NIA Digital & AI Insights

#2
Korea's Data Space Initiative (K-Data Space)

NIA NATIONAL INFORMATION SOCIETY AGENCY

Table of Contents

Korea's Data Space Initiative
(K-Data Space)

01. Concept and Necessity of Data Space 5

02. Global Practices and Standardization 11

03. Korea's Data Space Initiative 45

04. Strategy for Advancing Korea's Data Spaces 57

Executive Summary

Data Space is a decentralized data sharing framework that ensures data sovereignty, interoperability, and trust-based exchange, emerging as an alternative to overcome the limitations of centralized platforms.

The EU is expanding data spaces across regional and industrial sectors, starting with publicly-led Common Data Spaces and through the Gaia-X initiative.

Governance and technical standards are being established to realize data sovereignty, interoperability, and trust-based exchange — including participant authentication, standard metadata, smart contract-based data exchange, and audit trail management.

Early outcomes of data spaces are being generated across public and private sectors within the EU, such as joint responses to climate change (Green Deal Data Space) and supply chain management optimization (Catena-X).

Japan is also establishing its own domestic data space model (Ouranos Ecosystem) and embarking on data innovation to respond to EU environmental regulations and expand its domestic data sharing ecosystem.

A reference model and key components for building a Korean version of Data Space have been derived by synthesizing overseas data space cases and standardization trends.

The model is structured across three layers: a Governance Layer encompassing data sovereignty assurance, consensus-based governance, federated frameworks, trust, and interoperability; a Business Layer covering use case-oriented domain design, participant registration, role and contract management, data access, and settlement and value creation mechanisms; and a Technical Layer comprising federated catalogs, identity management, policy and contract modules, clearing, and digital tokens.

A new data governance strategy is now needed — one that eliminates barriers to cross-sector data sharing that has been accumulated over time, and creates utilization-driven added value.

#2

Korea’s Data Space (K-Data Space)

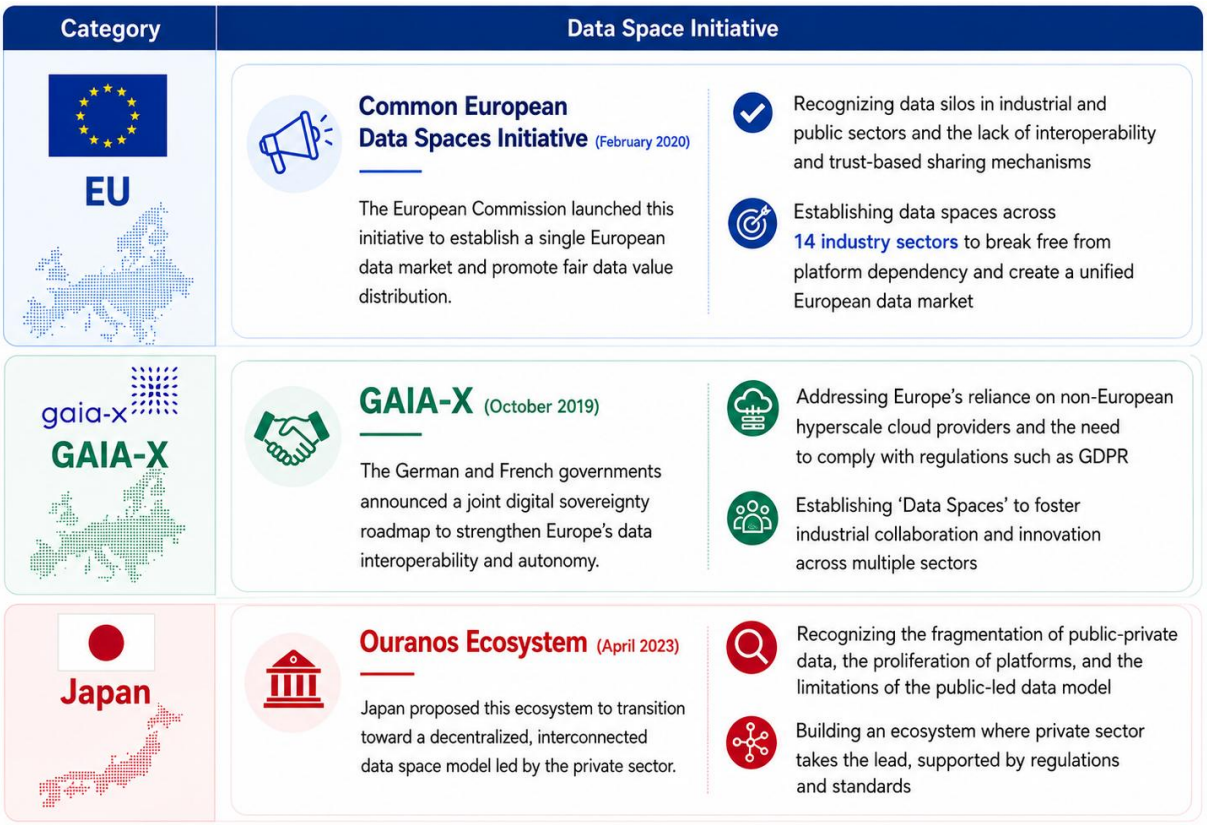
1. Concept and Necessity of Data Space

1.1 Concept of Data Space

Data Space is a framework designed to enable the safe distribution and transaction of data among various participants within a specific organization or country, built upon a policy-based and technical foundation of trust — through decentralized data sharing that guarantees data sovereignty, interoperability, and trust-based exchange.

Rather than relying on a centralized platform, the federation-based distributed structure allows participants to directly control their own data, and to configure and automatically enforce usage conditions, access rights, sharing history, and more through policy-based mechanisms (IDSA, Gaia-X, etc.)

[Global Data Space-Related Initiative]



1.2 Background and Necessity of Promoting Data Spaces

■ Laying the Technical Foundation to Secure Data Sovereignty

[Issues with Securing Data Sovereignty at the National and Individual Level]

National Level
Risk of Data Sovereignty Infringement
· The U.S. CLOUD Act allows U.S. government agencies (e.g., law enforcement) to access data stored on U.S. cloud companies' servers, even if the data belongs to another country. This has the potential to technically neutralize the data sovereignty of other nations
Efforts and Limitations in Establishing Norms
· The European Union[1](GDPR), Japan (DFFT initiative), and South Korea (Personal Information Protection Act, etc.) are promoting cross-border data controls and the establishment of international norms. However, most of these efforts remain at the level of legal declarations or policy measures (John G. Dale et al., 2024 / Son Hyeong-seop, 2025)
Limitations in Technical Control
· In centralized overseas cloud environments, data is stored on foreign servers, making practical protection under domestic laws and policies difficult and weakening control at the national level
Individual Level
Lack of Individual Control
· Institutionally (e.g., via the Personal Information Protection Act), individuals are guaranteed the right to access, delete, and transfer their data. In reality, however, the structure allows service providers (platforms, cloud companies) to dictate the conditions for data utilization · There is a need for the widespread adoption of technical means that allow individuals to directly control the scope of their data's use, whether it is provided to third parties, and its storage location

[1] https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers_en?utm_source

[Application of Technologies to Secure Data Sovereignty via Data Spaces]

· To secure practical data sovereignty, a structure where the data provider can technically control the entire data utilization process is essential. This necessitates the introduction of "**Data Spaces**" to enable such control

① **Granular Access Control and Policy-Based Automated Enforcement**
Data owners can specify and automatically enforce "who" can access the data, "when," and "under what conditions"

② **Transparent Tracking and Auditing of Data Usage History (Log & Traceability)**
Enables the management of a history detailing when, for what purpose, and by whom the data was utilized

③ **Linkage with Usage-Based Compensation Systems**
Allows for the design of a structure where compensation is delivered to the provider based on data usage history and contracts

④ **Legal and Regulatory Compliance Verification**
Supports the automatic verification of the regulatory frameworks of relevant countries and institutions throughout the entire data utilization process

⑤ **Implementation of a Decentralized Data Processing and Utilization System within a Federated Data Ecosystem**

Technically controls access and utilization according to predefined policies, allowing consumers to utilize only the processed results within their local environments

■ Strengthening Data-Driven Industrial Competitiveness through Interoperability and Reliability

The increasing demand for high-quality industrial data to support AI Transformation (AX) has exposed structural limitations in current data ecosystems. Fragmented data formats, poor interoperability, and isolated data silos hinder efficient data utilization, while concerns over confidentiality, data sovereignty, and the inability to transparently manage data access and usage continue to discourage organizations from sharing data across institutional and industrial boundaries.

[Issues with Current Industrial Data Distribution and Utilization]

Poor Data Interoperability

- While securing high-quality, specialized data is essential to driving AI Transformation (AX) across various fields such as manufacturing, robotics, and healthcare, actual industrial sites face inconsistent data formats and structures. This results in significant time and costs being spent on refining and standardizing data
- Consequently, the “data silo” phenomenon-where data accumulates in isolation across departments, organizations, and industries-is intensifying, and interoperability required for integrating heterogeneous data or utilizing it in AI models is compromised

Concerns Over Industrial Data Leakage

- Sharing and utilizing data require procedures such as combination, processing, cleansing, anonymization, and pseudonymization. During these processes, concerns arise regarding the external exposure of sensitive information or corporate secrets
- In particular, because the structure makes it difficult to track who accesses the data, its purpose of use, and its distribution history once it has been provided, many companies experience an amplified psychological resistance to data sharing

Data spaces provide a strategic foundation for overcoming fragmented data ecosystems by combining interoperability, trusted governance, and provider-controlled data sharing. Through automated data standardization, policy-based access control, and secure exchange of verified data, they enable organizations to collaborate without relinquishing data sovereignty. This trusted data ecosystem supports the large-scale utilization of industry-specific data, laying the foundation for Vertical AI development and accelerating AI Transformation (AX) across the industrial sector.

[Ensuring Interoperability and Reliability Through Data Spaces]

- The adoption of data spaces is necessary to enable trust-based integration through secure data sharing, control, and automated standardization

① **Automatic Standardization of Heterogeneous Data and Securing Interoperability**

Based on technologies such as AAS(Asset Administration Shell) and data harmonization, this system automatically aligns data of different formats into an agreed-upon common standard, thereby reducing the time and cost required for standardization and enhancing interoperability

② **Granting Provider-Centric Control over Data Sharing**

It provides a structure where data providers can decide whether to approve or reject cross-industry linkage requests and specify data usage conditions in advance, allowing them to maintain control over their data even after it has been shared

③ **Establishing a secure exchange system limited to verified data**

Only data that has undergone technical verification is shared and utilized; distribution is limited to data that meets security and quality standards, thereby minimizing the risk of sensitive information exposure

④ **Expanding Vertical AI and Creating a Foundation for Industry-Wide AX Innovation**

Establishing a data ecosystem that supports the training of advanced AI models by aggregating and linking industry-specific data, and promotes AI-driven business innovation (AX)

■ Securing Federated Governance through Consensus-Based Rules and Autonomous Operation

[Limitations of Existing Centralized Platforms]

Rigid Operational Standards and Rules
· In centralized data platforms, a central institution unilaterally sets and manages various standards and rules, including data formats, access procedures, the scope of data openness, quality standards, and personal information processing rules
· Since providers must unilaterally comply with the standards and rules set by the central authority or platform, it is difficult to reflect industry-specific needs and respond flexibly to new technologies and policy changes

Lack of Incentives for Participation

- Data providers not only find it difficult to participate in the design process for standards and rules but must also bear legal and security risks, thereby weakening their motivation to share and utilize data and participate in the ecosystem

[Centralized ⇨ Federated Structure, Securing Participant-Centric Flexible Governance]

- It is necessary to overcome the limitations of existing rigid data policies, operational structure, and centralized platforms by **building Data Spaces with a federated governance structure** that operates autonomously based on participant consensus and ensures interoperability

① **Establishing a Purpose-Based Collaboration Structure through Federated Governance**

Data Spaces support purpose-driven, autonomous data collaboration by forming a federation comprising various stakeholders, such as data providers, consumers, platform operators, and technology developers

To achieve this, participants collaboratively define and execute policies, operational rules, transaction terms, and access rights within the Data Space. This allows the data ecosystem to operate based on flexible, mutually agreed-upon norms rather than rigid external regulations

② **Consensus-based Establishment of Common Standards and Contractual Rules**

By independently establishing and managing core elements for data exchange within the space, such as data standardization, sharing/trading protocols, and technical integration methods, it secures practical interoperability and a trust-based trading structure among participants

③ **Creating an Open and Fair Data Ecosystem**

Data Spaces are designed based on a decentralized structure where various participants share equal rights and responsibilities, rather than depending on a specific company or platform. This overcomes closed monopolistic structures and realizes a fair and open governance system

2. Global Practices and Standardization

2.1 EU Common Data Spaces

EU Common Data Spaces were launched (February 2020) to strengthen data sovereignty within Europe and facilitate secure data sharing and utilization across industries. They are strategically based on A European Strategy for Data and legally grounded in the Data Governance Act (DGA) and the Data Act

[Core Pillars of the EU Common Data Space[2]]

Category	Key Components	Description
Business	Business Model	Designing the business model and operational structure of the data space
	Use Case Development	Discovering and disseminating practical use cases for value creation
	Data Product Development	Defining data product templates, establishing provisioning policies, and building network effects
	Intermediaries	Defining the role of data intermediaries and supporting governance decisions
Governance	Regulatory Compliance	Establishing a governance framework to ensure compliance with EU regulations
	Contractual Framework	Laying a contractual foundation that defines the rights and obligations among participants
Technology	Data Models	Managing common semantic frameworks(ontology) and metadata(vocabulary)
	Data Exchange	Providing standards-based APIs and data exchange tools
	Provenance & Traceability	Mechanisms for tracking data transaction history and providing proof
	Access & Usage Policies	Defining policy-based access and usage conditions (Policy as Code)
	Identity Management	Supporting participant identification and authentication systems (e.g., VC, DID) and onboarding

[2] https://dssc.eu/space/BVE2/1071252426/Building+Block+Overview

- **Multi-layered Operational Structure**: Overseen by the European Commission, operated by public-private consortiums for each data space, and supported in implementation by technology alliances such as Gaia-X and the Data Spaces Support Centre (DSSC)
- **Current Scope:** The EU is currently establishing a total of 72 data spaces* across 14 domains: health, agriculture, manufacturing, energy, mobility, finance, public administration, media, cultural heritage, language, research, tourism, the Green Deal, and skills

