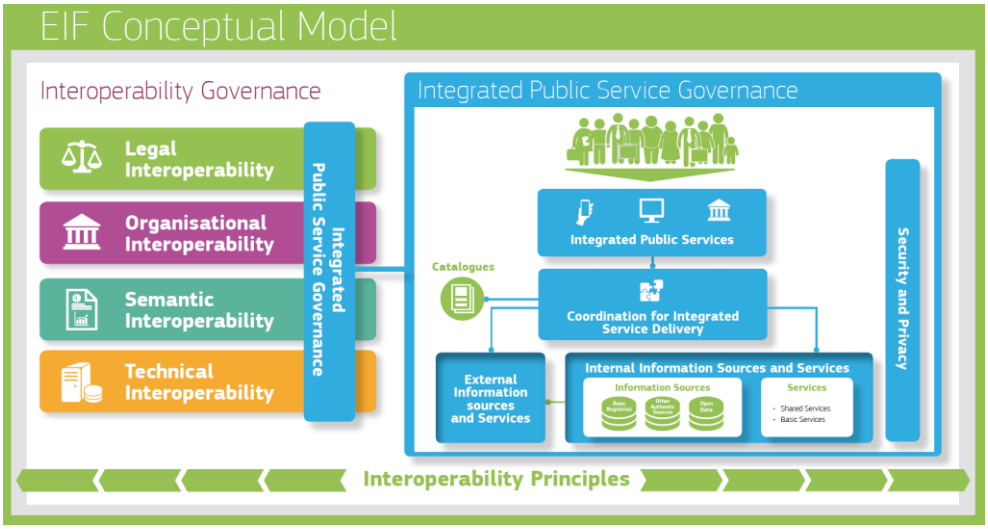

Figure 5 EIF Conceptual Model

The European Interoperability Reference Architecture[24] (EIRA©) is a reference architecture promoting a common framework for designing interoperable solutions within the EU. Among the main objectives there 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. Among its functions, this reference architecture provides support on the selection and assessment of standards and specifications that are aligned with the EIF core principles. Moreover, since the Interoperable Europe Portal should make publicly available and easily findable interoperability solutions, EIRA should be considered for defining the reference architecture of DEPLOYTOUR as for the publication of the solutions and processes in the portal following the IEA.

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

3 Assessment of Data Space Stacks

In this high level analysis, we will address EDC and SIMPL stack since they are the most common technological stacks for Data Spaces.

3.1 Data Spaces components

Based on the DSSC blueprint v2.0, there are different types of services that implement the technical building blocks of the data space. These are, in particular, the so-called Federation Services[25] and Participant Agent Services[26]. The services are used to implement the core components of a data space. The following section uses these components to compare EDC and SIMPL in order to highlight the characteristics of the two software stacks.

3.1.1 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, which is one of the most important components of the data space. The connector makes it possible to implement the basic functionalities required by each participant of the data space and relate to the credential store, local catalog publication, contract negotiation, transfer process and data plane. EDC and also SIMPL provide connectors, which can be deployed either in the participant's infrastructure or by a cloud provider as software as a service (SaaS).

One general difference between the developments of EDC and SIMPL is that SIMPL differentiates between agents for data providers and data consumers, from which different functions are derived. If a participant in the data space wants to be data provider and data user simultaneously, they need two agents with SIMPL. Figure 6 shows the participant agent services, so the functions of the connector according to DSSC, and their relation. These building blocks are described in the following.

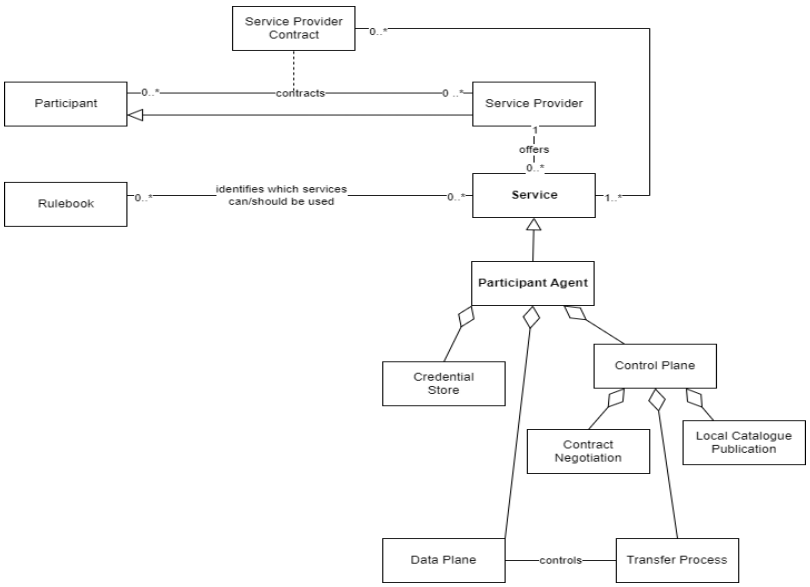

Figure 6 Participant Agent Services diagram

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

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

3.1.1.1 Credential Store

The credential store is used to track the identities and credentials of participants. In addition, the credential store is also used to present a participant's credentials to other participants and to validate the credentials of other participants and is strongly aligned to the "Validation and Verification services" by the Federation. 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 (VC) developed by the W3C for providing credentials and both, EDC and SIMPL use VCs for the identity management.

EDC implements the Eclipse Decentralized Claims Protocol (DCP)[27] which is based on core standards of decentralized identity, including Decentralized Identifiers (DIDs)[28], the did:web method[29], and the VC Data Model v1.1[30] in the so-called Identity Hub. The Identity Hub manages organizational 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 presentation. 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 and without centralized identity management.

The identification system in SIMPL is grouped into two tiers and therefore different to EDC. The main reason for dividing users into two groups is that end users of an organization verify themselves to the organization's connector through company specific Identification, Authentication and Authorization (IAA) mechanism, e.g. EU Login, eID, etc. The core component responsible for these functions is the so-called Tier 1 Authentication Provider which contains information about the users and roles. It uses extended version of Keycloak, an open-source OpenID Connect (OIDC)[31] Identity Provider. Role-based access control (RBAC)[32] 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 have to store credentials in the form of OIDC Access Tokens, more specifically JSON web Token (JWT).

The Tier 2 identity management, managed by the Dataspace Governance Authority, ensures secure and encrypted communication between connectors of the participants and is realized through centralized and decentralized components. The centralized Identity Provider Federation creates, validates, and manages Tier 2 certificates. When a new participant is onboarded, a Tier 2 certificate is created and installed in the participant's connector. It also manages the Security Attribute Provider Federation, which creates and assigns identity attributes for attribute-based access control (ABAC) and provides them in the form of signed ephemeral proofs. The decentralized 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. Authorization at the Tier 2 level is realized through an API gateway that enforces ABAC policies based on the information provided by authentication to control access to resources. The Tier 2 certificate is

[27] DCP: https://github.com/eclipse-dataspace-dcp
[28] DIDs: https://www.w3.org/TR/did-1.0/
[29] did:web Method Specification: https://w3c-ccg.github.io/did-method-web/
[30] VC Data Model v1.1: https://www.w3.org/TR/vc-data-model/
[31] OIDC: https://openid.net/developers/how-connect-works/
[32] RBAC: https://csrc.nist.gov/projects/role-based-access-control

an x509 certificate issued by the certificate authority of the Identity Provider Federation. Identity attributes are assigned by the Data Space Governance Authority and shape the interaction rules between participants.

3.1.1.2 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.

In EDC, catalogs are technically realized 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[33] schemes adhering to DCAT[34] and ODRL[35] specifications, containing datasets that represent the offered data. Each dataset contains a usage policy defined with ODRL. This policy specifies conditions for accessing the data. The datasets also contain one or more distributions, each of which describes the wire protocol (e.g., HTTP pull, S3 push) through which the data can be accessed. In addition, access services are included, which provide the 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 customized 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 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 contract negotiation ID is created to initiate contract negotiations with data consumers. 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.

3.1.1.3 Contract negotiation

Contract Negotiation refers to the part of the connector in which access and usage policies are enforced. After publication of the data product, the connectors of the data provider and the data consumer initiate the contract negotiation and match the policies of the two participants.

In EDC, contract negotiation is realized 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[36]. 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 exchanges by implementing transactions where state transitions are only committed upon successful acknowledgment from the counterparty. Messages are idempotent and include unique IDs. If not acknowledged, they are resentful, and the receiver handles de-duplication. The EDCs eventing system allows developers to subscribe to events, such as the finalization of a contract negotiation, using the EventRouter with support for asynchronous or synchronous transactional notifications.

[33] JSON-LD: https://json-ld.org/
[34] DCAT: https://www.w3.org/TR/vocab-dcat-3/
[35] ODRL: https://www.w3.org/TR/odrl-model/
[36] 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 SIMPL, contract negotiation refers to the same process as EDC. Nevertheless, the Contract Negotiation Adapter component is very important in 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 and sends requests for an offering from 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 the contract negotiation with the provider's connector and retrieves the status of the contract negotiation. This guarantees that both, data provider and data consumer have a mutual understanding and agreement on the data usage policies.

3.1.1.4 Transfer process

The transfer process is available as soon as the contract negotiation has been successfully completed and executes the concluded data sharing contract via the data plane.

In EDC, the transfer process manages data sharing between data provider and data consumer after the contract is finalized. Initiated via the Management API, transfers can be finite (like a file transfer) or ongoing (like continuous data streams). EDC supports two modes: First is a data consumer pull, where the data consumer retrieves data from the data provider, and second is 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 synchronized 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 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 and facilitates their exchange between participants, efficiently managing this process by implementing the 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 seamless and secure data exchange within the data space by utilizing standardised connectors and protocols suited to different data types and transfer requirements.

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

3.1.1.5 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, utilizing 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 like a Kubernetes cluster, allowing for 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 offers 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.

3.1.2 Federation Services

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

It is important to note that data spaces are usually distributed in nature. This means that there is not necessarily a central platform where all data is stored. In most cases, participants in a data space manage their own data and can decide for themselves whether or not to share it with other participants, sometimes even in multiple data spaces.

