

Data spaces facilitate the trustworthy implementation of data-based applications and business models and allow all participants a high degree of flexibility and sovereignty.

Objectives

Value added

New data-based applications, business and collaboration models.



Self-determination

Keeping control over the conditions of data sharing (With whom do I want to share which data and for how long?).



Efficiency

Data is shared solely for a specific purpose.



Characteristics

Decentrality

Decentralised solutions are prioritised.



Federation and interoperability

Stakeholders are encouraged to work together both within and beyond the confines of a data space.



Sovereignty

Control over one's own data and their use is always guaranteed.

Trust

Technologies, control mechanisms and unique digital identities help to build trust in the ecosystem. Standards for data quality ensure a high level of trust in the data.



Transparency

Digital identities and the traceability of data transfers promote transparency.

Data spaces are flexible and open IT structures that guarantee the absolute sovereignty of the participants involved. As such, they facilitate the trustworthy and transparent use of decentralised data according to pre-defined scopes of use.

Data spaces are set up as federal entities and are based on various basic concepts/elements:

- Data space operation and management services (core services)
- Technical standards
- Operational processes
- Regulatory frameworks (governance model)


A key feature of data spaces is that they create a level playing field for sovereign data sharing. This means that all participants can benefit from the use of data in the same way.

Key concepts



Federation

A data space follows federal principles, which, for instance, allows a local data space view to be evolved into a global one. This is possible thanks to the syntactic and semantic harmonisation of different approaches and the use of standards.




In a data space, the data provider decides how data offerings are displayed, e.g. in terms of volume. Harmonising the descriptions of the data offerings and the use of standards paves the way for individual offerings to be findable and usable by a large number of actors.



Trust and transparency

An important prerequisite of trust in data spaces are digital identities for participants. Moreover, the application of and adherence to the above basic elements a) to c) (core services, technical standards, operational processes) also builds trust in data spaces.




This allows for transparency and traceability of data use and provides a technical proof of compliance with data sharing agreements.



Sovereignty

In the context of data spaces, sovereignty has several levels:

- Data sovereignty and adequate control mechanisms for providers, who need to be able to determine whether and to what extent their data is used.
- Technological sovereignty that enables data providers to manage data within their own systems. Only for the purpose of exchanging data, they need to use components dictated by a data space (e.g. a connector).




Ultimately, data providers always have full control over their data. Further, the data space comes with very few technological constraints for its users.



Interoperability within the data space

The adherence to the above basic concepts and elements a) to c) (core services, technical standards, operational processes) supports the compatibility of individual data offerings in the data space.



This creates a marketplace for a specific data offering, e.g. focusing on one single domain of application.

Key concepts



Decentralised set-up

A data space is not a centralised repository or centralised platform. The actual management of the data sources linked to a data space always takes place within the participants IT systems. This implies that peer-to-peer structures are set up for actual data use.

Data providers themselves retain control over the use of their data.



Meshed data spaces/Data space mesh

Meshed data spaces facilitate the integrated use of data from data sources that come from different data spaces. In this context, operation and management services of these different data spaces help clarifying syntactic and semantic conflicts, which can arise, for instance, in connection with the cross-sectoral use of data.

As a result, the data offerings of different marketplaces can flow more easily across sector boundaries. For example, the integration of data offerings from the mobility and energy domains is important for realising use cases for improved e-vehicle charging.

Example of a Data Space Mesh



Data space from the culture domain



Data space from the energy domain



Data space from the mobility domain



Data space from the health domain

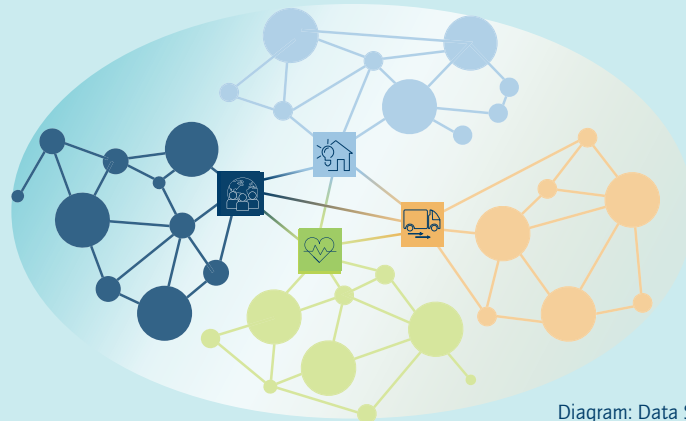


Diagram: Data Space Mesh



Interoperability beyond the boundaries of a data space

The adherence to the basic elements a) to c) (core services, technical standards, operational processes) supports the compatibility of individual data offerings beyond data spaces.

This means that it does not matter to a user or application developer by what technical means they obtain the data – from an individual data space or from different data spaces.

Implementation of data space standards: The example of the Mobility Data Space (MDS)

Federation and interoperability

To facilitate data sharing across data spaces (in technical, structural and legal respects), data spaces must meet open standards such as those provided at European level, e.g. by Gaia-X. The Mobility Data Space (MDS) establishes a Gaia-X-aligned data space whose data sharing infrastructure follows the principles of the IDS reference architecture.

Based on the use of interoperable connector technology, data providers and data consumers in different data spaces can share their data. By connecting to other data spaces using the Eclipse Dataspace Components (EDC) Connector, the MDS aims to promote a meshed data space in the mobility sector. Internal and external interoperability are important aspects of MDS development.