The EU Common Data Space proposes a minimum of three Key Technical Standards[3] and specifications that data spaces must comply with to secure interoperability

① Verifiable Credentials, VC

- A specification developed by the W3C that supports the creation, sharing, and verification of digital credentials
- Enables the confirmation of authenticity and integrity, along with tamper resistance and cryptographic verification, without relying on a central authority
- Defines the methods for issuing, storing, and presenting credentials to ensure they can be verified by all involved parties

- Various protocols for the issuance and verification of Verifiable Credentials are under development. Currently, OpenID4VC and W3C DCP (Decentralized Messaging Protocol) are cited as primary examples
- OpenID4VC is a protocol being standardized by the OpenID Foundation, encompassing VC Issuance (OID4VCI), VC Presentation (OID4VP), and Self-Issued OpenID Provider (SIOPv2), which is managed directly by the user
- This protocol is integrated with the EU's EUDI Wallet architecture and the eIDAS 2.0 framework, with plans to support all EU citizens and legal entities in securely storing their digital identities in the EUDI Wallet by 2026

[3] https://dssc.eu/space/BVE2/1071254873/Building+on+Top+of+Foundational+Technical+Standards

② **DCAT(Data Catalog Vocabulary) v3**

- It enables organizations to describe datasets consistently, making it easier for users to find and use the data they need. It is designed to be extensible, allowing organizations to add their own properties and classes to meet specific requirements
- The DCAT vocabulary includes classes and properties that describe datasets and their relationships. It creates rich metadata that can be used for effective indexing and searching, and it supports data integration, analysis, and reuse across various platforms and domains

③ **Open Digital Rights Language(ODRL)**

· A policy expression language developed by the W3C that allows for the specification of permissions, prohibitions, and duties related to digital assets. It is an essential tool for digital rights and license management, and it is used to express access and usage policies for datasets within data spaces

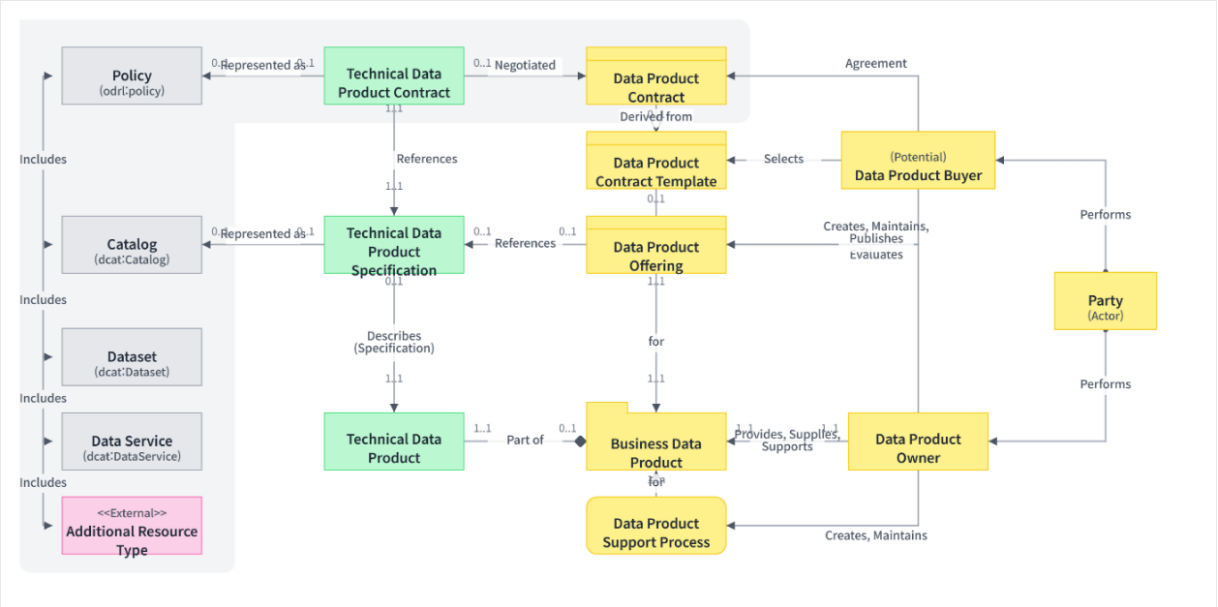
· It includes permissions (allowed actions), prohibitions (forbidden actions), and duties (actions that must be performed). It can also incorporate constraints, such as time or location restrictions, as well as duties like fees that must be paid to exercise a specific right

The IDSA has developed the Dataspace Protocol, which defines the methods for distributing datasets as DCAT catalogs, establishing ODRL-based usage control policies, electronically negotiating data usage contracts, and accessing data through transfer protocols

* Note: This protocol only specifies the common elements; the actual APIs for data exchange are implemented differently for each specific data space

The EU has developed the Data Spaces Conceptual Mode l(via the DSSC) to provide guidelines for the configuration and operation of sector-specific data spaces

① Conceptual Model for Data Product Registration and Provisioning



* (Source) DSSC, Data Spaces Blueprint v1.0, Conceptual Model - Data Products and Offerings

[Conceptual Model of Data Products and Offerings]

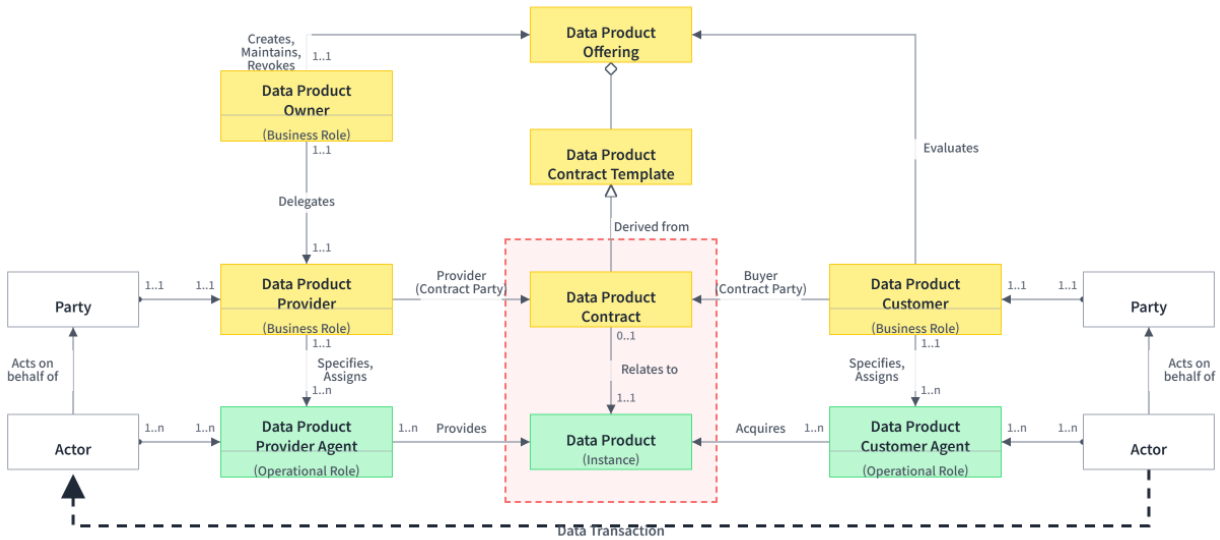
Data products are classified into Technical Data Products (TDP) and Business Data Products (BDP), which encompass the former. A Technical Data Product includes the **actual datasets, data services, and derived resources** provided, and is defined through a DCAT-based **Metadata Catalog**

This catalog includes not only the structural definitions for each data resource but also ODRL-based policies (Usage Policies, Access Policies) that define access control and conditions of use. This enables data providers to automatically evaluate and provision data according to the service conditions

A Business Data Product is a structure that adds operational processes—such as customer support, claims processing, and provisioning procedures—on top of the technical product. Based on this, the data product owner configures Data Product Offerings, which include various Service Levels, Pricing Models, and terms of use

A data offering is linked to one or more Smart Contract Templates. Using these templates, customers can proceed with contract negotiation and execution, thereby enabling the integration of data provisioning and legal contracts within the Data Space

② Conceptual Model of Data Product Transactions

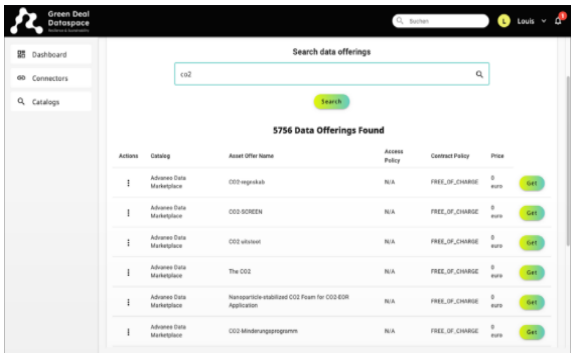


* (Source) DSSC, Data Spaces Blueprint v1.0, Conceptual Model - Data Transactions

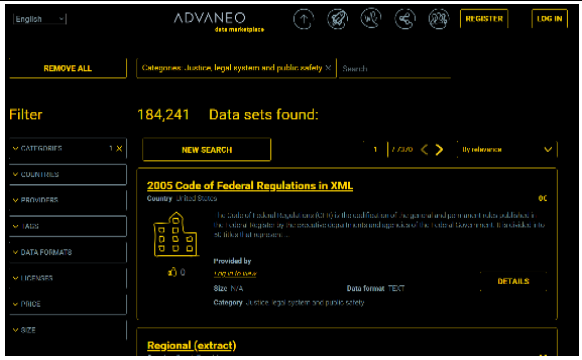
[Conceptual Model for Data Transaction]

- The EU DSSC's conceptual model for data transactions defines the exchange of data products not merely as a simple technical transfer, but as a process founded on a contract-driven trust structure and technical infrastructure
- In this model, a data transaction begins with a contract negotiation between a 'Data Product Customer' and a 'Data Product Provider.' This negotiation is based on one of several predefined data product contract templates. Once the contract is concluded, both parties enter into a legally binding contractual relationship and simultaneously designate an 'Agent' as the technical execution entity
- Technically, these agents are primarily implemented as Data Space Connectors, which execute functions such as the actual data transfer, access control, policy enforcement, and catalog referencing
- The connector utilizes a DCAT-based metadata catalog to provide structural descriptions of the data product. It codifies access rights and usage conditions using an ODRL-based policy language (Policy as Code). Furthermore, built-in mechanisms for Traceability and Provenance are included to track data usage history and policy compliance, thereby ensuring transaction transparency and accountability
- Specifically, the data product provider pre-configures and deploys various settings (such as policies, catalog links, and data endpoints) to this technical agent. The customer-side agent then receives and utilizes the data in the technically contracted manner according to these settings. This effectively implements the contract-policy-technology linkage structure of data transactions, enabling automated contract execution and policy-based control within the Data Space

- **(Overview)** The Green Deal Data Space (GDDS) is a common data space that integrates various industrial, public, and citizen data in high quality and makes it available in an interoperable manner to support the EU's Green Deal priorities (e.g., climate change response, circular economy, biodiversity, zero pollution)



Green Deal Data Space Portal[4]



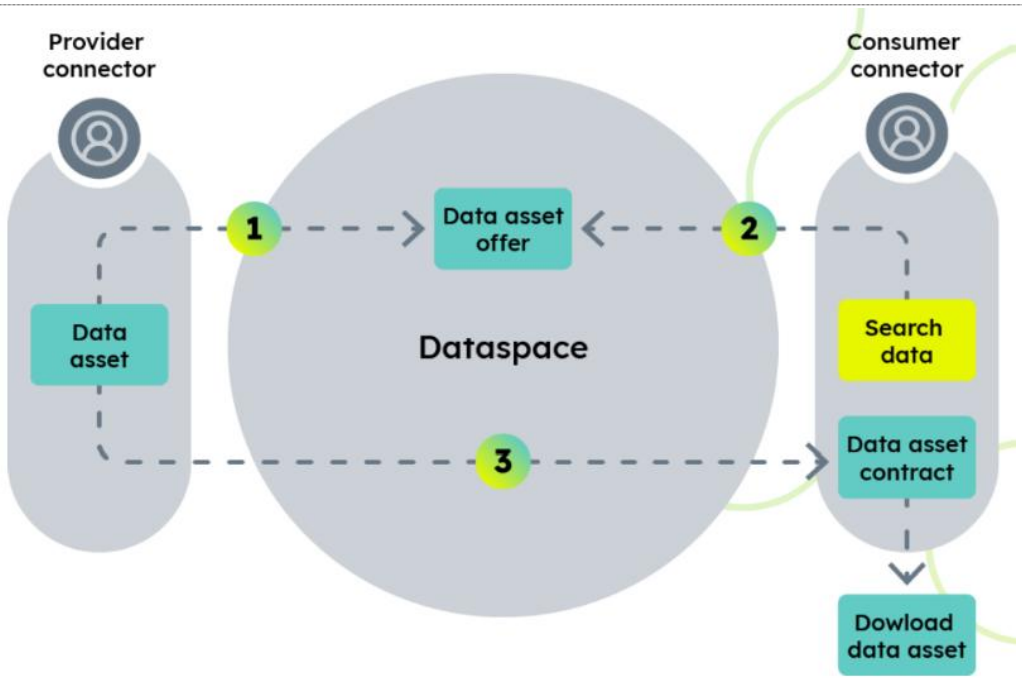
Green Deal Data Space Marketplace[5]

- **(Key Activities)** Demonstrating and scaling use cases of data spaces in the Green Deal sector through Lighthouse Projects, R&D projects, and more
- **(Lighthouse Projects)** Presenting data space demonstrations and success models in specific industrial domains
  - (Supply Chain Radar) Providing data infrastructure support for supply chain management AI within the PAIRS project, which develops an AI-based solution to predict corporate crisis situations
- **(R&D Projects)** Projects designed to support the execution and market launch of data-driven innovations
  - (CIRCMAN 5.0) Enhancing product modeling and simulation pipelines and assessing environmental sustainability in the manufacturing of photovoltaic (PV) products
  - (SPELL) Providing artificial intelligence-based decision support to execute crisis prevention, emergency assistance, and response measures—such as for natural disasters and large-scale blackouts—more rapidly and accurately