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

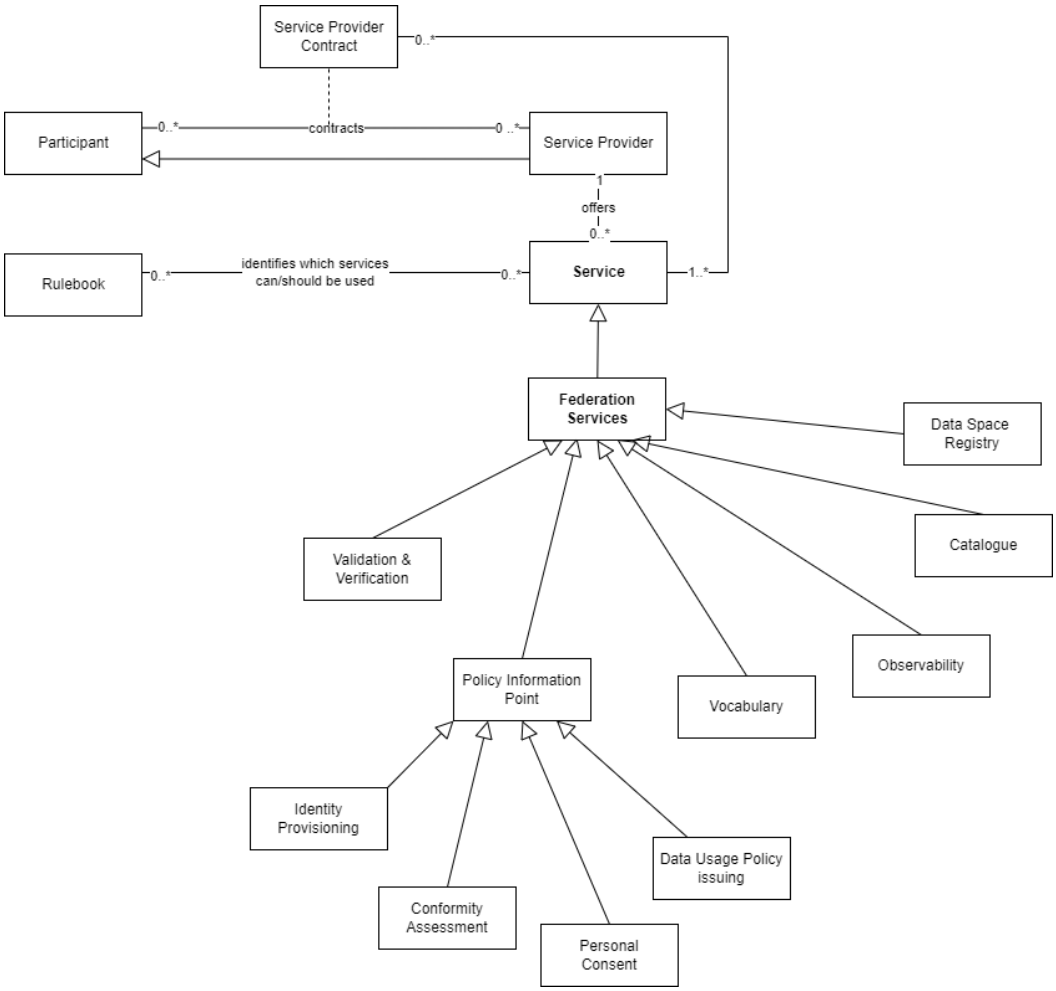

Figure 7 Federated Services diagram

3.1.2.1 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 and therefore, unmatured service.

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 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).

3.1.2.2 Validation and Verification services

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

The services are very closely related to the credential store of the connector and have already been described there in section 4.1.

3.1.2.3 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 (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 through the sections of 4.1.

3.1.2.4 Catalogue services

Catalogue services offer an overview of registered data products within the data space and provide links 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[37].

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 facilitates the two-tier approach for IAA, 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[38] 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.

3.1.2.5 Vocabulary services

Vocabulary Services provide an overview of available data models within the data space, allowing participants to select common data 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.

In SIMPL, the Vocabulary Management component is part of the Metadata Description building block and 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 frontend application.

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

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

3.1.2.6 Observability services

Observability Services are services that 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.

EDC has several extensions for this. These are based, for example, on Micrometer[39], JDK logger[40] or Events Cloud[41] and thus offer solutions for monitoring, logging and the management of event streams.

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 component. The key functions of the Observability component are monitoring technical logs of the SIMPL-Open agent infrastructure, automating of the deployment of a preconfigured monitoring dashboard and monitoring of 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.

3.2 Analysis of related Data Spaces and initiatives

Analysis of other DS initiatives that might be relevant for 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 (Annex II).

3.2.1 Austrian Data Space

The Austrian Tourism Data Space[42] is a national initiative with a strong focus on enhancing interoperability and driving innovation within 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) provided by Nexyo (an Austrian IT company), which facilitates secure data sharing and consumption, while also enforcing usage policies and ensuring traceability. By aligning with X split model of the Gaia-X, the data space further promotes technical compliance and fosters trust at the ecosystem level, while preserving data sovereignty for all participating actors.

Within this framework, Austria Tourism (Austria's national tourism organization) plays a pivotal role acting as a Trust Anchor and Governance body, ensuring the data space operates according to Gaia-X principles. (See figure 8)

[39] Eclipse EDC Micrometer: https://github.com/eclipse-edc/Connector/tree/main/extensions/common/metrics/micrometer-core
[40] Eclipse EDC Extension JDK logger: https://github.com/eclipse-edc/Connector/tree/main/extensions/common/monitor/monitor-jdk-logger
[41] Eclipse EDC CloudEvents Specification: https://github.com/eclipse-edc/Connector/tree/main/extensions/common/events/events-cloud-http
[42] Austrian Tourism Data Space: https://www.tourism-dataspace.com/en

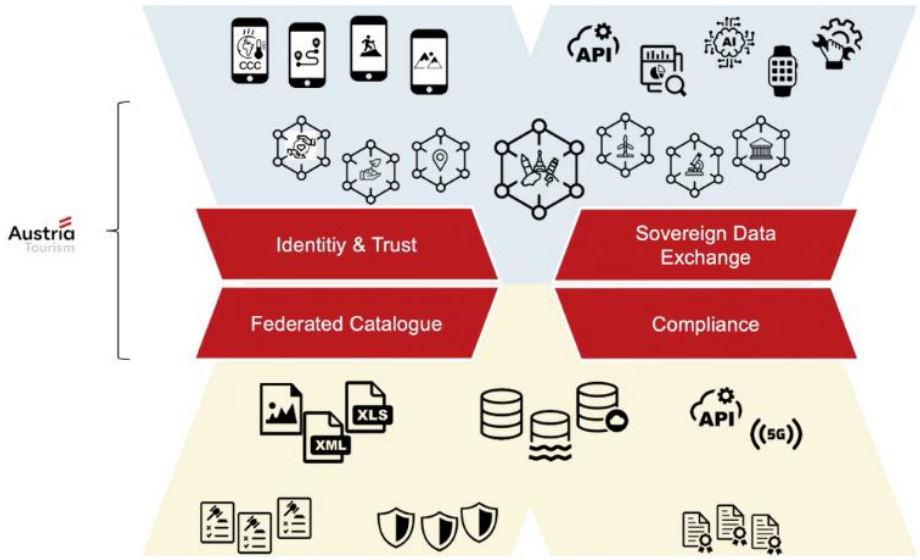

Figure 8 Austrian Tourism operating according to Gaia-X principles

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 organizations 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 decentralized identity of the organization 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 organizations 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 they can share only the desired data and nothing in addition. For those who wish to share highly sensitive data, vector embeddings, etc. it is foreseen that anonymization, 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 decentralized, federated catalogue. This setup is shaped by the current maturity level of related EDC components, which limit immediate realization. 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 decentralized 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.

3.2.2 EONA-X

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

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

3.2.2.1 Architecture principles

EONA-X technical architecture aims at being 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 emphasises:

- 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.

3.2.2.2 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) that implements this protocol as the default within the framework and thus provides ready-to-use extensions devoted to it. In addition, the EDC follows the latest version of the IDSA rulebook in terms of concepts and organization of data spaces. IDSA's principles aim towards decentralization as the default solution architecture, having centralized components where applicable and useful (feature-wise or to allow business models).

The Dataspace Protocol (DSP) works around well-adopted industry standards such as the W3C DCAT V3 catalogue vocabulary and the W3C ODRL policy expression language, which is an enabler to ensure interoperability with other data paces.

3.2.2.3 Self-Sovereign Identity (SSI) management

The Identity and Access Management (IAM) strategy to be enforced for exchanges between the components is setup 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 authorization (relying on a centralized authorization server to authorize access to the resources).

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

This decentralized identity approach enables each participant to remain in control of their identity and credentials and removes the need for a centralized authorization server that can be a central point of failure for the data space. Hereafter, we will focus on this decentralized identity management approach.

3.2.2.4 High level design

The following high level design diagram depicts the components of the architecture. Mandatory components are represented with solid bold lines and optional ones are depicted with dashed bold lines. All these components fall in 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.