Decentralised set-up

The MDS implements a decentralised data infrastructure; that is, data are not stored centrally, but shared between participants using the connector infrastructure.

Architecture Data Exchange Infrastructure

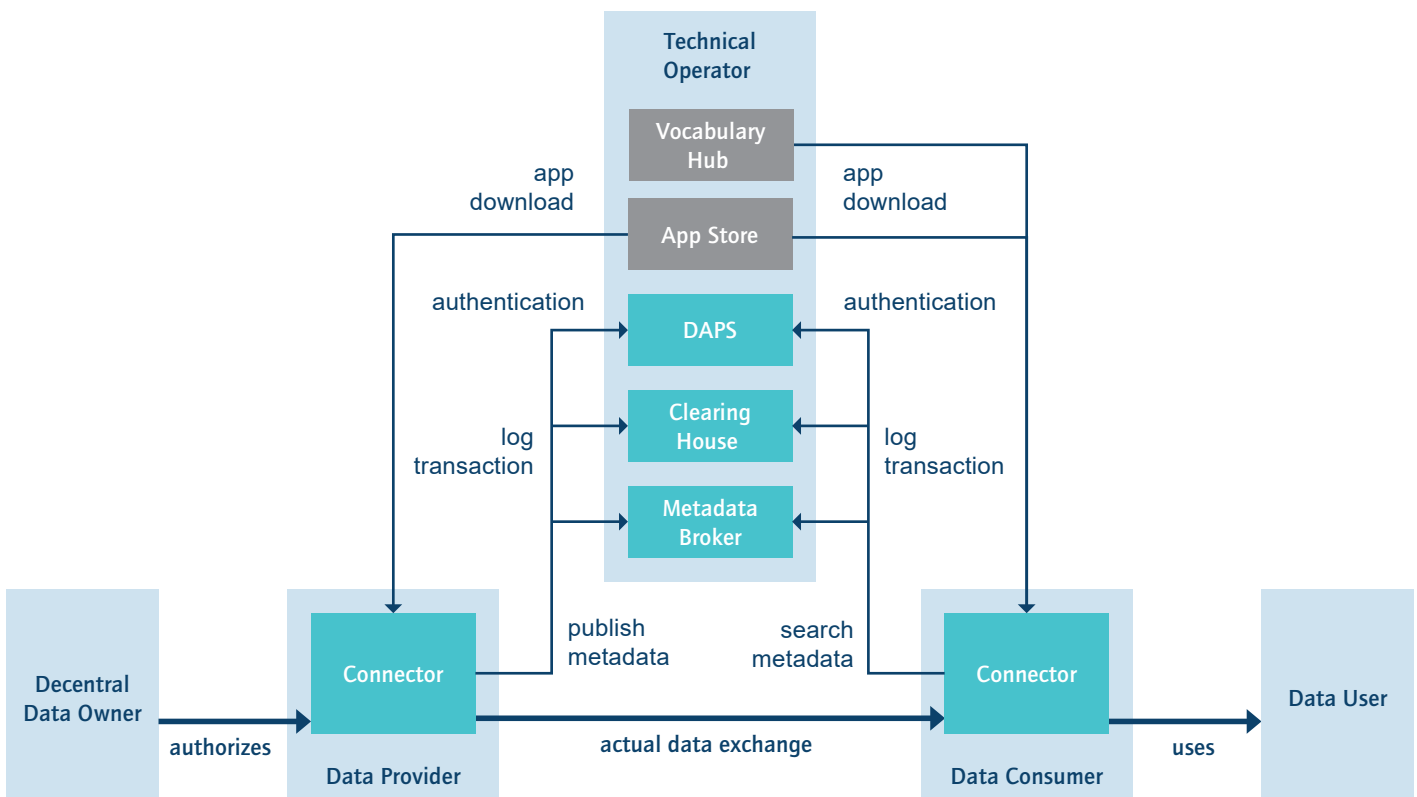


Diagram: Data Space - Data Exchange Architecture

Implementation of data space standards: The example of the Mobility Data Space (MDS)

Trust

As a neutral data intermediary, the MDS ensures the provenance and authenticity of the data source by subjecting all participants to a standardised certification process. Participants subsequently each receive their own token, which is assigned to their own connector, ensuring that they are using a certified connector. Technically, connectors ensure that the data bundle moves from the stated, certified source to the data recipient's connector. Data sharing between the connectors is manipulation-proof. No third party can access, divert or manipulate the transferred data.

Sovereignty

In the MDS, data providers themselves decide whether, with whom, and under which conditions they share their data. Data providers and users negotiate the specific usage policies of the shared data between themselves. Connectors allow the attachment of pre-agreed usage policies to a data bundle. This ensures that data providers always have full control over their data.

Transparency

The Metadata Broker, accessible on the MDS website, provides MDS users and partners with descriptions of the data offerings. This catalogue function forms the basis for matching data providers with data users.

Contact

Dr. Andreas Heindl
Project Lead Mobility Data Space
acatech – National Academy of Science and Engineering
Email: heindl@acatech.de

Jan Fischer
Hub Coordinator Gaia-X Hub Germany
Email: gaia-x-hub@acatech.de

Prof. Dr. Frank Köster
Steering Committee member Gaia-X Hub Germany
Email: gaia-x-hub@acatech.de