[4] https://www.advaneo-datamarketplace.de

[5] https://www.advaneo-datamarketplace.de

- **(Main Data)** Integration and sharing of environment and climate-centric data provided by EU institutions, member state public agencies, research institutes, private companies, and civil society
- **(GDDS Data Transaction Procedures)** A transaction structure where a data provider registers data with specified conditions, and once a user discovers it and agrees to those conditions, the data is securely transferred based on principles of security and transparency



Category	Key Details
Data Provider Listing	• Defines data assets and creates transaction conditions for the data provider's dataset
Data Consumer Purchase Request	• The data consumer searches through the data catalog, reviews the transaction conditions, and accepts them (Smart Contract)
Data Asset Transfer and Usage	• Once the conditions are met, the data provider transfers the data to the data consumer (Connector)

2.2 Gaia-X Data Space

■ Overview of Gaia-X

- **(Purpose of Launch)** A project launched in 2020, spearheaded by the EU, Germany, and France, aimed at securing data sovereignty within Europe and creating an federated, trust-based data infrastructure ecosystem
  - ✓ This can be seen as a strategic attempt to reduce dependence on the cloud and data markets dominated by transnational big tech companies from the US and China, and to establish Europe's own data value chain
- **(Objectives)** Rather than aiming to build a single centralized platform, the goal is to provide a technical foundation based on a federated structure. This allows various data providers and consumers to share data in a trustworthy manner through data spaces and maintain control over their own data
- **(Gaia-X Framework)** Operates standards such as common technical architectures and operational policies, along with programs to discover best practices, to ensure that data spaces can operate in a manner equipped with federation and trust[6]

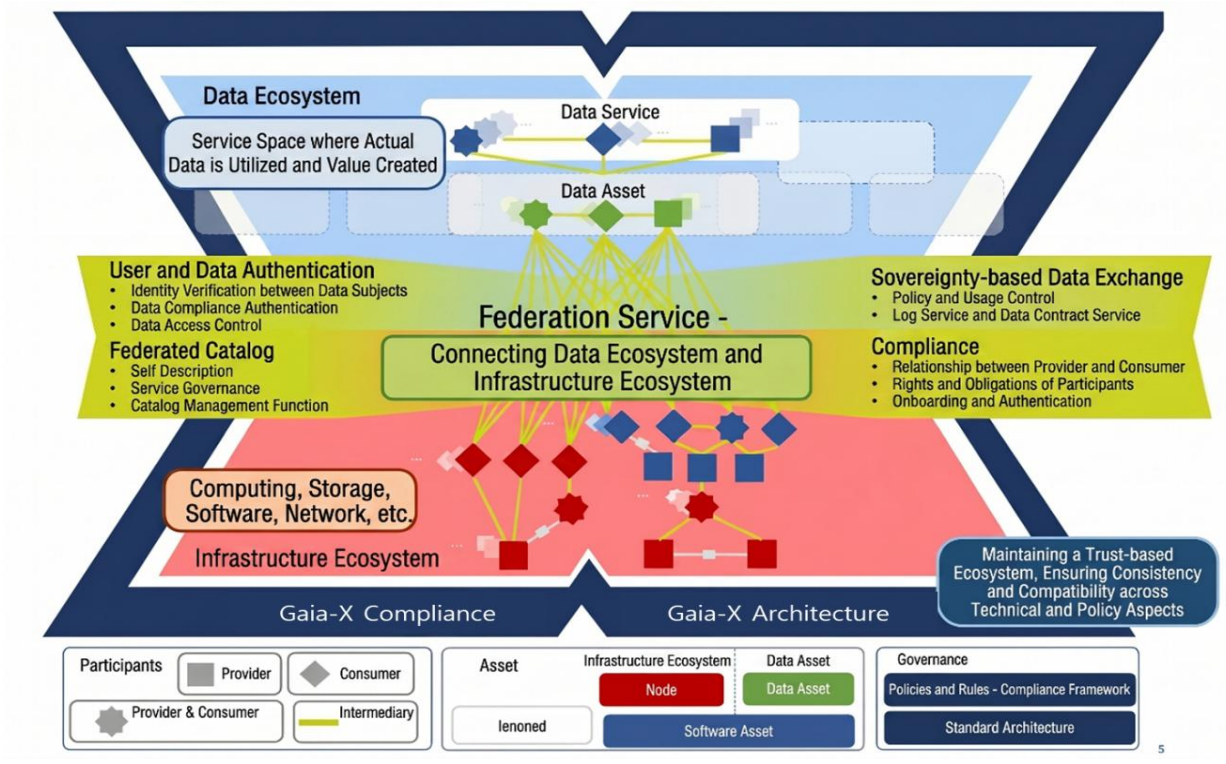
[Gaia-X Framework]

Category	Component	Key Details
Technical Standards & Requirements	Gaia-X Architecture Document	· Defines the technical structure and design principles for implementing data spaces
	Data Exchange Document	· Defines interoperable data exchange procedures and format standards between data providers and consumers
	Access Management Document	· Policies and standards for identity and access management, such as participant authentication and permission settings

[6] https://docs.gaia-x.eu/#/framework

	Ontology	· Defines common concepts and semantic systems to enable meaning-based(semantic) linkages between data
	Reference Toolkit	· A set of tools that supports data space participants in verifying technical compatibility and implementation
Compliance	Gaia-X Label Criteria (Level 1~3)	· Evaluates and specifies by tier that data and services are trustworthy and compliant with policies
	Digital Clearing House (GXDCH)	· A core trust infrastructure that monitors and verifies data usage history, access rights, and policy violations in real-time
Certification Program	Outstanding Data Space Certification Program	· Designates excellent data space implementation cases, providing criteria to verify scalability and technical/policy feasibility

* (Source) Reconstructed based on the Gaia-X Framework



[Gaia-X Federated Data Infrastructure Ecosystem]

* (Source) Reconstructed based on the Gaia-X Architecture Document

[Gaia-X Ecosystem Common Components]

Area	Key Components	Key Details
Data Ecosystem	Smart Services, Data Spaces	· A service space that creates added value using actual data, where higher-layer data-driven services operate
Federation Services	Federated Identity Management, Trust and Access Management	· Secures trust for data sovereignty-based operations, such as authenticating data subjects and participants, setting trust levels, and establishing an integrated authentication system
	Federated Catalog (Self-Description, Service Governance, Catalog Management Functions)	· A catalog based on Self-Descriptions that detail participants' assets (data, services, etc.). Supports mutual search and linkage
	Sovereign Data Exchange (Policy & Usage Condition Setup, Logging & Data Contract Management)	· Defines policies for sovereign data exchange, sets usage conditions, logs history, and provides contract services
	Compliance (Defining Rights&Obligations between Providers /Consumers, Certification & Onboarding)	· Defines and verifies responsibilities, obligations, and rights among participants. Certifies compliance within the ecosystem and provides onboarding procedures
Infrastructure Ecosystem	Compute, Storage, Network, Software Assets (Node, Software Asset, etc.)	· Physical and virtualized computing resources and the network/storage-based infrastructure components that connect them
Governance	Gaia-X Policy Rules, Gaia-X Architecture	· Defines the technical and policy operational principles and the standard structure of the data space

■ Gaia-X Data Spaces

- **(Overview)** Gaia-X supports the demonstration of Lighthouse Data Spaces that meet Gaia-X standards at the technical, operational, and security levels through its Lighthouse projects
- **(Operational Status)** As of July 2025, a total of 28 data space demonstrations are underway across various sectors, including agriculture, manufacturing, and construction
  - ✓ Based on their level of compliance with Gaia-X criteria, they are categorized into 3 Qualified Projects, 21 Lighthouse Projects, and 4 Lighthouse Data Spaces

[Key Gaia-X Data Spaces[7]]

Category	Field	Data Space	Key Participating Companies	Overview
Lighthouse Data Space	Automotive	Catena-X	BMW, Mercedes-Benz, SAP, Siemens, Fraunhofer	Standardized data ecosystem for the entire automotive supply chain, from OEMs to suppliers
	Aerospace	COOPERANTS	AIRBUS, DLR, Fraunhofer, neusta	Heterogeneous data sharing across systems and smart service operations in the aerospace sector
Lighthouse Projects	Manufacturing	EuProGigant	deltaDAO, CONCIRCLE, HELLER, eit Manufacturing	Austro-German joint project aimed at preventing accidents in manufacturing companies

[7] https://gaia-x.eu/community/lighthouse-projects/

	Agriculture	AgrospAI	I+Porc, FEMAC, GrupoTragsa, TEF	Agri-food demonstration project linked with the Common European Agricultural Data Space (CEADS)
Qualified Projects	Cloud	FAIR Data Spaces	Fraunhofer, National Research Data Infrastructure	Cloud-based data space for sharing research data between industry and academia
	Construction	DigitalTER-X	Cerema, DAWEX, egis, eurostep	Creation of a sustainable data sharing environment across the built environment

※ Reconstructed based on the Gaia-X Lighthouse projects list

『Catena-X』 is presented as a representative data space case within Gaia-X, implementing data interoperability and trust-based collaboration across the entire value chain of the automotive industry

[Overview of Catena-X]

- **(Overview)** An automotive industry-specific data space centered in Germany, establishing a transparent and trustworthy data exchange system across the entire automotive production value chain
- **(Participating Entities)** Manufacturers, suppliers, and research institutions including BMW, Mercedes-Benz, Volkswagen, ZF Friedrichshafen, Robert Bosch GmbH, SAP, Siemens, T-Systems, Fraunhofer Institute, German Aerospace Center(DLR), etc.
- **(Key Functions)** Contributes to ESG response and supply chain management advancement within the automotive industry

Function Area	Key Details
Carbon Footprint Tracking	. Calculates and tracks carbon emissions per product at the battery and component level

Battery Passport	· Issues a digital ID containing battery production history, usage conditions, recycling information, etc.
Supply Chain Risk Analysis	· Automatic detection and monitoring of risks for specific suppliers or regions within the supply chain
Component Traceability	· Manages the lifecycle history from production to installation and disposal of specific components within a vehicle(Digital Twin-based)

- **(Operating Organization)** Operating committees and expert groups are active to expand the Catena-X network and achieve common goals

[Catena-X Thematic Committees and Expert Groups][8]

Committee/Group	Key Role
Architecture Management	· Designs the architecture to ensure Catena-X strategies and goals are realized as actual technology
Data Space Operations Committee	· Refines operating methods and establishes criteria for releasing and deploying new versions for efficient management
Ecosystem Activation Committee	· Coordinates regional hubs and drives strategies to expand overseas users
Industry Core Committee	· Creates core components and broadens the use of standards for application in other industries
Internationalization Committee	· Promotes global expansion by establishing hubs in key locations like North America, Spain, and China
Network Services Committee	· Establishes plans for developing common services such as member registration, data search, and identity management
Sustainability Committee	· Manages standards, roadmaps, and cooperation for implementing Product Carbon Footprints (PCF) and Digital Product Passports (DPP)

[8] https://catena-x.net/association/expert-groups-committees/

Supply Chain & Quality Committee	· Formulates joint strategies to improve supply chain quality and enhance crisis response capabilities
Technical Committee for Modelling	· Conducts quality checks on data models before their adoption as international standards
Technical Committee for Standardization	· Reviews candidates and manages technical procedures when creating new standards

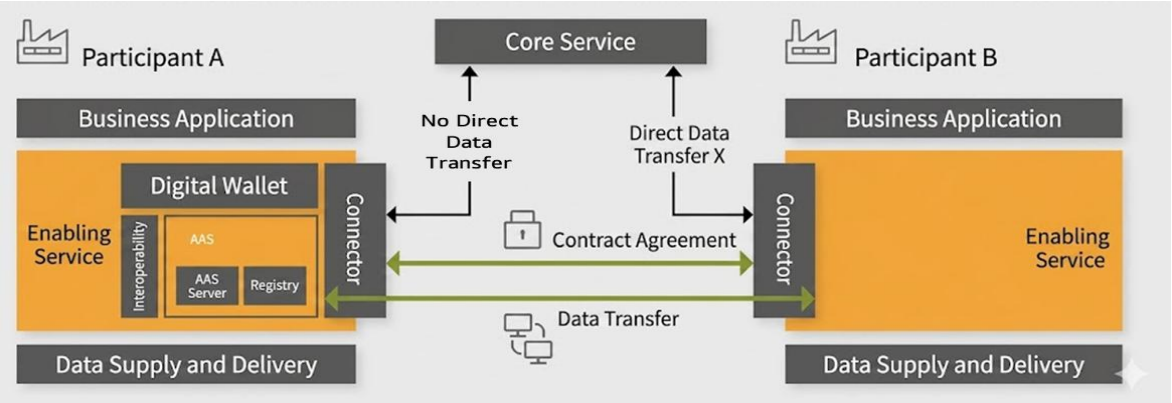
- **(Catena-X Standards)** A technical and policy standard framework designed to implement data interoperability and trust-based data exchange within the automotive industry, based on Gaia-X and IDS (International Data Spaces) principles

[Key Catena-X Standards[9]]

Category	Standard Name/Technology	Role & Description
Data Modeling	AAS (Asset Administration Shell)	A metadata structure that represents industrial data in the form of a digital twin
Identity & Trust Management	VC (Verifiable Credentials)	A verifiable representation of participant trust information and asset authentication information
Data Exchange & Policy	Usage Policy	Specifies data usage conditions, contract terms, retention periods, etc., in a machine-readable format
	Smart Contract	A contract mechanism that automatically executes conditions, costs, and durations during data exchange
Connection / Integration Tech	Dataspace Connector	A standard interface for secure communication between data providers and consumers
Certification & Compliance	Catena-X Compliance Gaia-X Labelling Criteria	Technical and policy compliance criteria for participating in the Catena-X ecosystem

[9] https://catena-x.net/association/standardization/

[Catena-X Data Space Data Flow]



No.	Step	Description	Related Components
①	Identity Identification & Trust Verification	Verifies the participant's identity based on DID and validates the trust level through certificates or VCs	Identity Wallet
②	Asset Metadata Registration	Structures assets (products, components, etc.) into AAS-based digital representations and registers them in the registry	AAS, AAS Server, Registry
③	Data Provision Preparation	Performs internal system data provisioning (cleansing, formatting, etc.) to enable actual data provision	Data Provisioning
④	Catalog Search & Connection Request	Searches for the counterpart's data offering in the Federated Catalogue and requests a connection	EDC (Connector)
⑤	Policy Negotiation & Contract Execution	Negotiates and concludes usage conditions, purposes, access restrictions, etc.	Smart Contract
⑥	Data Transfer Execution	Securely transmits and receives actual data according to contract terms (using secure protocols like TLS)	Data Transfer (EDC ↔ EDC)
⑦	Application Integration & Utilization	The data received by the consumer is linked to Enablement Services and business applications for utilization	Enablement Services, Business Applications