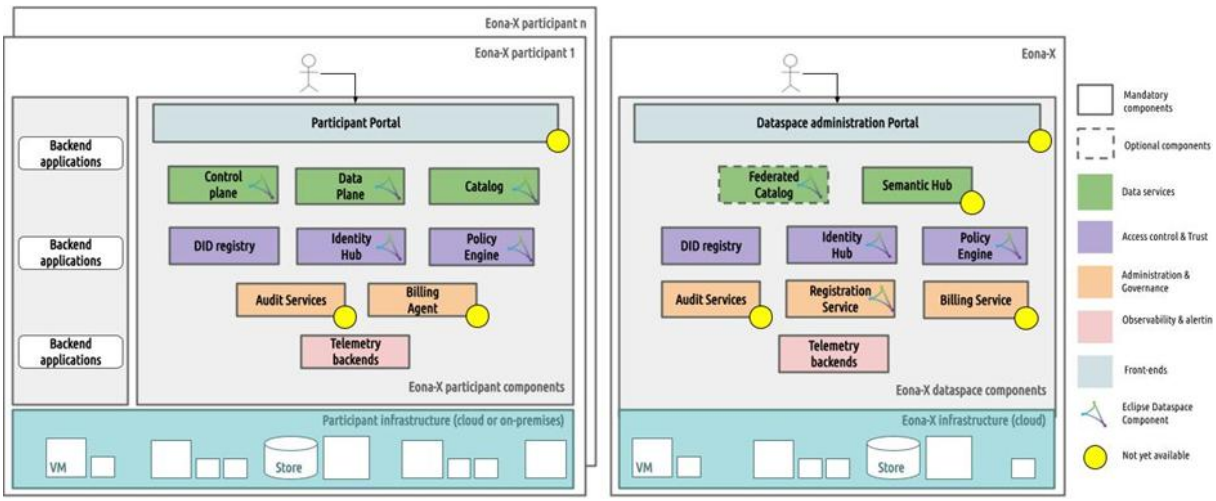

Figure 9 High-level design of the architecture

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

3.2.2.5 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 through REST API, and will support bulk data transfers (e.g., transfer of large files) 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 through other participant catalogues for discovering 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 is yet to be done, 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 decentralized 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 is yet to be done, and it is currently not available for participants or the data space.

- **Audit Services:** Audit Services are used for auditing purposes. They contain a log where all actions performed by participants are recorded immutably. Participants can be inspected by EONA-X through the data space Audit Services to ensure compliant behaviour and undertake organizational or legal measures if needed. The technology selection for this component is yet to be done, and it is currently not available for 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, 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.

3.2.2.6 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 Decentralized Identifiers (DIDs) to enable verifiable, decentralized 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). VCs are issued by trusted entities, 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 contract offer persist in a local database, whose technology is up to the participant as long as there is a suitable EDC extension for this 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 centralized 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 only allowed if all policies bound to the current scope are fulfilled.

- **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, a digitally signed contract is generated and stored by both parties. The negotiation can be automatic or involve manual acceptance. The provider can revoke the contract if 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 parallelizing the data.

3.2.3 deployEMDS

This section describes the deployEMDS[43] 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 the release of SIMPL occurred 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.

In terms of architecture the project is following the DSSC guidelines with the building blocks architecture mode (Figure 10).

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.

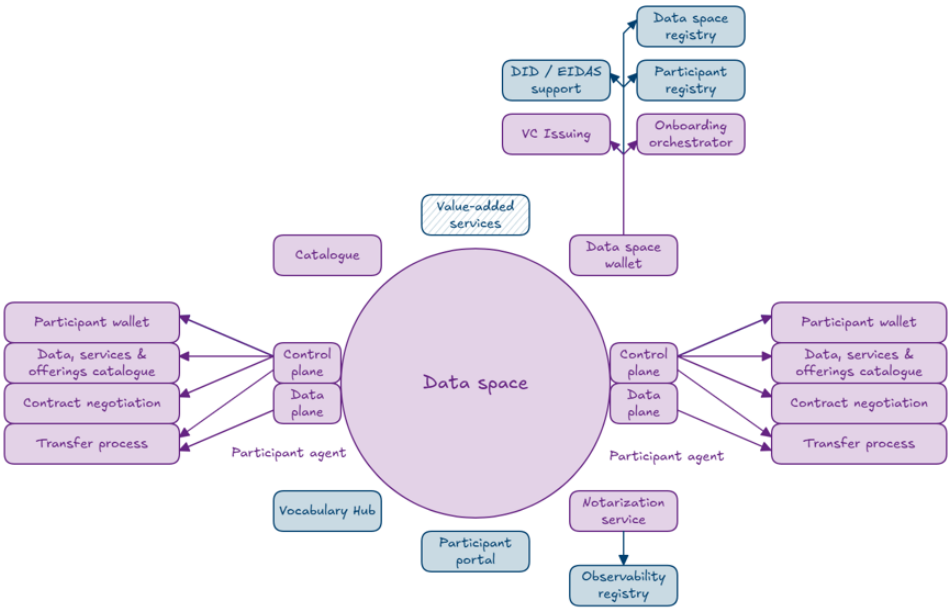

Figure 10 DSSC building blocks guidelines

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

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

implementations. Figure 11 illustrates the different 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 in operation or are operational for internal purposes with minimal features, like 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[44].
- 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.

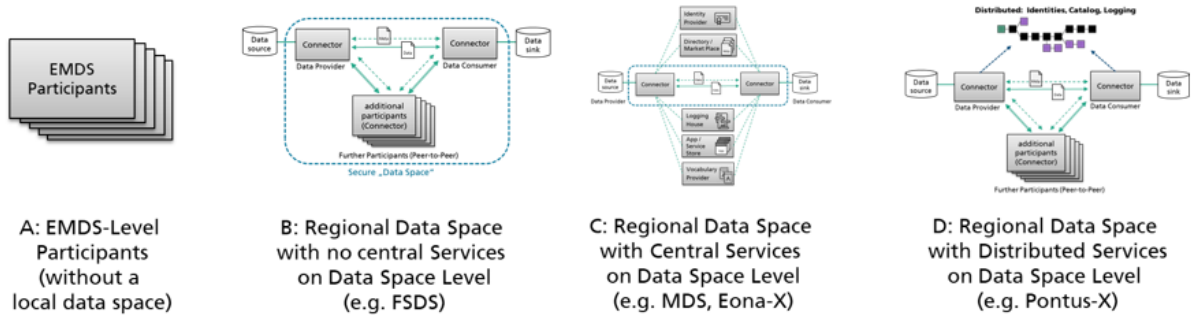

Figure 11 EMDS different architectural scenarios

The deployEMDS architecture includes a central data catalogue for efficient data discovery across Europe, using harvesting mechanisms to synchronize 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.

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

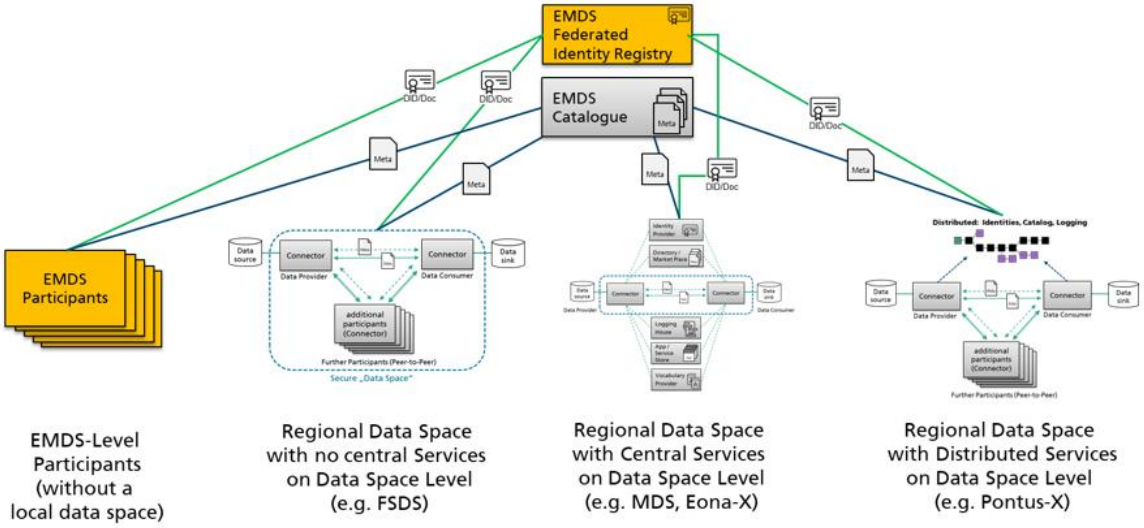

Figure 12 EMDS Decentralized Identifiers

3.2.4 Cultural Heritage Data Space

This section aims to introduce the infrastructure underlying the Europeana platform[45], 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.

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 digitized cultural content.

It operates on a **c**entralized aggregation model, where metadata from cultural institutions flows through trusted intermediaries, referred as aggregators, into a centrally managed infrastructure. These aggregators ensure high data quality, legal compliance, and metadata standardization.

The key layers of the platform, depicted in Figure 13, are:

- Europeana Portal**.** The public-facing platform where users can search and explore cultural heritage collections which are available through 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.

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

- 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, linked open data principles, and aligns with major cultural heritage standards like Dublin Core, LIDO, and CIDOC CRM.

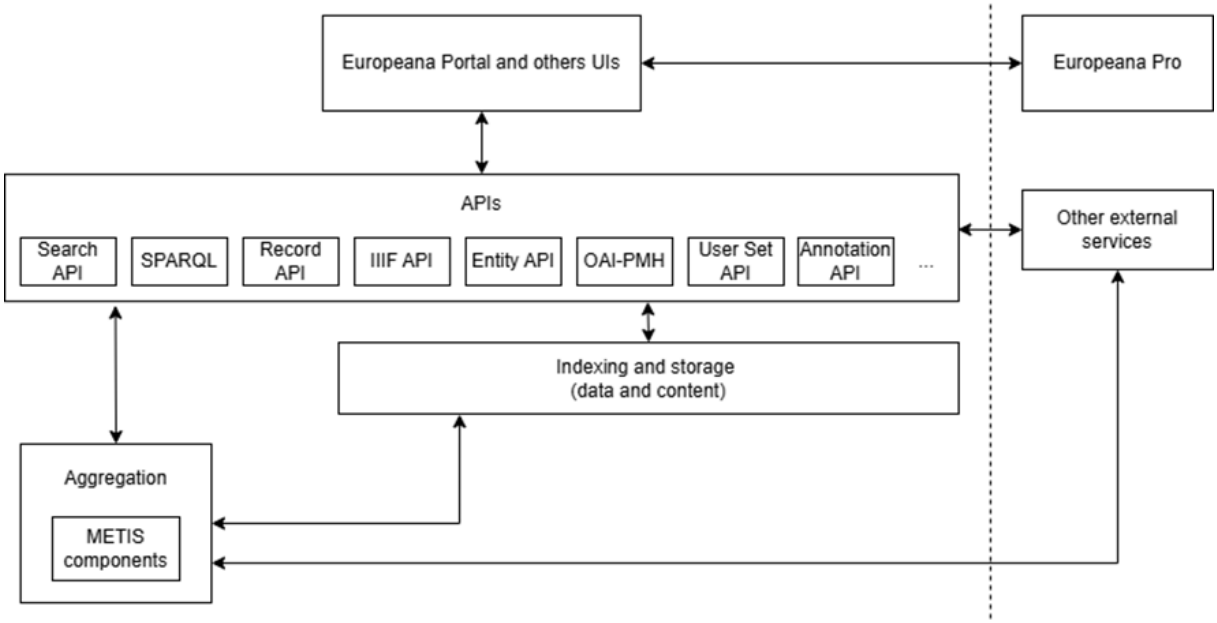

Figure 13 Key layers from Europeana Platform

Regarding asset publication, Europeana follows a centralized process where cultural institutions, mostly via the aggregators, submit metadata about 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 decentralized, peer-to-peer API frameworks, Europeana aggregates and indexes the data centrally, offering a unified and optimized API layer.

While the metadata flow is centralized, the federated aspect is supported by the distribution of the actual content, which resides in the data providers' own repositories. Most of the organizations participating in this initiative adhere to open data principles as Europeana initiative strongly encourages to share the data as openly as possible to boost the reuse of

digitalized cultural data. For the possible few that do 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, machine-readable declarations that indicate the copyright status of a digital object and clarify whether, and under what conditions, it can be reused. 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 centralized Europeana approach and implement and provide access to these additional services in a decentralized 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 of use within the cultural heritage domain as well as 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 summarize, 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 like Gaia-X, promotes a decentralized, federated approach to data sharing, where both data and metadata remain distributed and are accessed through secure and transparent peer-to-peer mechanisms. In contrast, this initiative lacks a basic data catalogue (e.g., DCAT), opting instead for built-in functionalities that allow direct interaction with the data content. It adopts a centralized aggregation model for metadata, which is 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 working space for cultural heritage professionals and researchers. The ECHOES project[46] 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-

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

access APIs is essential, and detailed integration guidelines will be provided by ECHOES. Funded projects must dedicate resources to ensure technical compatibility, flexible design, and effective collaboration within the ECCCH ecosystem.

3.3 Establishing the Minimum Viable Data Space (NTT DATA)

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

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

Here we consider that the participant has implemented his connector as a CaaS (Connector as a Service) or on premise.

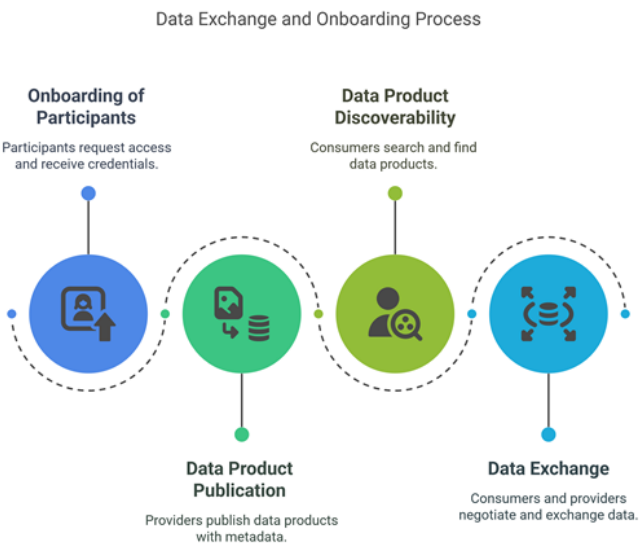

Figure 14 Data Exchange and Onboarding Process (Annex III)

3.3.1 Onboarding of participants

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

- Data space 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, data provider or a data consumer who joins the data space.

The onboarding process involves five main steps:

3.3.1.1 DS onboarding

The participant fills a request which is the formal petition to access the ETDS through the Data Space Portal. The request requires identification attributes in order to properly proceed to the registration.

3.3.1.2 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 demands that the data space is described, Data Space rules and policies are defined by the data space governance authority and should be machine-readable in order to automate the process. Based on these data space rules and policies, the Data Space Registry manages the registration of participants which can be in two phases: onboarding or offboarding. Hence, a list of trust anchors is obtainable, providing full insight on the list of trusted participants. Lastly, the Data Space Registry permits to issue and store through protocols a verifiable credential (VC), identifying each participant.

3.3.1.3 Management of the registration

Next step is to conduct an assessment, in which the Data Space Governance Authority manages the request of the participant. Two scenarios diverge from this point: on accepted requests the process will proceed, meanwhile, on the assumption the request is rejected, the participant is required to inquire for a new request.

3.3.1.4 VC issuing

Supported by the Data Space Registry, a verifiable credential (VC) is conceded and eventually integrated to a wallet, ultimately being the digital identifier throughout the Data Space.

3.3.1.5 Participant VC

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

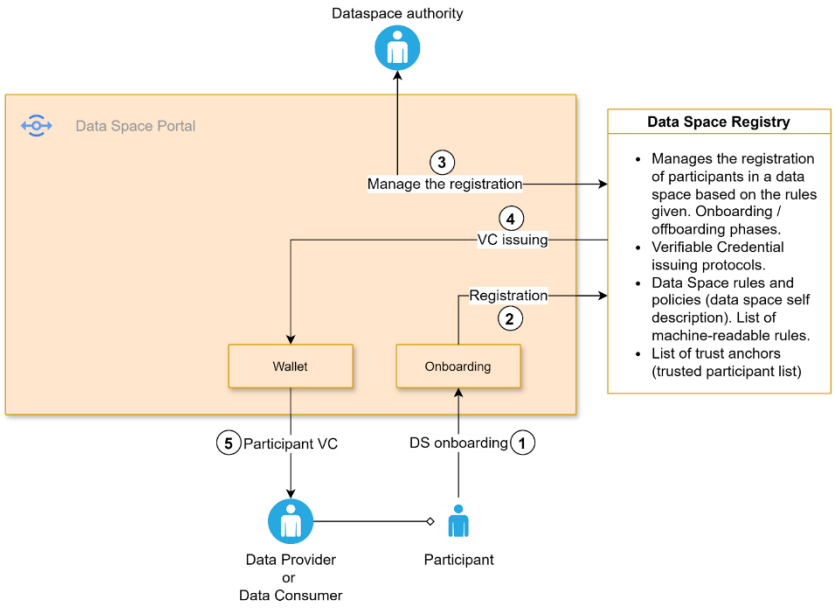

Figure 15 Onboarding of participants' diagram

3.3.2 Data product publication

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

The data product publication process involves seven main steps:

3.3.2.1 DS authentication

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

3.3.2.2 Authorisation

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

3.3.2.3 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.

3.3.2.4 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 organize semantic resources, granting coherence and interoperability. It includes resources in terms of vocabulary, ontologies, application profiles and data schemes.

3.3.2.5 Data space connector

The information regarding the dataset and their metadata is then validated through the Data Space Connector, a cataloguing functionality.

3.3.2.6 Catalogue publication

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

3.3.2.7 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.

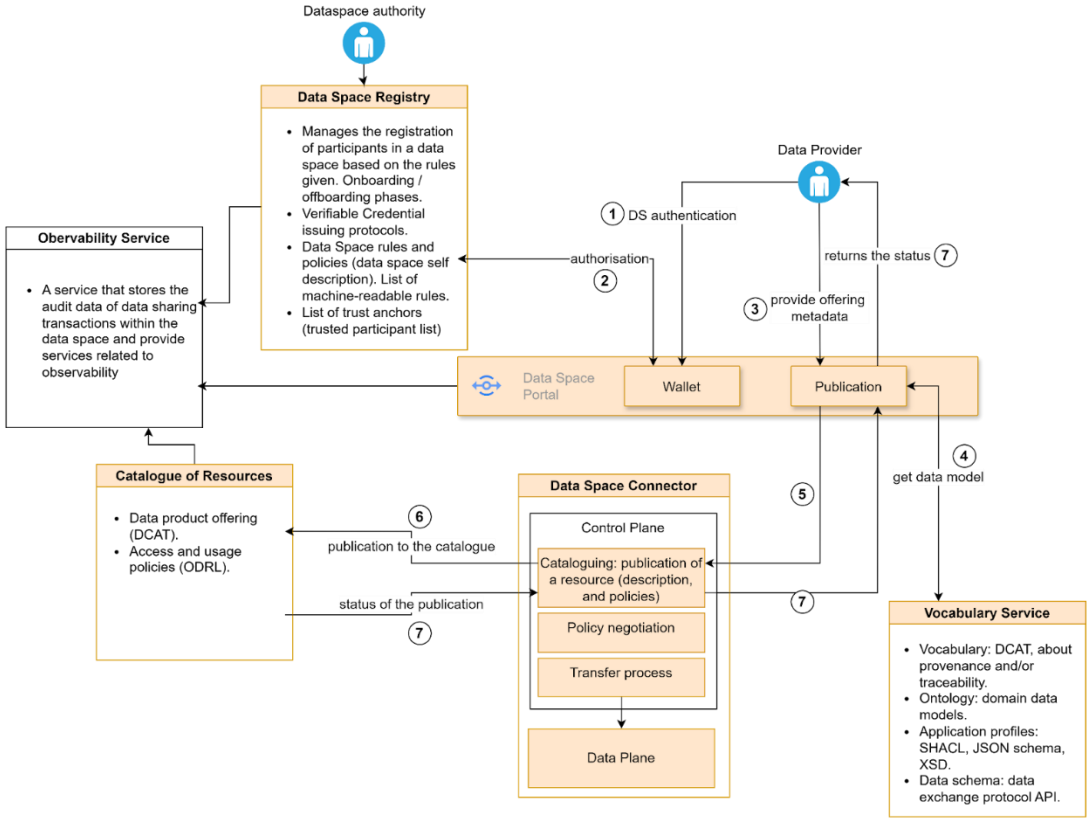

Figure 16 Data product publication diagram

3.3.3 Data product discoverability

Discovery of data products within the resource catalogue allows the data consumer to query datasets as well as information of what it contains as well as the use policies.