* (Source) Reconstructed based on Catena-X Standards: Framework of Data Exchange

■ Gaia-X Digital Clearing House

The Gaia-X Digital Clearing House (GXDCH) is a platform that monitors and verifies the reliability of transactions and adherence to common compliance within data spaces

[Operational Status of Gaia-X Digital Clearing House (GXDCH)[10]]

Company Name	Country	Overview
Aire Networks	Spain	· Provides telecommunications infrastructure and cloud solutions · Operating a GXDCH instance in the Spanish hub
ARSYS	Spain	· ·Specializes in web hosting and cloud services · Provides a GXDCH instance in Spain
ARUBA	Italy	· Italy's largest cloud infrastructure provider · Established the initial GXDCH in Italy
deltaDAO	Germany	· Develops open-source and decentralized data infrastructure · Provides a Web3/decentralized GXDCH environment
Neusta	Germany	· Digital transformation consulting and IT services company · Serves as the official GXDCH node for the German technology hub
OVHcloud	France	· Europe's leading hyperscale cloud company · France-based GXDCH provider
Pfalzkom	Germany	· Provides data center and network infrastructure · Operates as a regional-based GXDCH node
Proximus	Belgium	· Belgium's leading telecommunications company, actively investing in digital transformation · Established and began operating the first GXDCH in Belgium
T-Systems	Germany	· A global IT services company affiliated with Deutsche Telekom, leading the design and execution of Gaia-X infrastructure

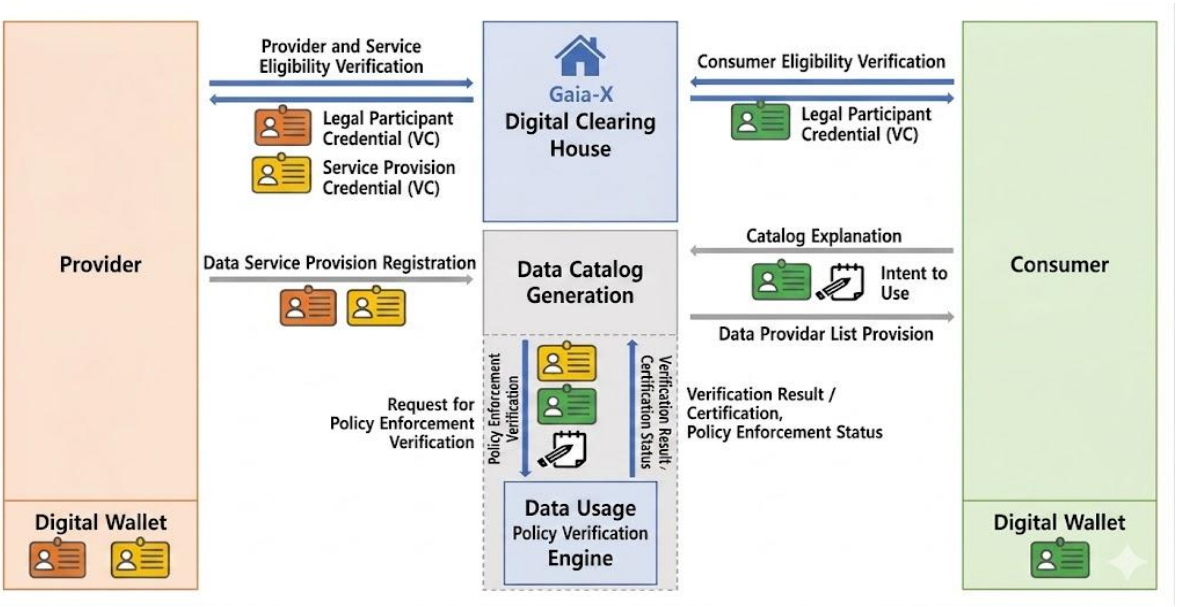
[10] https://gaia-x.eu/services-deliverables/digital-clearing-house/

[Key Services of the Gaia-X Digital Clearing House (GXDCH)]

Category	Component	Description
Mandatory (Free)	Gaia-X Compliance Service	· Issues Verifiable Credentials (VC) after confirming compliance status
	Gaia-X Registry	· Manages the list of trusted credential issuers (Trust Anchors)
	Gaia-X Notarization Service	· Validates corporate identity prior to issuing VCs
	Credential Event Service	· Provides distributed storage and synchronization of credentials (VC)
	IPFS Node	· Decentralized file system nodes that connect · GXDCH instances
	Logging Service	· Provides service record management functions to coordinators(federators)
Optional (Paid)	Wizard / User Interface (UI)	· GUI-based tools for creating and deploying VCs
	Catalog	· Acts as a federated catalog filter for discovering · related services
	Digital Wallet	· A digital wallet for securely storing and managing VCs
	Key Management System (KMS)	· Provides key lifecycle management for customers' cryptographic materials
	Policy Decision Point (PDP)	· Derives conclusions calculated based on multiple policies and input data
	Data Exchange Service	· Provides supplementary data exchange functionalities

* (Source) Gaia-X Digital Clearing Houses (GXDCH): Gatekeeper of the data economy

[Gaia-X Digital Clearing House Operational Model]



[GXDCH ↔ Data Space Data Flow]

Step	Entity	Core Activity	Component
1	Data Space Data Provider	(Credential Issuance) Obtains Verifiable Credentials (VC) for data provision and legal entity status	Digital Wallet Verifiable Credential (VC)
2	Data Provider → Clearing House	(Data Registration & Verification) Requests verification to confirm if the registered data meets Gaia-X compliance standards	Clearing House
3	Data Space Data Buyer	(Submission of Intent to Use) Registers and submits the desired data usage purpose and conditions to the Wallet	Digital Wallet
4	Clearing House	(Policy Compliance Judgment) Automatically verifies whether the buyer's conditions are compatible with the provider's policies	Usage Policy Verification Engine
5	Clearing House → Data Catalog	(Service Search Based on Conditions) Selects data providers from the catalog that match the purpose of use	Data Catalog Metadata Broker
6	Data Catalog → Buyer	(Provision of Search Results) Delivers a list of providers satisfying the policy conditions to the consumer	Data Catalog
7	Clearing House	(Identifier Generation & History Management) Saves contract execution and data transfer history; tracks policy implementation based on smart contract conditions	Smart Contract, DID Registry Digital Token

2.3 Japan’s Ouranos Ecosystem

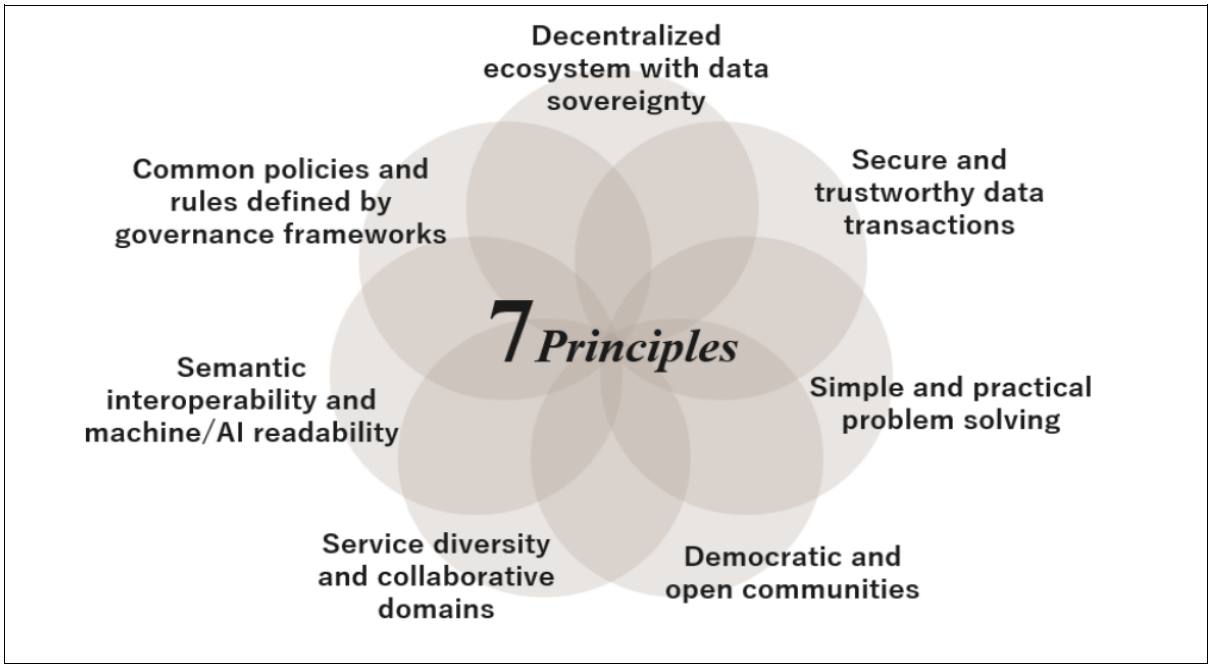
■ Overview and Core Principles of the Ouranos Ecosystem

With the goal of ensuring Data Free Flow with Trust (DFFT) and forming a common paradigm for cross-domain data interoperability, industry, academia, and government collaboratively developed and promoted the "Ouranos Ecosystem Initiative" in 2023, led by Japan's Ministry of Economy, Trade and Industry (METI)

While the Japanese manufacturing sector has seen improvements amid growing pressure for Digital Transformation (DX), industry-wide optimization and data sharing/collaboration across the entire value chain remained insufficient, prompting the pursuit of the Ouranos Ecosystem concept[11]

By enhancing data interoperability across industries, companies, and national borders, the initiative aims to resolve social challenges in Japan—such as labor shortages, climate change, and disaster response—and to accelerate industry-wide digital transformation (DX) while strengthening supply chain competitiveness, particularly in the manufacturing sector[12]

[Core Principles of the Ouranos Ecosystem Data Space]



11 White Paper on Manufacturing Industries 2024 Summary

12 https://www.meti.go.jp/english/policy/mono_info_service/connected_industries/ouranos.html

Principle	Key Details
① Ensuring Data Sovereignty	· A decentralized ecosystem where providers can lead data utilization and business
② Common Policies & Rules	· Clear operational standards through a multi-layered governance framework
③ Trust-based Transactions	· Secure data utilization based on security by design
④ Interoperability & AI Readability	· Securing semantic compatibility and AI usability through schema flexibility
⑤ Service Diversity	· Allowing open services that encompass both existing and new services
⑥ Democratic Community	· Operating an open community with free participation and withdrawal
⑦ Practical Problem Solving	· Emphasizing social value creation, as well as scalable simplicity and practicality

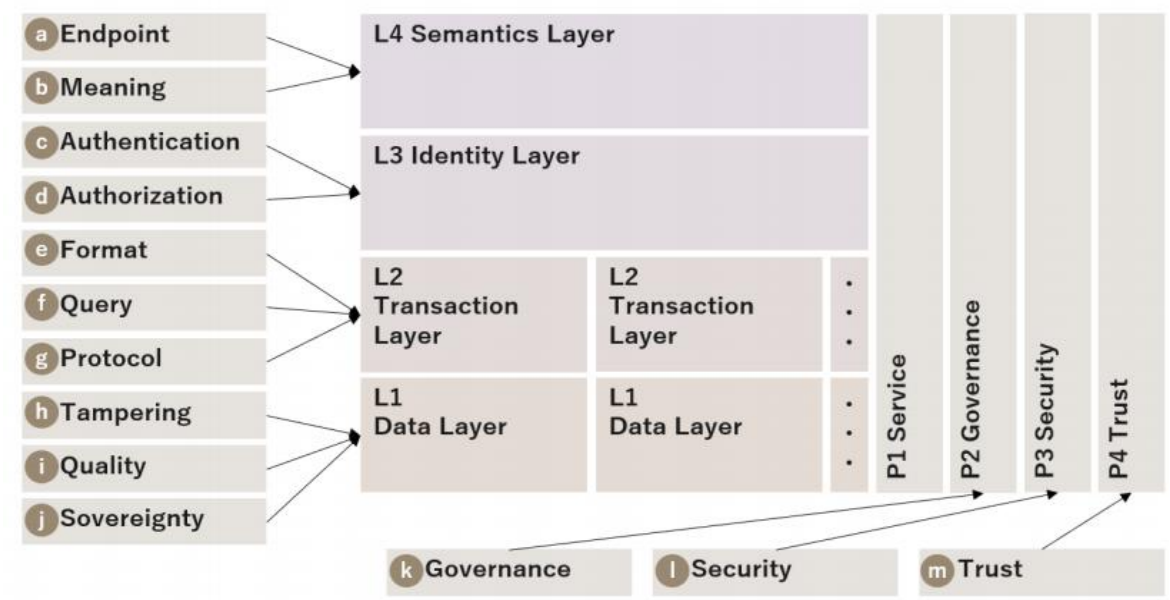
* (Source) METI, Whitepaper: Ouranos Ecosystem Dataspaces Reference Architecture Model

■ Ouranos Ecosystem Data Space Reference Architecture Model (ODS-RAM)

Japan's Ministry of Economy, Trade and Industry (METI) developed the Ouranos Ecosystem Dataspaces Reference Architecture Model (ODS-RAM) to present common elements to consider when establishing the nation's data spaces

ODS-RAM is a reference architecture aimed at ensuring the interoperability and reliability of data spaces. It consists of 4 layers(①Data, ②Transaction, ③Authentication, ④Semantics) and 4 perspectives(①Service, ②Governance, ③Security, ④Trust)

- ✓ **(Layers)** Layers that structurally divide the data space by role and function **(Perspectives)** Directions provided within the data space structure for delivering services to users, operating rules, and securing trust



[Layers and Perspectives of the Ouranos Ecosystem Data Space Reference Model]

Layers	Perspectives			
	Service	**Governance**	**Security**	**Trust**
Data Layer (Ensuring data sovereignty, integrity, and quality)	Provide storage and retrieval services	Reflect quality management rules and meta-identifiers	Encryption and integrity verification during transmission and storage	Secure reliability of data quality and sovereignty
Data Transaction Layer (Controlling and verifying data transmission in various formats and methods)	Support data exchange, transactions, payments, and settlements	Apply exchange rules and operational standards	Secure protocols, integrity verification	Secure reliability of transactions and exchanges
Authentication Layer (Identity management responsible for authentication, authorization, and access control)	Identity and access management services	Apply access control policies	Security design for authentication and authorization	Secure participant reliability and transparency
Semantics Layer (Ensuring interoperability through metadata and semantic interpretation)	Meaning-based services, search support	Semantics and standardization management	Protection of semantic integrity	Secure reliability of data interpretation