3.3.3.1 DS authentication

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

3.3.3.2 Authorisation

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

3.3.3.3 Search for an offering

Once the data consumer is authenticated and authorized, 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.

3.3.3.4 Return of the offerings

Lastly, the resource catalogue retrieves the available offering list that are 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, the service storing and auditing the actions within the Data Space. Overall, the focus is to trace datasets plus ensure the provenance.

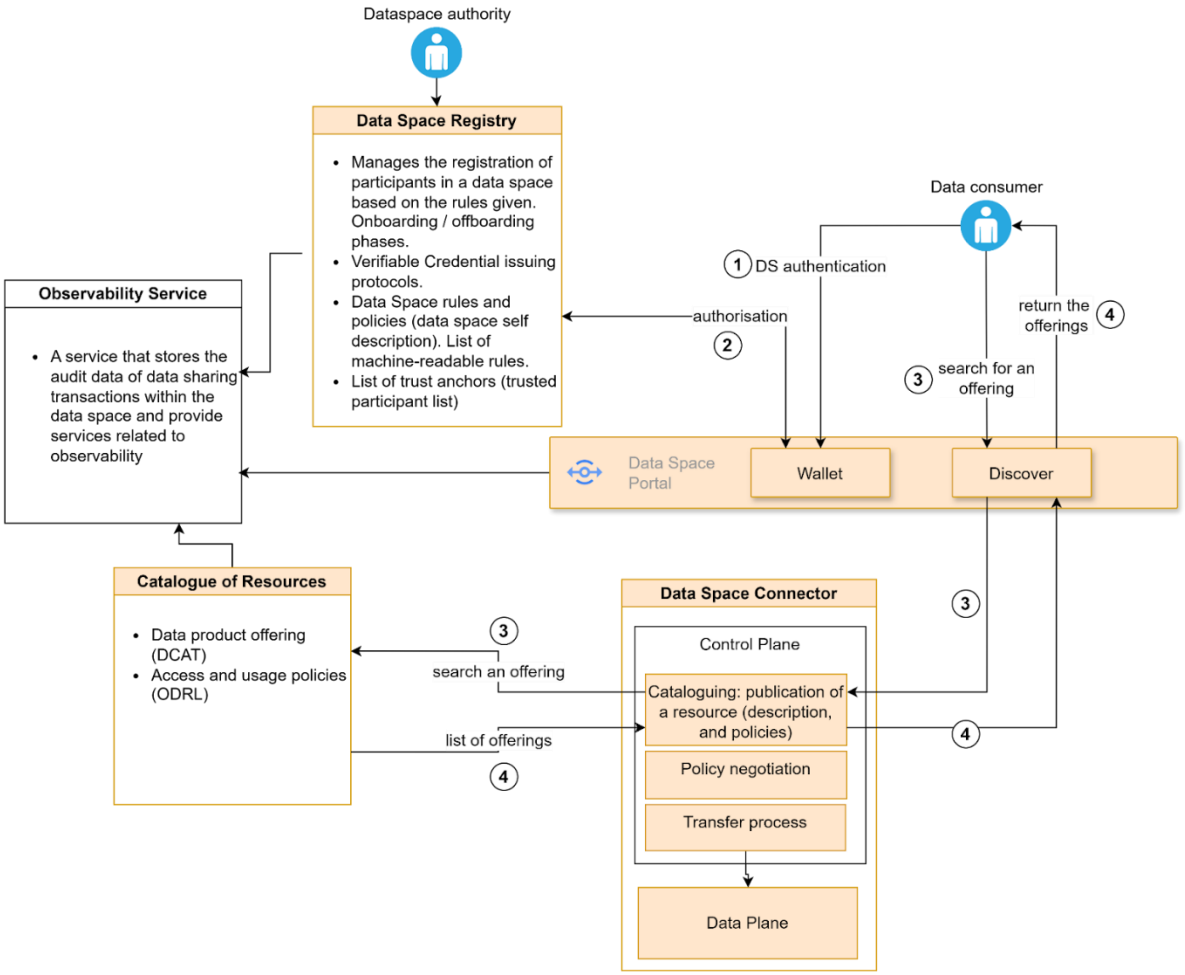

Figure 17 Data product discoverability diagram

3.3.4 Data exchange

Data exchange relies on a centralized ecosystem that allows potential data sharing between different organizations or companies. This process consists of two phases: contract negotiation and data transaction.

Contract negotiation implies that data provider and data consumer come to an agreement in order to utilise a dataset whose propriety relies on the data provider.

3.3.4.1 Request a contract for an offer

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

3.3.4.2 Negotiation protocol

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

3.3.4.3 Agreement/rejection of the offer

The data provider connector shares the offer to the data provider, who decides whether the offer is agreed or rejected. Given the scenario of a rejection, the negotiation concludes.

3.3.4.4 Persist agreement

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

Every transaction is monitored by the Observability Service, the service storing and auditing the actions within the Data Space, habilitating further data transactions.

Data transaction implies that every agent is authenticated and authorized beforehand to ensure the process can proceed through the 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 habilitate the transaction according to 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 authorizes the request. It is then transferred to the PDP (Policy Decision Point), evaluating the policies. 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) authorizes the request, the data exchange proceeds through the data plane of both connectors. On completion, data consumers can visualize the datasets.

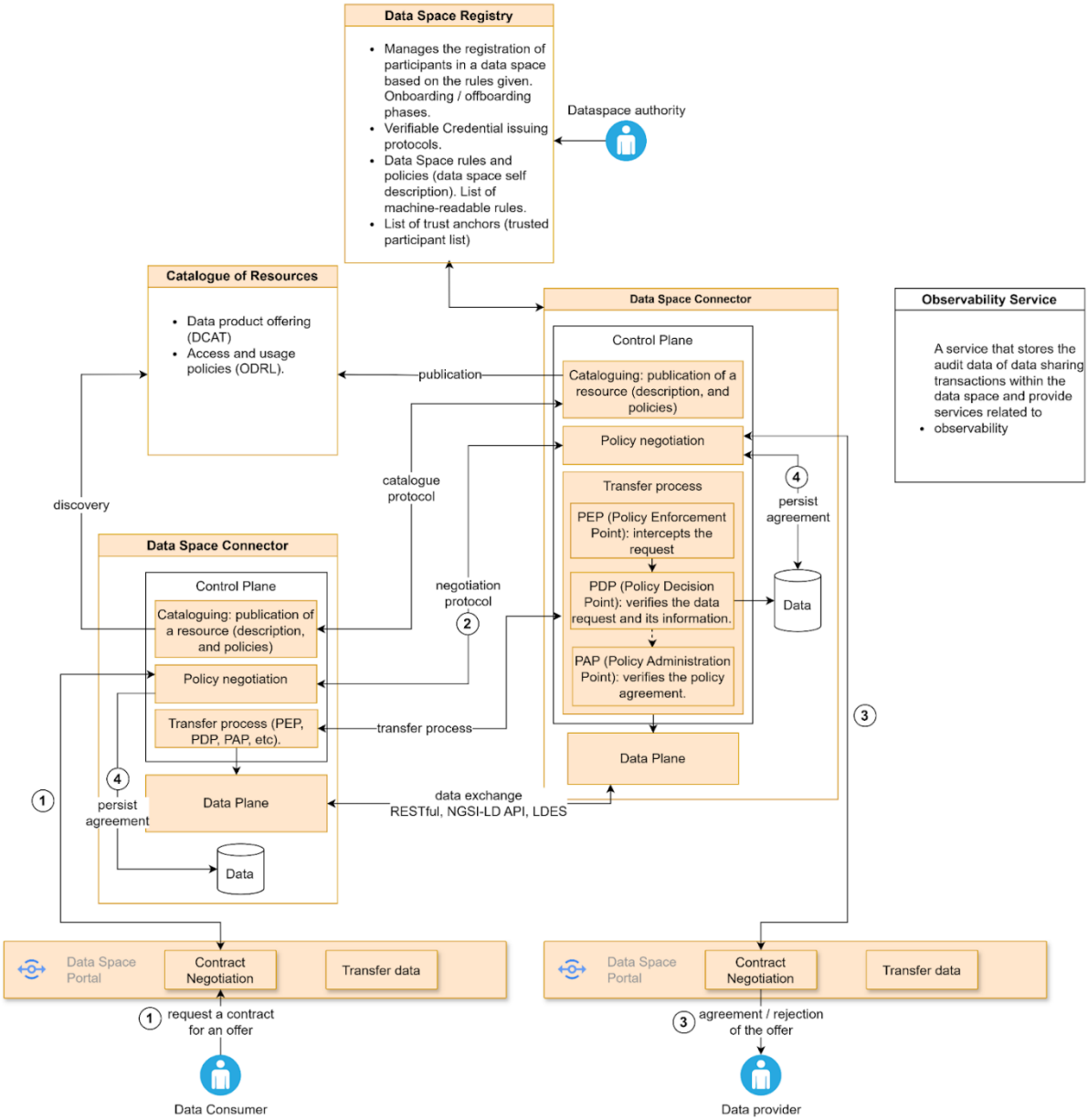

Figure 18 Data product exchange diagram

3.3.5 Technological Stack decision

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

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

Disclaimer: This section is incomplete. A primary analysis of the dataspace 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 achieved until the conclusion of the use case analysis.

Furthermore, during the assessment of stacks, some initiatives illustrated that distributed systems and their federation has become an architectural imperative. 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 prevents the deployment of MVDS.

This assessment also reveals key limitations that should be reshaped in a continued iteration to confirm the identification of requirements, their grouping, and the scalability and interoperability of either of the stacks in the context of the ETDS.

4 European Tourism Data Space Architecture

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

4.1 DEPLOYTOUR as a Federated Data Space Architecture

This section lists the minimum components of the ETDS enabling the federation of different 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 of the GAIA-X architecture, specifically for federation of catalogues, consisting of multiple components and reusing existing technology and allowing scaling. Among them, Keycloak is used 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.

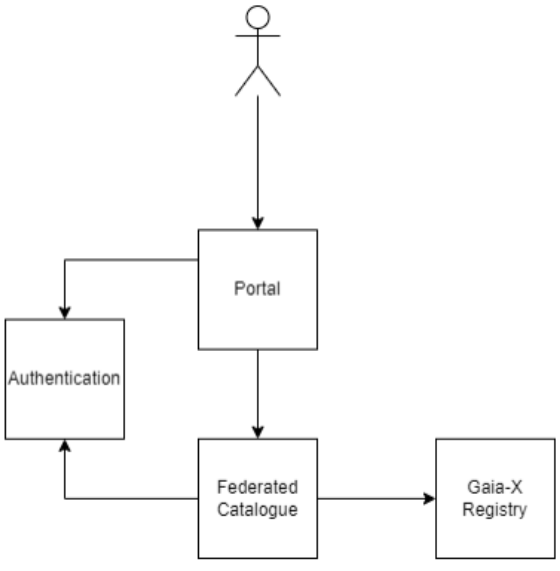

Figure 19 Overview of the architecture of the Federated Catalogue, according to GAIA-X

4.1.1 Identity and Access Management

Proposal: Implementing Self-Sovereign Identity (SSI)

Executive Summary

This proposal recommends that the Tourism Data Space adopts a Self-Sovereign Identity (SSI) framework based on the W3C Decentralized Identifier (DID) standard. This approach enables decentralised identity and verifiable credential exchanges using standard web protocols, offering enhanced user control, data protection, and interoperability. The proposal is aligned 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 organizations and individuals to create decentralised identifiers. Each identifier links to a DID document, which 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 in such a way that 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 trustable 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 contains a method, which refers to a dedicated specification explaining how the DID document can be resolved, depending on the nature of the registry wherein the DID document persists.

Specifically, the architecture relies on the did:web method, which involves that the DID registry is exposed via http web server.

DID can be leveraged to enable IAM by also introducing an Identity Hub (or Decentralized Web Node, see specification), which is a data storage where each subject stores its VCs. The endpoint of the subject's Identity Hub is made public through the DID document of the subject. Thus, when two subjects interact with each other in such 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).

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).

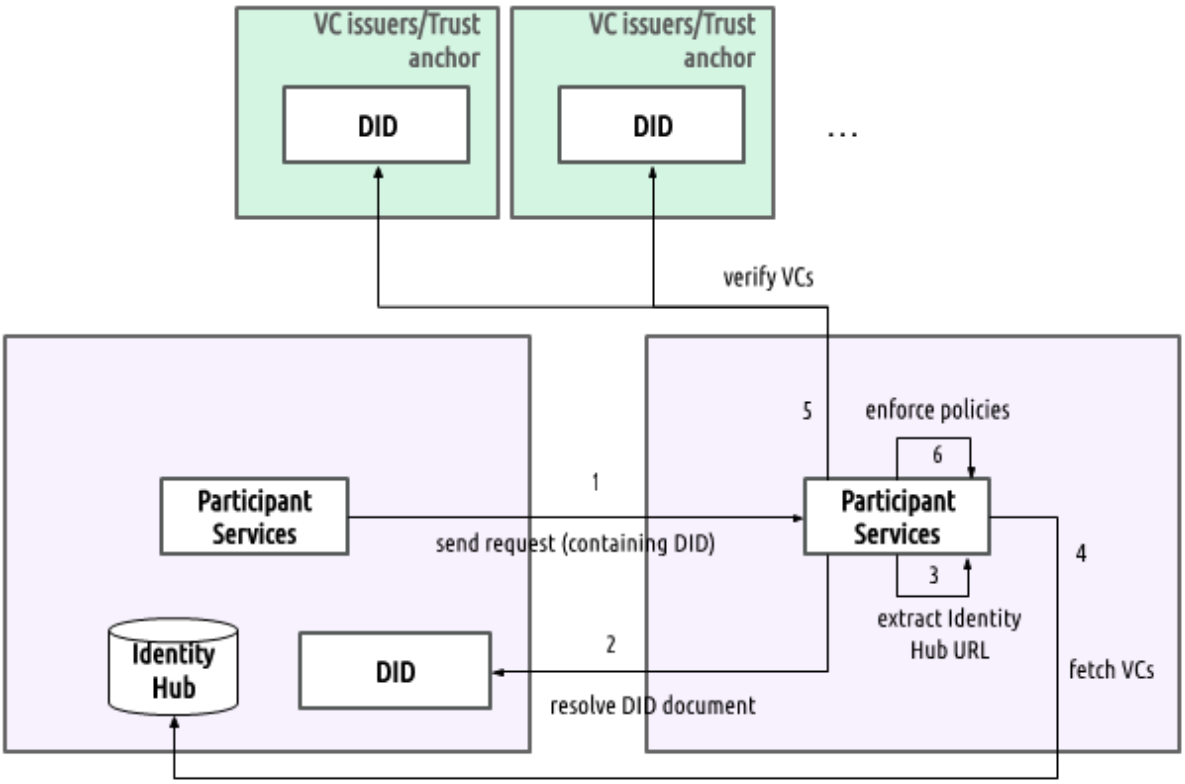

Figure 20 Participant authentication and access control in an SSI context

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 the trustable and relevant VC Issuers in the context of this data space, which are called the Trust Anchors. The following diagram illustrates the complete IAM process described above.

As an important consideration, the implementation of Attribute-Based Access Control (ABAC) for leveraging VC and dynamically evaluating access conditions will allow for more contextual and role-specific access control, extending beyond simple role-based schemes.

Conclusion

This model fosters secure and trusted data exchange while ensuring that identity management is decentralised, standards-based, and in line 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.

4.2 High level Architecture design

This section aims to provide a first sight of the high level architecture design of the ETDS. The proposed high-level architecture is not supposed to describe the various layers of the reference architecture of the ETDS but seeks to design a general perspective of how the data space should resemble.

4.2.1 Recommendations

The Consortium considers using a standardised language for the description of the different capabilities that have been defined in the requirements collection. These languages are the Business Process Model and Notation (BPMN), the Unified Modelling Language (UML) and the ArchiMate specification. These three languages are maintained by the Object Management

Group (OMG) and can be used in open access tools such as Modelio or Archi. According to the Open Group website, among the main benefits of using these languages there 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, components 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 design of the ETDS reference architecture is ArchiMate. While UML makes use of a formal language for designing any type of software component or system, and BPMN on the other hand, 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 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 EU level.

4.2.2 ETDS high-level architecture

Both the EIRA model and its specialisation to e-government, the eGovERA model, uses and extends the ArchiMate modelling language to represent their models visually and logically. As analysed in section 3.2.6, 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. The interesting point is that eGovERA provides a specific approach to tackle data spaces.

A view of the ArchiMate diagram-model depicting the eGovERA building blocks and the relationships between these building blocks is available online (Annex III).

4.2.3 Connector and Data Transfer

The EIRA/eGovERA Business Agnostic Reference Architecture 6.1.0 is modelled through the Cartography Tool (CarTool©), using the Archi plug-in for EIRA. In the centre of the diagram, the data space connector is depicted considering both the connector provider and consumer (i.e., the data space participants) with an association relationship with a data-related building block. Interestingly, (which "enables the implementation of digital or non-digital information collected, stored or processed by a computer system or other information technology infrastructure").

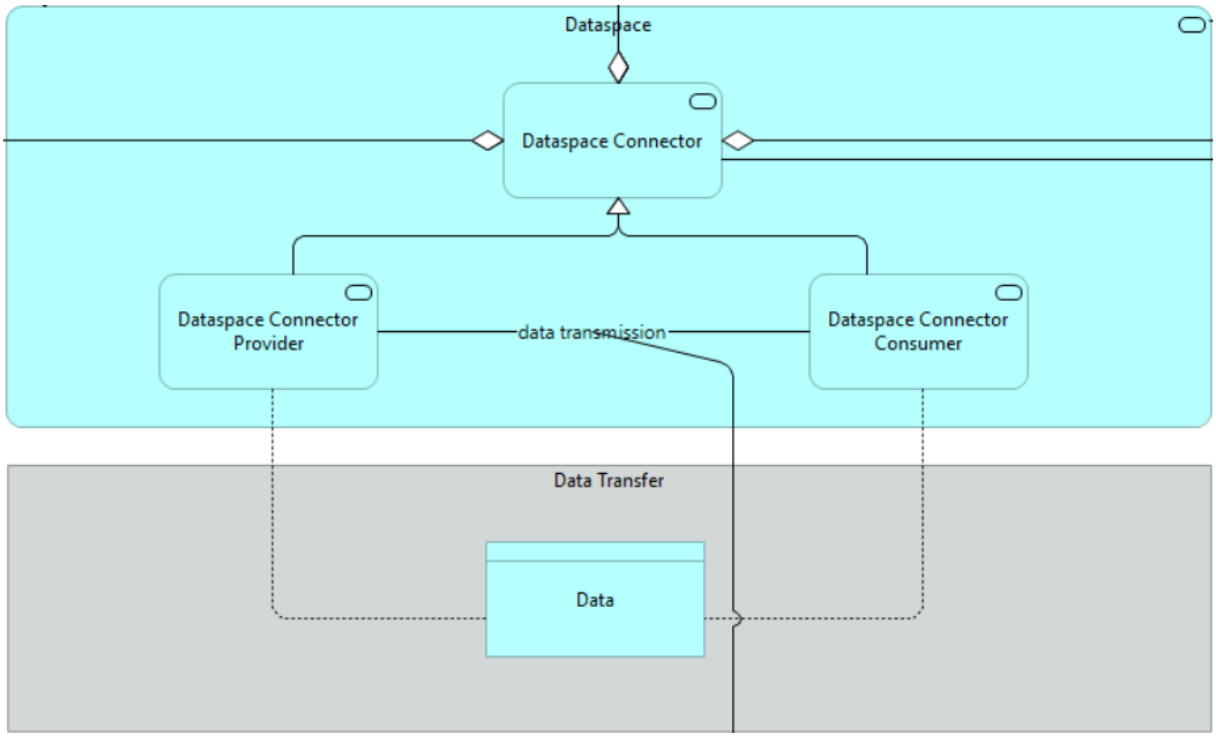

Figure 21 EIRA/eGovERA Business Agnostic Reference Architecture approach for data spaces. See Annex *III* to zoom on the different parts of the data space enabler

4.2.4 Identity and access to platforms and vocabulary hubs

Following the top side of the diagram, in the Identity Provider package, the building blocks related to Identity Management, both in a decentralised and centralised approach, models the processes, policies and technologies that manage and secure digital identities (either of participants, systems or applications). It is also interesting to point out the Vocabulary Management package, which contains the Vocabulary Hub as a centralised repository or platform comprehending source of terms, definitions and relationships between concepts in use among participants, systems and applications. The building blocks for identification and access are conceptually aggregating to 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).