* (Source) Reconstructed based on the Ouranos Ecosystem Dataspaces Reference Architecture Model

To provide the functionalities required to ensure interoperability between data spaces, the Ouranos Ecosystem Dataspaces Protocols* are presented

- ✓ In the reference model that outlines the conceptual structure of the Ouranos Data Space, a 'protocol' serves as an interaction rule for the actual implementation and operation of the reference model. It refers to a convention that ensures the diverse service functions provided within the data space are consistently integrated and utilized across various entities

It consists of Fundamental Protocols, which are mandatory for compliance, and Complementary Protocols, which can be selectively applied to enhance the convenience of participation

- ✓ (Fundamental Protocol) Conventions that must be adopted for the Ouranos Data Space to operate at a minimum level
- ✓ (Complementary Protocol) Optional conventions that can be expansively and supplementarily adopted to facilitate the easy participation of various entities

[Ouranos Ecosystem Dataspaces Protocols]

Category	Protocol	Description
Fundamental Protocol	Versioning	Management of protocol version information
	Logging	Recording and observation of historical information
	Monitoring	Activity management, anomaly detection, and operational optimization
	Sovereignty	Self-determination and guarantee of data usage conditions
	Data Trust Assessment	Integrity assessment and provision of results
	Data Trustworthiness and Quality Assessment	Quality assessment and provision of results
	Transaction	Control of the data transmission process
	Identity and Trust	Management of participant identity, authentication, and authorization
	Metadata Exchange	Sharing and processing of schemas and ontologies

Complimentary Protocol	Discovery and Search	Semantics-based information search and discovery
	Heuristic Contracting	Support for electronic contract execution
	Clearing and Payments	Clearing, payment, and billing for service usage
	Marketplace	Management of data purchases and sales

* (Source) METI, Whitepaper: Ouranos Ecosystem Dataspaces Reference Architecture Model

Presents the Ouranos Data Space service sequence model (step-by-step data flow), ranging from metadata collection, identity and credential verification, and contract execution, to data exchange, usage logging, and clearing

[Ouranos Ecosystem Data Space Service Sequence Model]

Step	Description
1. Metadata Collection (Semantics Crawler)	· Crawls metadata, such as RDF, published by data providers to collect semantic descriptions of the data of interest
2. Metadata Visualization & Comprehension (Semantics Viewer)	· Visualizes the collected metadata as ER(Entity-Relationship) diagrams or tables, allowing data consumers to easily grasp its meaning and structure
3. Service Integration Code Generation (Semantics Compiler)	· Automatically generates API integration modules based on semantic descriptions, supporting rapid adaptation when service versions are updated
4. Discovery & Search (Discoverer & Discovery Finder)	· Searches for data or services desired by the consumer and identifies discovery endpoints
5. Data Request (Request Initiation)	· The data consumer initiates a data request for a specific dataset/service (authentication and policy verification run in parallel)
6. Identity & Trust Establishment (Identity Component)	· Performs mutual authentication between the data provider and consumer, verifying credentials and attributes

7. Dataspace Connector Initialization (ODS-FDC)	· The connector receiving the data request activates the Control Plane and Data Plane nodes
8. Transmission Routing Setup (Control Plane Orchestrator)	· Dataplane Selector: Selects the transmission module suitable for the data characteristics · Dataplane Controller: Instructs the start, suspend, and terminate of data transmission · Mutual Authentication: Re-verifies with the counterpart connector
9. Data Transmission Execution (Dataplane Modules)	· Executes data transmission through the selected module (Web API, Stream, File/Bulk, Media Stream)
10. Data Termination (Terminate)	· After data transmission is complete, the control plane issues a Terminate command to end the session. If necessary, the consumer can resume with a new request
11. Auxiliary Functions Execution	· Logging: Records and aggregates transmission history Authentication Federation: Checks the user's authentication status · Managers: Integrates with Credential, Semantics, and DCS functions

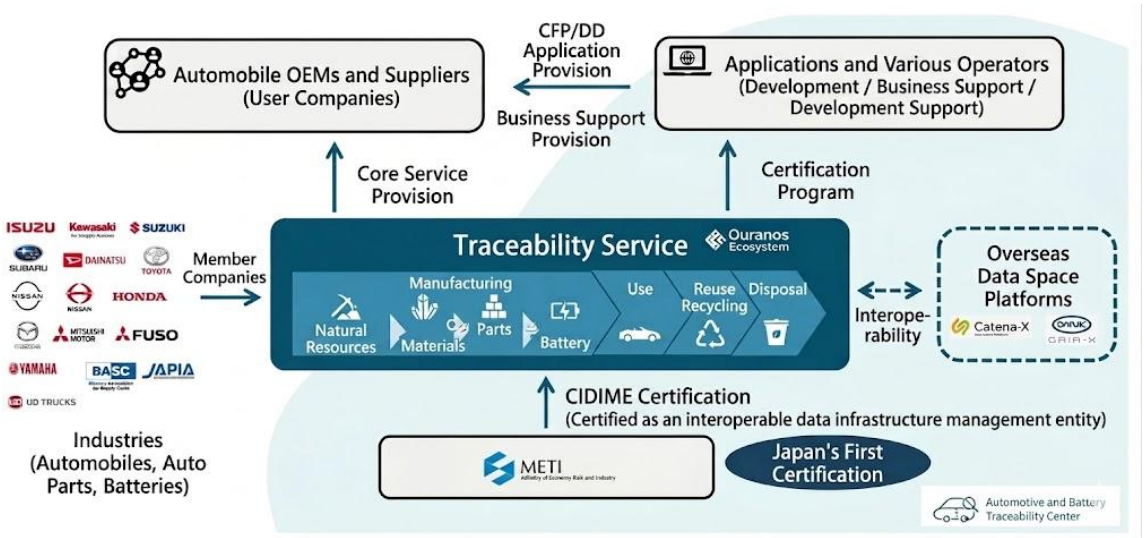
* (Source) METI, Whitepaper: Ouranos Ecosystem Dataspaces Reference Architecture Model

[Ouranos Data Space Case Study: ABtC (Battery Carbon Footprint Tracking)[13]]

- **(Overview**) As the disclosure of the Carbon Footprint (CFP) for electric vehicle batteries sold in Europe becomes mandatory starting in the second half of 2025 under EU battery regulations, this initiative supports companies in complying with regulations while protecting confidentiality. It also aims to resolve social challenges, such as carbon neutrality and resource circulation, and strengthen competitiveness through cross-industry cooperation
- **(Participants)** Automotive OEM manufacturing companies including ISUZU, HONDA, YAMAHA, and SUZUKI
- **(Key Data)** Carbon footprint data generated from battery components and manufacturing processes

[13] https://abtc.or.jp/en

- **(Service)** Accurate and transparent calculation, verification, and sharing of product carbon footprint and Due Diligence (DD) information across all stages of the battery supply chain
- **(Key Process)** Tracking and aggregating the carbon footprint across the entire battery lifecycle → Management based on data sovereignty → Submission to third-party certification bodies → Securing EU regulatory compliance certification → Ensuring continued sales of electric vehicles in Europe



* (Source) Project Certification of Ouranos Ecosystem - Ouranos Ecosystem Leading Project

[Battery CFP (Carbon Footprint) Management and EU Regulation Response Process]

Step	Key Details
Integration of CFP Calculation Applications	Integrates applications from CFP calculation app providers to aggregat CO_2 emissions across the entire battery lifecycle(raw materi procurement → manufacturing → use → disposal/recycling)
Ensuring Data Sovereignty	The CFP data provider directly controls the scope of data disclosure an the recipients (including trade secrets)
Submission to Third-Party Certification Bodies	Submits the aggregated CFP values as evidentiary data to obtain E regulatory compliance certification
Disclosure to the European Market	Discloses the CFP value along with certification data upon the launch the battery pack

2.4 Data Space Standardization Trends

■ IDSA, Promoting Standardization of Data Space Reference Architecture Model

IDSA (International Data Space Association) is a global consortium established in 2016 under the leadership of the Fraunhofer Institute in Germany, responsible for developing and operating data space standardization and governance frameworks

IDSA developed the Data Space Reference Architecture Model (IDS-RAM) to provide a standard structure that supports trust-based data exchange between companies and institutions

It provides a practice-oriented guide for designing and implementing data space architectures, and its core structure consists of 5 Layers and 3 Perspectives

- ✓ IDSA independently established the concept of data spaces and is expanding it into the ISO/IEC AWI 20151 international standardization in 2024, driving global consensus and institutionalization through the launch of an official working group[14]
- ✓ IDSA's data space model is utilized as a core reference framework ensuring trust and interoperability in GAIA-X, the EU Common Data Space, and Japan's Ouranos Ecosystem

[IDSA Reference Architecture Model (IDS-RAM) Layer·Perspective[15] Matrix]

Perspective Layers	Security	Certification	Governance
Business Layer	Defines security requirements in contracts & protection conditions based on data usage purposes	Requires certification of the reliability of participants & organizations	Participation rules, role definitions, contracts & dispute resolution mechanisms
Functional Layer	Designs access control & policy enforcement functions	Certifies whether connector & service functions comply with standards	Ensures rule compliance during function execution & operates monitoring systems

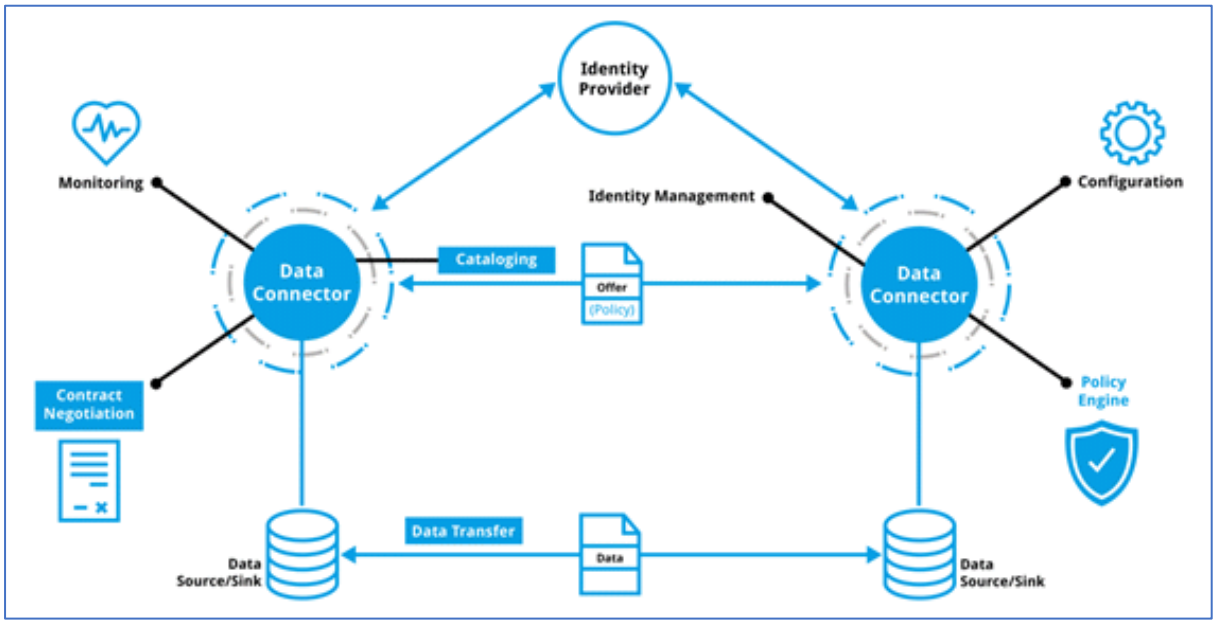
[14] https://internationaldataspaces.org/iso-standard-on-data-spaces-officially-registered/

[15] https://github.com/International-Data-Spaces-Association/IDS-RAM_4_0/tree/main/documentation/3_Layers_of_the_Reference_Architecture_Model

Process Layer	Ensures integrity & confidentiality during data request & response processes	Conducts process conformity verification & audits	Secures process transparency & dispute response procedures
Information Layer	Applies data integrity, anonymization & encryption	Certifies that data format & quality standards are met	Metadata management rules & data management/ utilization governance
System Layer	Applies encryption, authentication-based communication, identity management, & hardware security modules	Certifies IDS Connectors & system components	Operational rules, audit/log management, & system-level governance

* (Source) Reconstructed based on IDS-RAM 4.0

The IDSA defines the Data Space Protocol[16] to facilitate trusted data discovery, exchange, and usage by enabling identity verification among participants and contract-based policy enforcement



[16] https://internationaldataspaces.org/offers/dataspace-protocol/

[IDSA Data Space Process & System Components]

Phase	Key Description	System Components
① Data Discovery	Data consumers search for necessary data resources and verify metadata.	Broker, Catalog Service, Self-Description Repository
② Identity & Access Verification	Verifies the identity of participants and validates data access permissions.	Identity Provider (IdP), DAPS (Dynamic Attribute Provisioning Service), Certificate Management (CA/PKI), VC/DID
③ Contract Negotiation & Policy Application	Confirms and agrees upon data usage terms, enforcing policies based on the contract.	Contract Negotiation Service, Policy Engine (PDP/PEP)
④ Data Transfer	Executes the actual data exchange according to the agreed-upon conditions.	Data Connector, Secure Channels (TLS, mTLS), Data Adapters (DB, File, IoT, etc.)
⑤ Usage Control	Continuously applies usage conditions even after the data has been transferred.	Usage Control Module, Policy Enforcement Point (PEP), Internal Data Apps within the Connector
⑥ Logging & Clearing	Records data exchange and usage history to ensure traceability.	Clearing House, Audit Log Service, Blockchain-based Distributed Ledger Technology (DLT)

* (Source) Reconstructed based on IDS-RAM 4.0

■ Germany: Standardization of the『Data Space Connector』 for Trusted Data Exchange

The German Institute for Standardization(DIN), in collaboration with IDSA and Fraunhofer AISEC, established the standard for 『Security Gateway(Connector) Requirements and Reference Architecture for Industrial Data and Service Exchange』(DIN SPEC 2707017, February 2020)

Connectors must include fundamental security functions such as Encryption, Integrity Verification (detecting data tampering), Mutual Authentication (identity verification). Depending

[17] https://internationaldataspaces.org/ids-is-officially-a-standard-din-spec-27070-is-published/

on the security level (Base, Trust, Trust+), additional requirements—such as isolated execution environments and the prevention of administrator privilege abuse—are mandated

[DIN SPEC 27070 Connector Security Levels (3 Stages)]

Security Level	Key Features
Base	• Guarantees basic safety by meeting the minimum security requirements (encryption, mutual authentication, etc.) necessary for inter-enterprise data exchange
Trust	• Provides enhanced reliability by preventing data tampering and breaches through container isolation and integrity verification
Trust+	• Ensures the highest level of data sovereignty and safety by applying top-tier security capable of defending even against malicious administrator attacks

This connector standard serves as the benchmark for all connector development within the IDSA reference model. It is also utilized as the core framework for verifying standard compliance in various EU flagship projects, such as Catena-X and Manufacturing-X

■ Japan: Standardizing Trust-Based Data Transaction Models

The Data Society Alliance (DSA) of Japan, in cooperation with the IEEE, established the IEEE P3800-2024 standard (2024), which defines the reference model and object framework for trust-based data distribution and transaction architecture

By adopting this standard, Japan aims to establish a principle-based data transaction reference model as an international standard to ensure interoperability and trust during cross-domain data transactions

- The framework defines the roles, relationships, and responsibilities of Data Providers, Data Consumers, and the Data Marketplace.
- It models the data transaction workflow from registration and discovery to contracting, data exchange, and settlement

Through IEEE P3800, Japan seeks to lead global standards for data transaction systems, pursuing a strategy to secure international influence via a path distinct from the EU's Gaia-X/IDSA models.