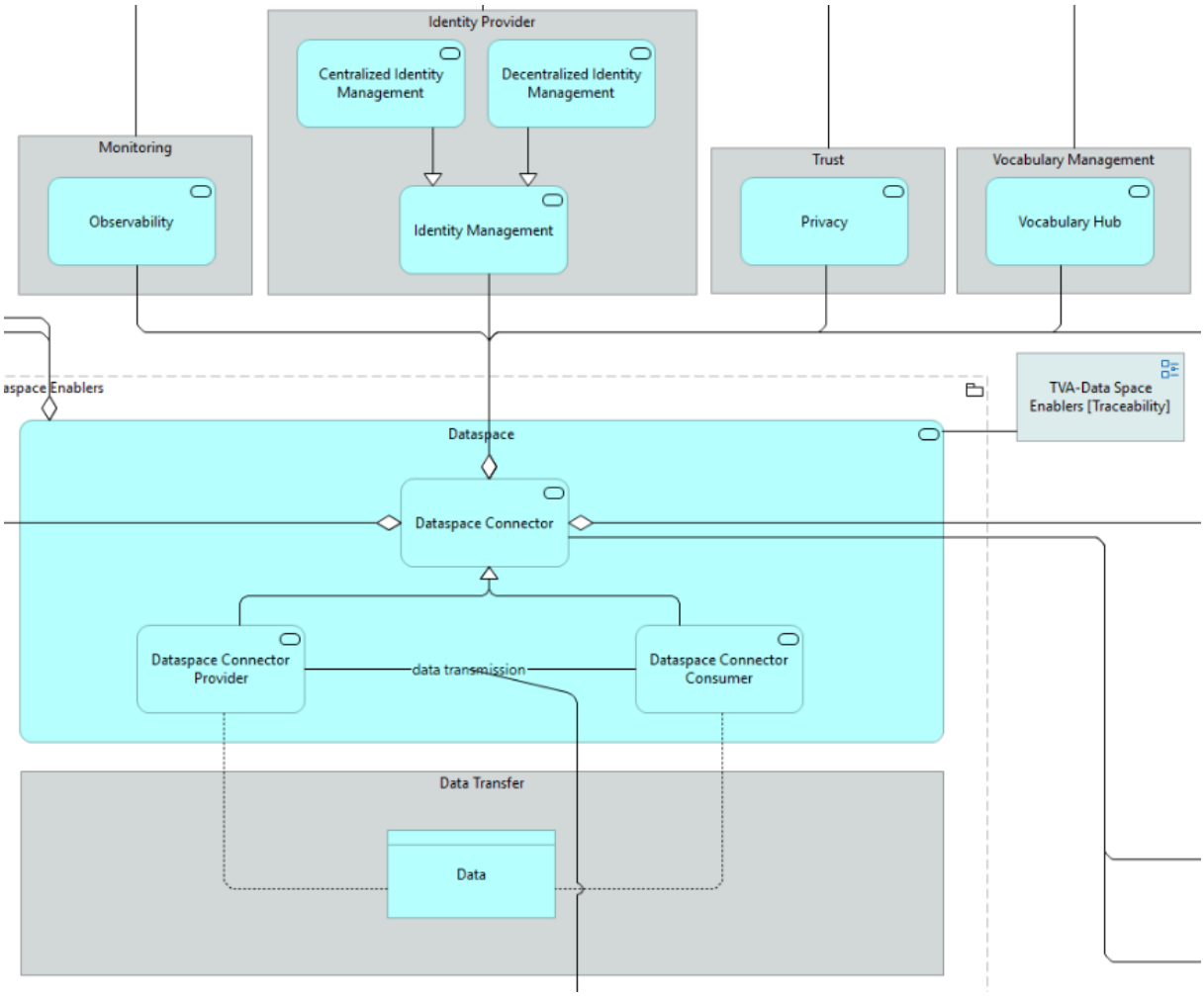

Figure 22 EIRA/eGovERA Business Agnostic Reference Architecture approach for data spaces. See Annex III to zoom on the different parts of the data space enabler

4.2.5 Registry and App Store

Following the left side of the diagram, in the Connectors Registry and App Store package, the building blocks Service Registry and Service Discovery and Registry supports the discoverability of services and connectors. At this first stage, the Consortium considers providing a Dataspace Portal from where participants get the connector and find products and services from a centralised perspective; however, the idea of providing decentralised portals will be on the loop in future iteration. 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. All the two packages are aggregating to the Dataspace Connector building block facilitating federated data discovery and indexing and ensuring that all participants agree on usage rules, as well as compliance and data governance principles before engaging in the data exchange.

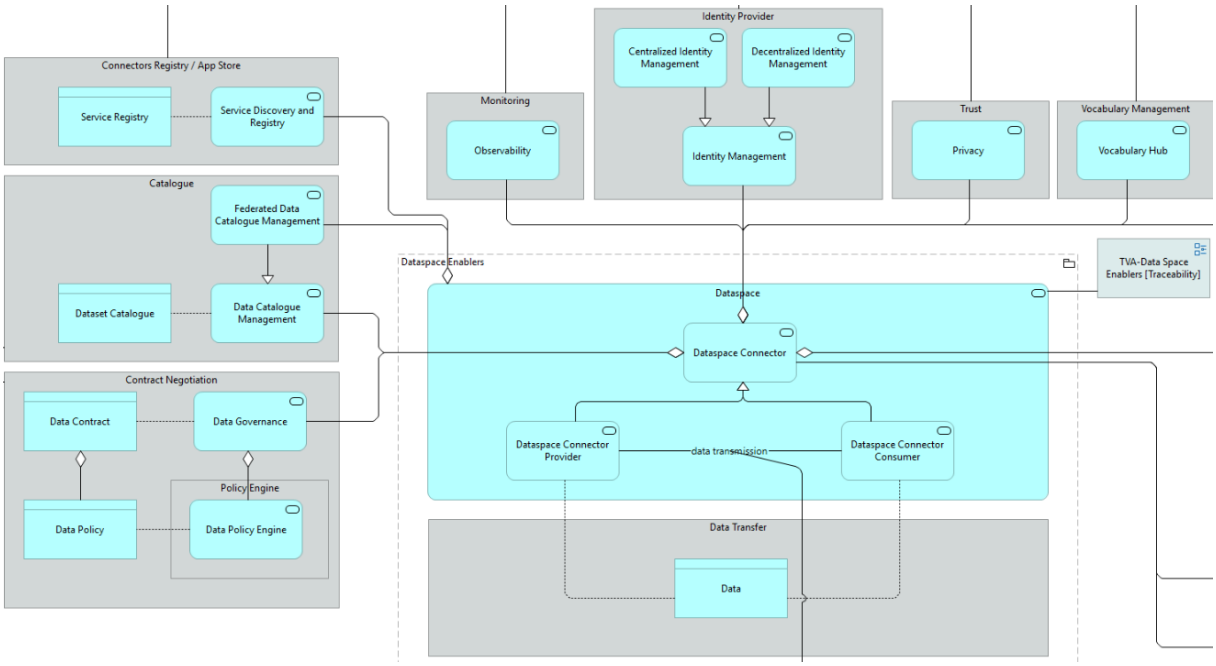

Figure 23 EIRA/eGovERA Business Agnostic Reference Architecture approach for data spaces. See Annex III to zoom on the different parts of the data space enabler

4.2.6 Analytics and Data Quality

Finally, on the bottom right side, the Data Analytics and Quality package comprehends the Data Analytics and the Data Quality building blocks ensuring that the shared and integrated data is fit-for-purpose across the ecosystem as well as optimising business processes.