Reference. Summary of Global Data Space Cases

Category	Gaia-X Data Space	EU Common Data Spaces	Japan: Ouranos Ecosystem
Overview	• A federated data infrastructure project aimed at securing European digital sovereignty (Operates 28+ industry-specific "Lighthouse" projects.)	• Driven by the 『European Strategy for Data』 focusing on building 72 data spaces across 14 sectors throughout the EU	• A Japanese-style data space initiative led by METI to link manufacturing supply chains
Key Features	• Adheres to IDSA reference models and international standards • Industry-level implementation of EU data policies • Federated structure with Self-Description metadata-based catalogs • VC/DID-based identity and policy management. • Clearing House for usage logging and settlement tracking	• Based on EU common standards (DCAT-AP, ODRL, eIDAS) • Works complementarily with industry implementations like Gaia-X.Provides API specifications and toolboxes (common technology, standards, guidelines) • Data exchange based on smart contracts and usage tracking	• Benchmarks EU Gaia-X/IDSA models but adapted for Japan's manufacturing and supply chain characteristics. • Modular design allows for combining data spaces to meet specific industry needs • Operations based on a sequence model (Registration → Verification → Contract → Exchange → Logging) • Proprietary authentication for participant registration and policy-based access control
Implications	• There is a need to design interoperable data spaces by adopting federated architectures that guarantee data sovereignty and trust/settlement systems via Clearing Houses	• Government-led policies and standards must be clearly defined, providing industry-specific toolboxes to help the public and private sectors expand data spaces without excessive cost or time burdens	• It is necessary to develop customized data space models that reflect domestic industry specifics, ensuring they comply with international standards while remaining practical for real-world industrial application
Use Cases	• Catena-X (Automotive) ✓ Supply chain traceability, Product Carbon Footprint (PCF), quality management, and ESG monitoring	• Green Deal Data Space (ESG) ✓ Analysis of climate change and biodiversity using satellite, sensor, and urban data	• ABtC (Battery) ✓ Sharing of battery carbon footprint, raw materials, and supply chain info; interoperable certification systems

2.5 Data Space Reference Model Based on Global Case Studies

By synthesizing international case studies, we have identified the common essential components required to implement data spaces across various domestic sectors. The proposed reference model consists of three layers: Governance, Business Layer, and Technical Layer

■ Governance Layer

By integrating the core principles of the EU, Gaia-X, and Japan's Ouranos, we have derived common elements focused on guaranteeing data sovereignty, applying a federated framework based on agreed common rules, ensuring trust, security, and interoperability, and securing transparency, governance flexibility, and participant autonomy

[Common Components of the Data Space Governance Layer]

Case	Overseas Case Studies
Gaia-X	• Federated structure & decentralization principles • Guarantee of data sovereignty • Consensus-based governance • Ensuring interoperability • Transparency & participant autonomy • Trust-based data exchange environment
EU Common Data Spaces	• Incentive & revenue-sharing systems • Securing transparency • Guarantee of reliability & security • Guarantee of data sovereignty • Consensus-based governance & federation • Ensuring interoperability • Ensuring data reusability & quality
Japan: Ouranos Ecosystem	• Guarantee of data sovereignty • Decentralized data exchange structure • Federated service operation • Consensus-based operation & federation • Securing transparency & trust

Common Components
• Guarantee of Data Sovereignty • Consensus-based governance • Federated operational structure (common rules among participants) • Trust-based data exchange and service model operation • Ensuring interoperability • Securing transparency • Governance flexibility and Federated participation

■ Business Layer

The Business Layer encompasses the service and business models of the data space. It defines the roles and responsibilities of participants, the value flow of data products and services, and operational mechanisms such as contracting and settlement. Through these, it realizes economic and social impacts while ensuring the sustainability of the ecosystem

[Common Components of the Data Space Business Layer]

Case	Overseas Case Studies
Gaia-X	· Sector-specific use case development and management · Data product definition and permission management · Participant registration management (onboarding) · Role definition and collaborative operation · Transparent and policy-based contract management · Payment and settlement functions · Value creation and ecosystem networking
EU Common Data Spaces	· Provision of business, organizational, and technical components · Data exchange and access rule setting · Contract and usage tracking functions · Data product and service development · Stakeholder-demand-based use case development · Definition of roles and responsibilities · Cost and revenue model configuration
Japan: Ouranos Ecosystem	· Promotion of sector-specific use cases through cross-industry collaboration · Provision of industry-digital collaboration business domains · Data sharing and transaction functions · Participant registration and qualification verification · Rule-based access control · Value creation and socio-environmental contribution based on real industrial data

Common Components
· Participant registration, role, and contract management · Development of domain-specific use cases for the data space · Value creation and incentive design · Data access rights and usage policy setting · Provision of data products and services · Usage logging and settlement/clearing functions

By synthesizing the business components of Gaia-X, the EU, and Japan, common elements have been derived, including domain-centered use case development, participant registration management(onboarding), role/contract management, data access and usage policy setting, settlement functions, and value creation and incentive design

■ Technical Layer

The Technical Layer defines the underlying technologies, standards, and components that enable the registration, discovery, transfer, management, and settlement of data within a data space. It provides the technical infrastructure to ensure that the service models and value flows defined in the Business Layer can be practically implemented and operated.

[Common Components of the Data Space Technical Layer]

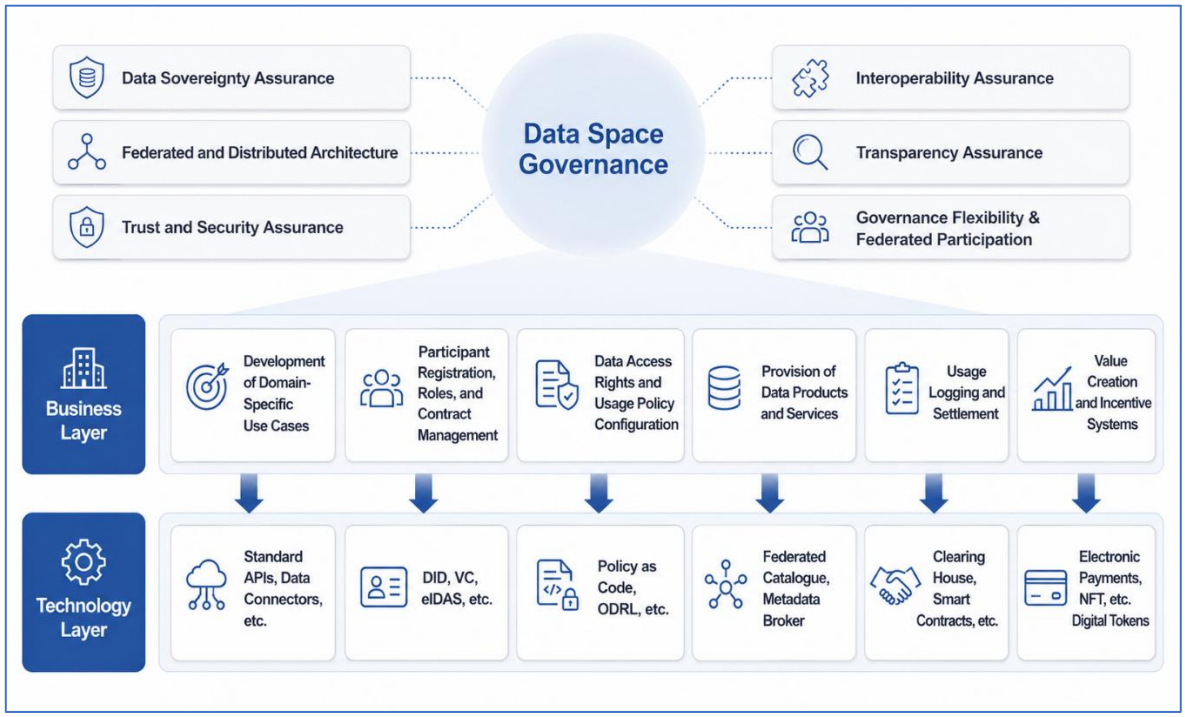
Case	Overseas Case Studies
Gaia-X	· Federated Catalogue · Self-Description Metadata · Identity & Trust Management (DID/VC, Federated Trust Anchor) · Policy-as-Code exchange modules · Data Connectors (IDS/EDC Connector) · Clearing House · Electronic payments and Token (NFT) / Coin-based settlement
EU Common Data Spaces (DSSC)	• DCAT-based Metadata Broker • Common Data Models and Reference APIs • Electronic Signature-based identity authentication • Data Connectors (Optional) • Policy & Contract Management (ODRL-based, etc.) • Smart Contracts & Usage Tracking/ Logging modules • Euro (EUR)-based electronic payments

Common Components
• Federated Catalog • (Registration of data products/services based on standardized metadata) • Metadata Broker (Discovery of data products) • Standard APIs & Data Connectors • (Secure, trust-based data transfer) • Identity & Trust Management (DID, VC, eIDAS, etc.) (Participant authentication and credential verification) • Policy & Contract Management (Policy-as-Code, ODRL, etc.) (Access and usage control) • Usage Logging & Clearing (Clearing House) (Traceability and settlement monitoring)

Japan: Ouranos Ecosystem	• Federated Catalog and Metadata Hub • Lightweight Connectors (Integration with existing ERP/IoT systems) • Sequence-based exchange pipelines • Transaction management and Logging/Clearing modules • Semantic Interoperability Engine • Heuristic Contract-based electronic payments	• Electronic Payment & Digital Tokens (NFTs, Stablecoins, etc.) (Automated payment and transparent settlement)

By synthesizing the technical components of Gaia-X, the EU, and Japan, common data technologies have been identified, including Metadata Brokers, Federated Catalogs, Data Connectors, DID/VC-based Identity Management, Policy/Contract Management modules, Clearing Houses, and standards like DCAT.

This reference model serves as the essential set of components for designing and operating data spaces and functions as a guiding framework to facilitate data exchange and utilization across regions and industries. Ultimately, it aims to align with global standards to secure international interoperability and trust



[Data Space Reference Model]

3. Korea's Data Space Initiatives

3.1 Current Status of Domestic Data Ecosystem

■ Insufficient Tangible Effects of Existing Data Systems

Despite establishing a legal foundation through the "Framework Act on the Promotion of Data Industry and Use", which includes standardized contracts, data valuation, and licensing types - these systems have not gained significant traction in actual data trading and utilization fields.

- Lack of Dynamic Settlement: Current domestic data marketplaces and platforms lack a system where settlement and pricing are determined based on actual usage volume or patterns. This fails to provide clear compensation for providers and prevents a rational cost structure for consumers
- Absence of Execution Monitoring: While standardized contracts exist, there is no operational system or consensus body to monitor, track, or prevent unauthorized use (use beyond the intended purpose) during the contract execution phase. Consequently, when disputes arise, parties must rely on reactive legal action or administrative sanctions

Data spaces establish a fair compensation system by systematically integrating and managing contract terms and usage history. Furthermore, they provide a trust-based environment for data sharing and utilization by automatically detecting and blocking use beyond the agreed-upon purpose.

■ Structural Constraints of Centralized Platforms

Currently, the 21 sector-specific big data platforms operate on a centralized model where data is aggregated into a single repository. This results in a loss of control for data providers and limits the voluntary participation of data consumers

This structure creates barriers to autonomous cross-industry analysis and data fusion between participants across different sectors. Furthermore, the supplier-centric data delivery model makes it difficult to produce and distribute high-quality data that meets high market demand

Data spaces leverage federated governance and decentralized data exchange structures to connect and utilize data at its source. This enables seamless data fusion and the distribution of high-quality data while ensuring providers maintain full control

- Despite the establishment and official announcement of common standardized terminology for domestic data platforms, field adoption remains insufficient. Consequently, data formats and terms vary by institution, and inconsistent quality control levels make it difficult to ensure data integrity and consistency[18]
- From the providers' perspective, there is a hesitant stance due to the fear of losing rights and control over their data once it has been provided (NIA, 2024)

■ Limits of Data Collaboration and Business Model Creation

Current domestic data marketplaces and platforms lack a functional collaboration mechanism between providers and consumers. This forces providers to manually seek out and onboard consumers, making it difficult to achieve sustainable, data-driven business model creation

In particular, high-value data, such as high-quality AI training datasets, remains restricted due to regulatory burdens and ambiguities in current laws (e.g., Copyright Act, Personal Information Protection Act). Despite being the area of highest demand, this data is not circulating effectively in the market

- Most data platforms and marketplaces focus on functions centered around data processing and sales, such as providing raw data or processed outputs (e.g., reports)
- Platforms generally operate in a unidirectional (Provider → User) structure, with almost no cases of project-based collaboration aimed at creating new services or business models.

✓ **The Data Space Solution**: Data spaces facilitate collaboration between providers and consumers, allowing for the autonomous development of business models. Moving beyond the secure utilization of high-value data, they support the creation of a virtuous data ecosystem that spans from production and creation to distribution

[18] https://online.kofst.or.kr/news/316787?category=COM045_7DaOeSe

[Improvement Directions for Domestic Data Platforms]

Category	AS-IS	TO-BE
	Big Data Platforms (Finance, Agricutlrue, etc.)	Data Space
Primary Function	Collecting and aggregating public/private data to provide services via processing and analysis	Trust-based data sharing and the creation of innovative services through collaboration
Storage & Management	Institutions and companies migrate and aggregate data to a central platform	Data is stay-at-source (retained/managed by each entity) with distributed/federated access control
Operational Model	Led by the platform operating agency	Consensus-based operation involving providers, consumers, and operators
Demand Creation	Providers must manually discover consumers	Joint participation of providers and consumers to co-discover business models and collaboration opportunities
Revenue & Settlement	Centered on fixed-fee or one-time contracts; difficult to reflect actual usage or post-trade conditions	Automated settlement and profit distribution based on Smart Contracts and Clearing Houses

3.2 Government Initiatives to Establish and Scale Data Spaces in Korea

① Ministry of Science and ICT (MSIT)

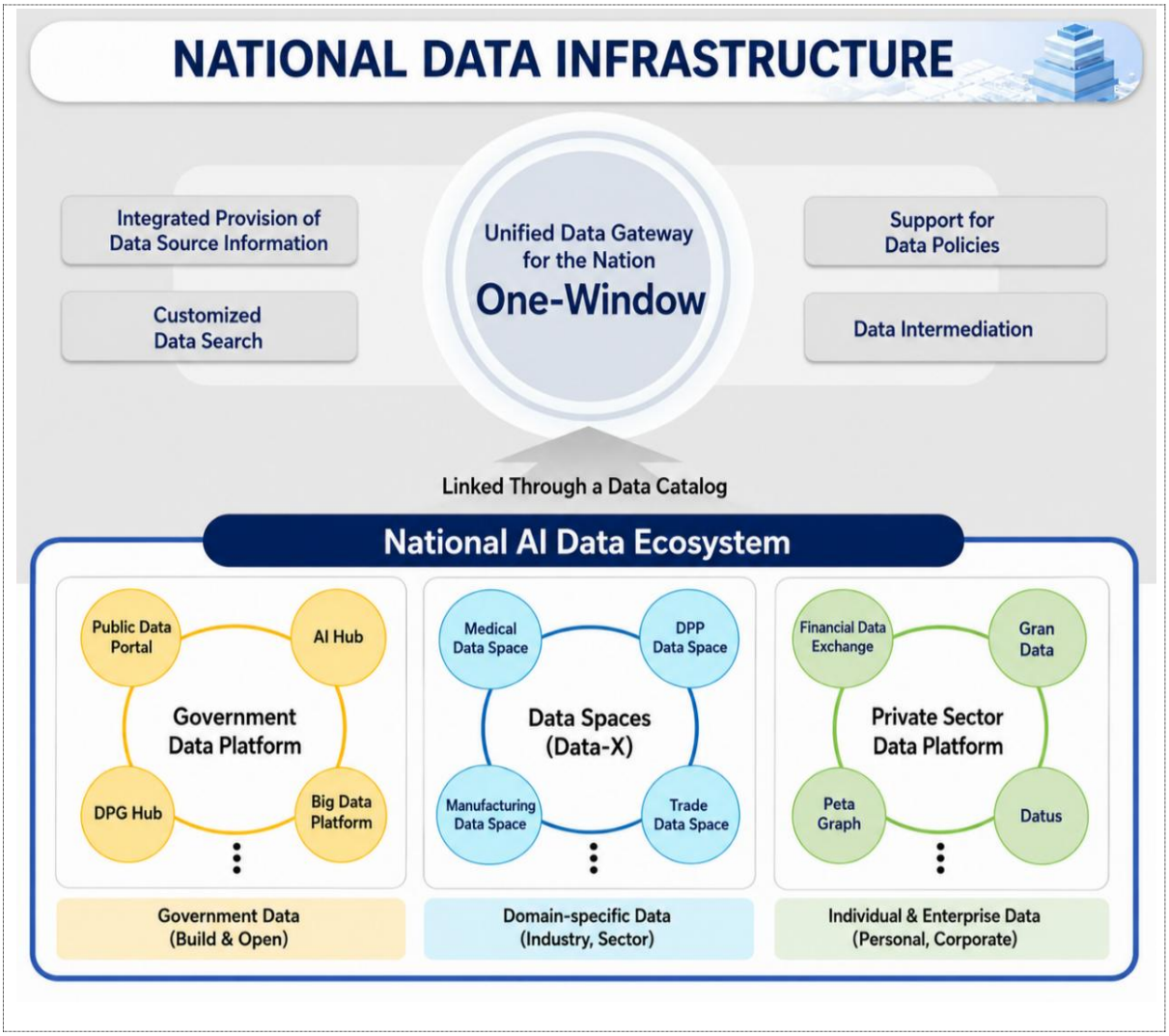
To overcome the limitations of fragmented data utilization caused by data asset protection–centric environments, the Ministry of Science and ICT (MSIT) is promoting the adoption of data spaces as a foundational framework for accelerating AI Transformation (AX) across various sectors.

Beginning with the healthcare sector, MSIT plans to gradually expand the data space model, enabling each organization to retain ownership of its original data while allowing authorized use whenever necessary.

[Launch of the Korea’s Medical Data Space (June 2026)]

To address the fragmentation between existing public-private big data platforms and emerging data spaces, MSIT launched the National Data Infrastructure (NDI) initiative in 2024. The initiative aims to provide a unified gateway for discovering and linking public and private data while strengthening interoperability among data spaces through a federated data catalog and common compliance framework.

[Model for the National Data Infrastructure (NIA, 2025)]



② Ministry of Trade and Industry (MOTIR)

The Ministry of Trade and Industry (MOTIR) regards industrial data spaces as a key enabler for AI-driven manufacturing transformation and compliance with evolving global regulations. It defines industrial data spaces as a trusted infrastructure supporting data exchange, sharing, verification, and transactions throughout the entire supply chain.

In addition, MOTIR is promoting the development and demonstration of a standardized industrial data space model through the Manufacturing AI Transformation Alliance (M.AX Alliance).

MOTIR is also pursuing international cooperation, including interoperability with Germany's Manufacturing-X initiative to establish a trusted data exchange ecosystem. Furthermore, it

seeks to strengthen data-driven regulatory compliance in response to expanding global supply chain regulations, such as the EU Digital Product Passport (DPP).

[Hosting Korea-Germany Industrial Dataspace Forum (Oct 2025)]

③ Policy Implications

The policy directions of both MSIT and MOTIR demonstrate a shared recognition that expanding AI adoption and responding to global regulatory changes require more than individual projects or standalone digital platforms. Instead, both ministries emphasize the importance of establishing structural national- and industry-level foundations that enable trusted data utilization.

While MSIT focuses on strengthening data connectivity and utilization through sector-specific data spaces and the National Data Infrastructure, MOTIE is advancing industrial data spaces as trusted infrastructures for data exchange, verification, and transactions across supply chains while simultaneously promoting international collaboration.

Together, these initiatives indicate an emerging policy consensus that future AI competitiveness will depend not only on the capabilities of individual organizations or enterprises, but also on trusted data-sharing mechanisms, interoperable data ecosystems, and governance frameworks that enable secure and scalable data collaboration.

3.3 Korea’s Data Space Reference Model

Major international data space reference models, including IDSA IDS-RAM, DSSC Data Space Reference Architecture, and the Ouranos Reference Architecture Model (RAM), primarily define common building blocks that enable data exchange and utilization among participants, such as data catalogs, identity and access management, and connector-based interoperability. However, capabilities supporting AI-driven analytics and services, as well as data trading and settlement, are only partially addressed.

Building upon these international reference models, the Korean Data Space Reference Model reorganizes data space building blocks into two domains: Governance and Architecture. These building blocks are further classified into Common Building Blocks (essential capabilities) and Extended Building Blocks (optional capabilities) to provide a more systematic and scalable framework.

In particular, to address the limited coverage of AI utilization in existing reference models, the Korean model introduces AI infrastructure components as extended building blocks. This enables data spaces to evolve beyond secure data exchange into comprehensive platforms that support AI model development, distributed analytics, and AI-enabled service creation.

■ Korea’s Data Space Governance Building Blocks

The Korea’s Data Space governance model is designed as a federated collaboration ecosystem centered on shared trust and consensus for data and AI utilization, rather than on specific technologies or platforms.

Within this model, a data space is not a centrally controlled environment. Instead, it enables data providers and consumers to participate while retaining sovereignty over their own data, with collaboration established through agreed common policies, rules, and operational procedures.

Governance functions not merely as a collection of operational rules, but as the core operating mechanism that continuously defines, coordinates, and enforces what is permitted, how responsibilities are allocated, and how trust is established across the entire lifecycle of data access, integration, AI training, and service deployment.

Through this governance framework, the Korean Data Space extends beyond secure data exchange to provide an environment where AI models and data-driven services can be safely developed, validated, and scaled under agreed rules, while ensuring fair value distribution and fostering an autonomous yet accountable ecosystem for data and AI collaboration.

KOREAN DATA SPACE GOVERNANCE BUILDING BLOCKS

Principles, policies, and processes for trustworthy, fair, and sustainable data collaboration

GOVERNANCE FRAMEWORK

Trust • Transparency • Fairness • Security • Sustainability

1 PARTICIPANTS & ROLES

- **Operators**
  Overall operation, policy application, monitoring and dispute resolution
- **Participants**
  Data provision and usage, AI training, and service delivery
- **Common Service Providers**
  Data connectivity, trust & identity, settlement, and common services

2 GOVERNANCE ORGANIZATION

- **Steering Committee**
  Strategic direction and policy approval
- **Working Groups (Sub-committees)**
  Domain-specific consultation and policy development
- **Decision-making Structure**
  Transparent and inclusive decision-making process

3 POLICIES & RULEBOOK

- **Participation Management (Incentives & Sanctions)**
  Participation management and incentive / sanction rules
- **Data Standards & Metadata Policy**
  Data standards and metadata (DCAT, etc.)
- **Data Access & Usage Policy**
  Provider-controlled, conditional access and usage
- **Trust & Data Exchange Policy**
  Authentication, access control, audit trail and exchange standards
- **Contract & Settlement Policy**
  Standard data contracts and settlement procedures
- **Dispute Resolution & Liability**
  Dispute resolution and liability framework

4 OPERATIONS & USE CASES

- **Use Case Development**
  Identify and co-create high-impact use cases
- **Data Pipeline Management**
  Data linkage – AI training – service pipeline
- **AI Service Operation**
  AI model training, analysis, and service deployment management

5 SUSTAINABILITY

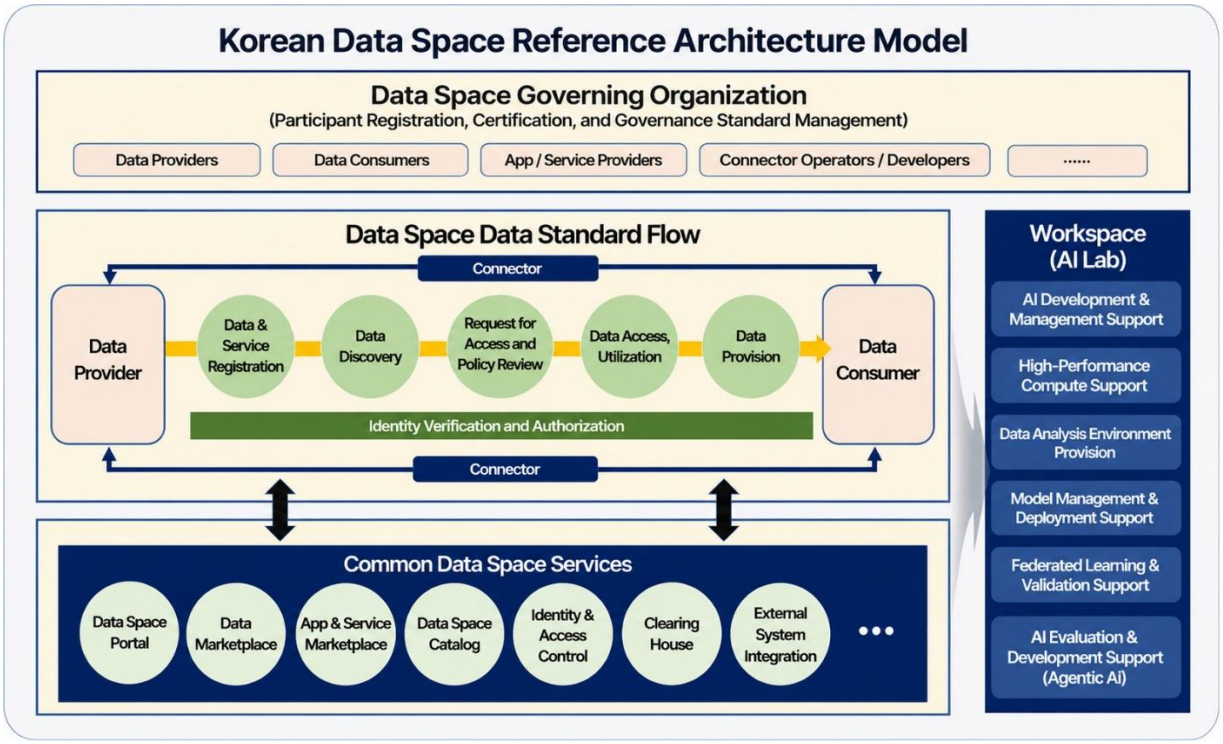
- **Membership Model**
  Onboarding and role-based membership structure
- **Fee Policy**
  Usage-based and contribution-based revenue model
- **Ecosystem Expansion**
  Enable a thriving data and service ecosystem

■ Korea’s Data Space Reference Architecture Building Blocks

The Korean Data Space Reference Architecture presents a trust-based, federated architecture that enables data providers and data consumers to securely connect, exchange, and utilize data through standardized data connectors while preserving their respective systems and data sovereignty.