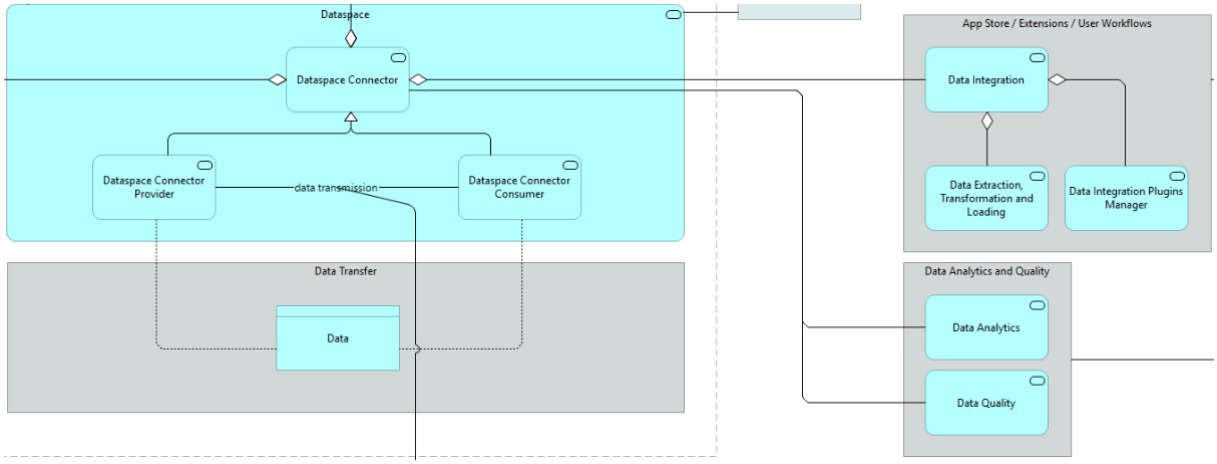

Figure 24 EIRA/eGovERA Business Agnostic Reference Architecture approach for data spaces. See Annex III to zoom on the different parts of the data space enabler

5 Conclusions

The proposition of an ETDS architecture faces technical challenges that the Consortium will continue tackling in the context of the use case development. A common agreement on a precise understanding of the final data product is paramount to enable the operationalisation and scalability of the ETDS. 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 the usable and secure process for sovereign data exchange. Those features consist of the following: onboarding of participants, 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 proposition of a high level architecture, based on EIRA/eGovERA Business Agnostic RA, allowed the Consortium to prioritise time investment: EIRA/eGovERA is aligned with the architecture principles adopted in SIMPL, and manage complexity during the early stage of the deployment.

When examining the available technological stack, the EDC and the SIMPL middleware emerge as the most relevant options. EDC offers a modular, standardised foundation for identity management, data transfer, and policy enforcement. In turn, SIMPL, some of its components building on EDC, adds more sophisticated capabilities, including dedicated onboarding and governance framework and integration with common federation services, which is ideal to fit future-specific requirements. 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.

Glossary

Term	Description
Business model	A description of the way an organisation creates, delivers, and captures value. Such a description typically includes for whom value is created (customer) and what the value proposition is. Typically, a tool called business model canvas is used to describe or design a business model, but alternatives that are 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 products' allowed purposes of use, quality and other requirements the data product fulfils, access and control rights, pricing and billing information, etc.
Data Product Offering	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, data delivery.
Dataset	A collection of data, published or curated by a single agent or identifiable community.
Data source	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	Interoperable framework, based on common governance principles, standards, practices and enabling services, that enables trusted data transactions between participants.

Term	Description
	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, 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.

Term	Description
	Explanatory Text: The data space governance framework specifies the data space functionalities and associated roles. Each functionality and associated role consist of 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. ● 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, data space building blocks, and recommended selection of standards, specifications and reference implementations identified in the data spaces technology landscape.
DSSC Asset	A sustainable open resource that is developed and governed by the Data Spaces Support Centre (DSSC). The assets can be used to develop, deploy and operationalise data spaces and to enable

Term	Description
	knowledge sharing around data spaces. The DSSC also develops and executes strategies to provide continuity for the main assets beyond the project funding.
Federated Data Spaces	A data space that enables seamless data transactions between the participants of multiple data spaces based on agreed common rules, typically set 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.
Final Data Product	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	A dataset, a data service or any other resource that may be described by a metadata record in a catalog.

Annexes

Annex I Comparative table of reference architecture and frameworks of EDTS

The rapid development of the European Data Strategy has given rise to multiple architectural frameworks and reference models designed 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, organizational, legal, and policy-driven—towards the realization 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 between these initiatives as they work towards implementing sustainable and future-proof data spaces in Europe.

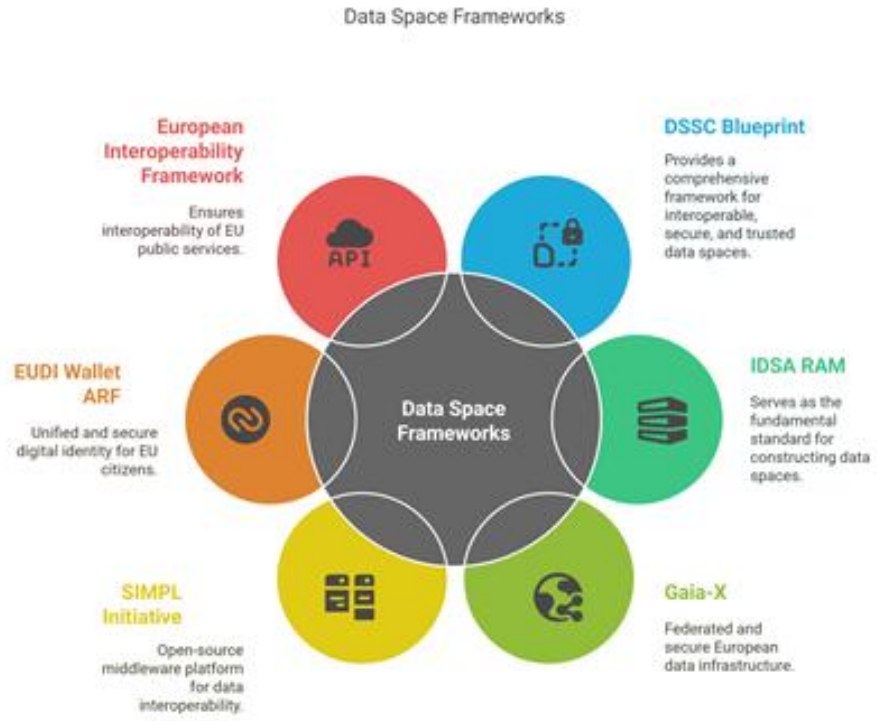

Figure 25 Data Space Frameworks according to the European Data Strategy

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 & organizational 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, organizational, semantic, and technical interoperability

Table 1 Comparative table of reference architectures and frameworks of EDTS

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.

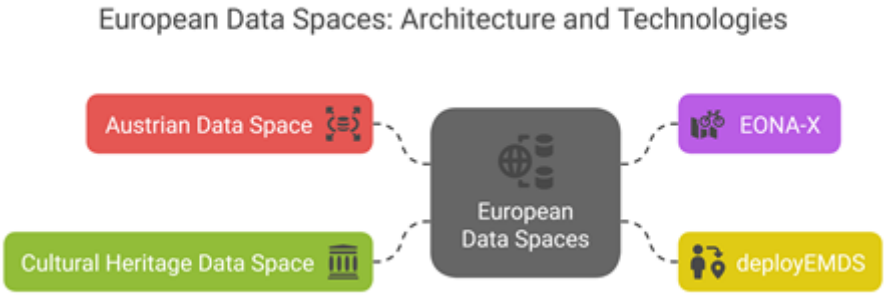

Figure 26 Data Space initiatives relevant to the ETDS

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	Decentralized 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, decentralized 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 Europeana platform; centralized metadata, distributed content	Focus on metadata quality, multilingualism, 3D contents, 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 at 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 organizations to combat fake news and misinformation.	TBD by TEMS	Data access, sharing and sovereignty that is compliance to the data protection legislation.	TBD by TEMS
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; uses 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	DSSC-based building block model; Gaia-X; future adaptation to IDSA RAM and EUDI Wallet;.	Data broker; Identity Management and Authorisation; Data API ();	W3C VC; XACML; ABAC, RBAC; JSON REST API; iSHARE;

	cities and communities.	The DS4SSCC architecture seeks to make the evolution of Smart Solutions/Data Platform to a dataspace, rather than creation of a dataspace from scratch.	Data Publication; Universal Trust Registry	i4Trust; DSP; DOME.

Table 2 Comparative analysis of data space initiatives related to ETDS

Annex III: EIRA/eGovERA Business Agnostic RA 6.1.0

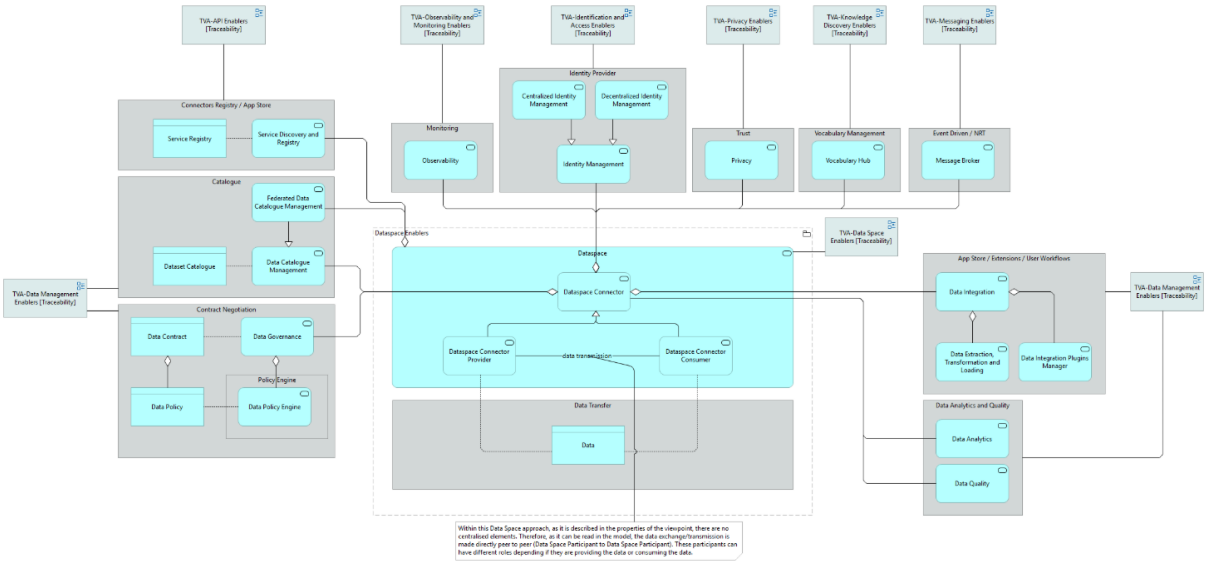

Figure 27 EIRA/eGovERA Business Agnostic RA 6.1.0