■ Korea’s Data Space Reference Architecture Model

The Korean Data Space Reference Architecture Model presents a trust-based, federated architecture that enables organizations to securely connect, exchange, and utilize data while maintaining ownership of both their data and underlying systems. Rather than relying on centralized data collection, the architecture allows data providers and consumers to collaborate through standardized data connectors, ensuring interoperability, data sovereignty, and policy-driven access control across heterogeneous environments. The model integrates governance, common services, and technical building blocks into a unified architecture that supports trusted data collaboration at scale.



[Korea’s Data Space Reference Architecture Model (NIA, 2026[19])]

Unlike existing international reference models, which primarily focus on secure data exchange and interoperability, the Korean model is designed to support the entire data value creation lifecycle. In addition to core functions such as metadata management, identity and access management, connectors, and policy enforcement, the architecture incorporates capabilities for data contracts and settlement, AI-ready data processing pipelines, audit logging, and federated service integration. This enables data spaces to evolve from simple data-sharing

[19] Korea’s Data Space Reference Model Ver 1.0 (NIA, 2026)

infrastructures into platforms that facilitate continuous collaboration, value creation, and sustainable ecosystem growth.

The Korea's Data Space Reference Architecture extends conventional data space capabilities by incorporating an AI Lab Workspace and an ontology-based semantic framework into the overall architecture. The AI Lab provides a shared execution environment that supports capabilities such as Compute-to-Data (C2D), AI model training and fine-tuning, GPU computing resources, MLOps, model registry, validation, and data preprocessing, enabling participants to develop and utilize AI models while maintaining data sovereignty. In addition, the ontology framework provides a common semantic foundation that enables consistent interpretation of concepts, relationships, and contextual information across heterogeneous datasets and domains. Together, these capabilities support interoperable data utilization, AI-driven analytics, and the development of data-driven services within a trusted and federated data space environment.

The Korea's Data Space Reference Architecture defines a standardized end-to-end workflow for trusted data sharing and utilization, integrating participant onboarding, federated data exchange, policy enforcement, contract management, secure data utilization, lifecycle auditing, and AI-ready capabilities including Compute-to-Data (C2D), federated learning, and semantic interoperability.

[Korea's Data Space Standard Data Flow]

Step	Process	Description	Key Technologies / Components
1	**Onboarding**	Establish trusted participation through participant identification, authentication, and onboarding.	Decentralized Identifier (DID), Verifiable Credential (VC), Digital Wallet, Level of Assurance (LoA)
2	**Data Space Connector Connection**	Establish a federated data connectivity environment between organizational systems and the data space.	Connector as a Service (CaaS), Self-hosted Connector, Data Space Protocol (DSP)
3	**Data & Service Registration and Validation**	Register metadata in the federated catalog and validate data quality, schema, and publication requirements.	Self-Description, ODRL-based Usage Policy, Schema & Metadata Validation

4	**Data & Service Discovery**	Discover available datasets and services through federated catalogs.	Federated Catalog, Semantic Hub, Ontology-based Mapping
5	**Access Authorization & Policy Verification**	Verify access rights and usage conditions according to provider-defined policies.	PDP/PEP/PIP Architecture, ODRL Policy Evaluation, Attribute-Based Access Control (ABAC)
6	**Data Contract Establishment**	Negotiate and establish contractual agreements between data providers and consumers.	Peer-to-Peer Data Contract, Payment Mechanism Integration
7	**Data Preparation**	Prepare and transform data according to contractual and policy requirements before utilization.	Data Profiling, De-identification, Data Standardization, Semantic Mapping
8	**Data Access & Utilization**	Execute secure data exchange and AI-enabled utilization under agreed policies and contracts.	Data Exchange, Compute-to-Data (C2D), Federated Learning, API-based Exchange
9	**Data Lifecycle Logging & Auditing**	Record and manage the complete lifecycle of data usage for traceability and compliance.	W3C PROV-based Provenance, Audit Logging, Traceability
10	**Settlement, Dispute Resolution & Post-Operation Management**	Manage settlement, revenue distribution, dispute resolution, and post-transaction operations.	Revenue Sharing, Usage-based Settlement, Dispute Resolution

4. Strategy for Advancing Korea's Data Spaces

① Phased Development and Expansion of Data Spaces

In the initial stage, multiple small-scale data spaces will be established at the industry and service levels, taking into account legal, regulatory, and technical considerations. Through diverse pilot projects, interoperability among standards, contractual and policy frameworks, and technical building blocks will be validated.

Based on the results of these pilot implementations, the ecosystem will be progressively expanded by increasing the number of participants, broadening the scope of data, and enhancing service capabilities. Federation among individual data spaces will ultimately enable the development of a scalable and interconnected data ecosystem.

② Expanding Data Spaces Beyond Regulatory Compliance Toward Vertical AI

While Europe has primarily adopted data spaces as a means of regulatory compliance, their industrial utilization and business value creation remain relatively limited. Korea aims to move beyond compliance-oriented adoption by actively identifying and scaling Vertical AI use cases across industries. By establishing a virtuous cycle connecting data provision, data utilization, and AI-driven service creation, Korea's data spaces will foster business opportunities and strengthen AI competitiveness across industrial sectors.

③ From Government-Led Demonstration to a Private Sector–Driven Ecosystem

During the initial phase, the government will lead the establishment and operation of data spaces by defining core foundations, including standards, technical architectures, and contract and settlement models, while generating reference implementations through pilot projects. As the ecosystem matures, responsibility will gradually shift to the private sector, enabling organizations to autonomously provide and utilize data, develop value-added services, and establish a sustainable, market-driven data ecosystem.

④ Improving Accessibility Through Data Space as a Service (DaaS)

In the long term, core data space capabilities, including connectors, data registration and discovery, contract management, and policy management, will be provided as Data Space as a Service (DaaS), enabling organizations to participate in data spaces without deploying dedicated technical infrastructures. This approach will lower entry barriers for SMEs and a broader range of stakeholders, promote the creation of new data-driven services and value-added business opportunities, and encourage wider participation across the entire data space ecosystem.

[Glossary]

Data Space

A decentralized data-sharing space where various participants can securely and reliably share and utilize data while maintaining data sovereignty within a distributed infrastructure environment

VC (Verifiable Credential)

A digital credential issued and verified to reliably prove a participant's identity or data usage rights

DID (Decentralized Identifier)

A unique digital identifier directly controlled by individuals or organizations without the need for a central authority, used to identify the issuer or subject within a VC

Data Connector

A technical component that exposes data or services hosted on an organization's IT infrastructure to the Data Space environment, supporting actual data access in connection with a catalog platform

Metadata Broker

An intermediary service that collects, manages, and provides metadata between data providers and consumers, supporting data discovery and utilization in conjunction with a data catalog

Smart Contract

An automated contract executing on a blockchain, where the contract terms are automatically performed when specific conditions are met, enabling trust-based automated transactions without intermediaries

Token Economy

An economic system that designs economic value and incentives using tokens; within a Data Space, tokens can be utilized as a means to trade data or adjust access privileges

Policy as Code

A method of defining policies in code form to enable automated processing and execution. This approach is advantageous for consistency and automation, as it allows policies to be version-controlled, automatically deployed, and tested just like software code

Policy Engine

The central component of a system that evaluates policies and makes decisions. It receives requests from a Policy Enforcement Point (PEP), interprets the policy, and issues an approve or deny decision

PEP (Policy Enforcement Point)

The component that actually enforces policies in a policy-based access control system. It forwards user requests to the Policy Decision Point (PDP) and allows or blocks access based on the result

ODRL (Open Digital Rights Language)

A W3C standard language developed to express rights, obligations, and restrictions regarding digital assets in a machine-readable format. In a Data Space, it is utilized to automatically interpret and execute policies set by data providers

IDSA (International Data Spaces Association)

A non-profit organization established in 2016 under German law that plays a key role in establishing a standardized data exchange framework by defining the Reference Architecture Model (IDS-RAM), Rulebook, and Data Space Protocol (DSP). Currently, over 140 global companies and institutions participate as members to support the vitalization of the data economy

Data Catalog

A system or tool that systematically collects and manages metadata for data assets, empowering users to easily search, explore, understand, and utilize data

Digital Clearing House

A platform that mediates transactions, payments, and settlements between data providers and consumers, performing tasks such as data license management, payment processing, and access right coordination

Self Description

A mechanism for providing a description of an entity independently; for example, a document or structure in which a system component or service self-describes its own functions, policies, and identification information

DAPS (Dynamic Attribute Provisioning Service)

A service that dynamically provisions and verifies credentials or attributes. In environments like Data Spaces, it is utilized as a necessary component for participant authentication and attribute-based access control

Onboarding

The formal procedure through which a new participant enters a Data Space, undergoes identity registration and authentication, and officially joins the network

Ontology

A knowledge representation framework that formally defines concepts and relationships within a specific domain. In a Data Space, it ensures semantic interoperability by providing a common semantic framework among participants

W3C PROV

A W3C recommended standard for describing the provenance, creation process, and responsible entities of data and processes. It is utilized to secure data reliability and traceability

AAS (Asset Administration Shell)

A core concept of Industry 4.0; an international standard data structure designed to realize digital twins by representing physical assets—such as machines, equipment, and products—as digital information for advanced utilization

DFFT (Data Free Flow with Trust)

A global data governance principle proposed by Japan at the 2019 G20 Osaka Summit. It embodies the concept of ensuring the free flow of data while simultaneously safeguarding privacy, security, and intellectual property rights. It is widely utilized as a core keyword for data governance in various international discussions, including those at the OECD, WTO, and EU

GDPR (General Data Protection Regulation)

The European Union's (EU) personal data protection regulation, enforced since May 2018. It applies strict standards for the processing of personal information and guarantees user rights

GAIA-X

A European data and cloud infrastructure project launched in 2020, led by Germany and France. It aims to build a safe and reliable data-sharing ecosystem through open standards and common specifications to secure data sovereignty and enhance interoperability, thereby supporting the vitalization of the European data economy

DSSC (Data Spaces Support Centre)

An institution supported by the European Commission, established to facilitate the development and ensure the interoperability of various Data Spaces within Europe. It develops common frameworks, technical reference architectures, and guidelines for industry- and domain-specific Data Spaces

Compute-to-Data

A mechanism where data providers do not directly export data externally; instead, algorithms are sent to the data's location to perform computations, and only the results are shared. This approach protects data sovereignty and privacy while still allowing external researchers and analysts to derive value from the data

Data Silos

A phenomenon where data becomes isolated and disconnected within organizational units, preventing it from being shared and utilized across other systems. This can lead to data duplication between organizations, as well as reduced consistency and operational efficiency

DAO
(Decentralized Autonomous Organization)

A decentralized digital organization operated through blockchain and smart contract-based governance. Members can participate in decision-making processes via blockchain-based voting mechanisms

eIDAS

A legal and institutional framework enacted to mutually recognize and guarantee electronic identification (eID) and trust services for electronic signatures and electronic transactions across the European Union (EU)

[References]

1. Data Spaces Support Centre(2025), Blueprint v2.0,
2. https://dssc.eu/space/BVE2/1071251457/Data+Spaces+Blueprint+v2.0+-+Home
3. European Commission(2025), Common European data space https://digital-strategy.ec.europa.eu/en/policies/data-spaces
4. Green Deal Dataspace(2025), https://green-deal-dataspace.eu/
5. ADVEANO Data Marketplace(2025), https://www.advaneo-datamarketplace.de/en/#
6. Gaia-X Framework(2025), https://docs.gaia-x.eu/#/framework
7. Gaia-X(2025), Gaia-X Architecture Document https://docs.gaia-x.eu/technical-committee/architecture-document/25.05/
8. Gaia-X(2025), Gaia-X Lighthouse Projects https://gaia-x.eu/community/lighthouse-projects/
   Catena-X(2025), Catena-X Expert Groups & Committees, https://catena-x.net/association/expert-groups-committees/
9. Catena-X(2025), Catena-X Standardization, https://catena-x.net/association/standardization/
   Gaia-X(2025), Gaia-X Digital Clearing House(GXDCH), https://gaia-x.eu/services-deliverables/digital-clearing-house/
10. Gaia-X(2024), Gaia-X and Catalogues, https://gaia-x.eu/gaia-x-and-catalogues/
11. METI(2025), Ouranos Ecosystem, https://gaia-x.eu/gaia-x-and-catalogues/
12. METI(2025), Ouranos Ecosystem Dataspaces Reference Architecture Model
13. Automotive and Battery Traceability Center (ABtC), https://abtc.or.jp/en
14. IDSA(2025), https://internationaldataspaces.org/
    International-Data-Spaces-Association, IDS-RAM 4.0 https://github.com/International-Data-Spaces-Association/IDS-RAM_4_0/tree/main/documentation/3_Layers_of_the_Reference_Architecture_Model
15. IDSA(2025), Data Space Protocol, https://internationaldataspaces.org/offers/dataspace-protocol/
16. Ministry of Science and ICT (2025), One-Window, https://www.data1window.kr/
17. National Information Society Agency(NIA) (2024), Concept and Implementation Strategy for National Data Infrastructure
18. Kim, Geon-wook, Daegu Digital Innovation Promotion Agency (DIP) (2025),

Implementation of a Mobility Data Exchange and Transaction System Based on a Decentralized Data Space
19. Alexander Bott et al(2025), Challenges in Implementing Gaia-X for Industrial Applications, 2025
20. Catena-X(2025), Business Areas in the Catena-X Ecosystem https://catena-x.net/overview-use-case-cluster/
21. John. G. Dale et al(2024), “Data Free Flow with Trust”: Japan’s struggle to integrate democracy and human rights into digital trade policy
22. Son, Hyeong-seop (2025), A Comparative Study of the Revised Personal Information Protection Act and Japanese Law – Focusing on the Domestic and International Transfer of Data
23. Oh et al(2026), Korea’s Data Space Reference Model Ver 1.0, 2026
24. European Data Protection Board(2025), International Data Transfers, https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers_en?utm_source

NIA Digital & AI Insights Series

Korea's Data Space Initiative (K-Data Space)

Published by

National Information Society Agency (NIA)

Hyung Chul Kim, President

Original Authors

AI Policy Department

Young Joo Lee, Executive Principal

AI Data Department

Daehoon Oh, Principal Manager

English Edition Prepared by

Department of Global ICT Cooperation

Yoon-seok Ko, Vice President

Hyang-nae Jeon, Director

Sora Jeong, Senior Manager

Won Ko, Manager

LLM (Large Language Model) technology was partially utilized in the translation process of this report.