



Position Paper | Version 1.0 | March 2025

Establishing a Unified, Sovereign, and Open Digital Infrastructure:

A Vision for Telecommunica-
tion Providers



- Position Paper of members of the IDS Association
- Position Paper of bodies of the IDS Association
- Position Paper of the IDS Association
- White Paper of the IDS Association

Publisher

International Data Spaces Association
Emil-Figge Straße 80
44227 Dortmund
Germany

Copyright

International Data Spaces Association,
Dortmund 2025



Editor

Christoph Mertens (IDSA)

Cite as

Mertens C., Establishing a Unified, Sovereign,
and Open Digital Infrastructure: A Vision for
Telecommunication Providers, International
Data Spaces Association, March 2025

Authors & Contributors

Christoph Mertens (IDSA)
Lars Nagel (IDSA)
Sebastian Steinbuss (IDSA)
Guido Luijten (KPN)
Domenico Chirico (KPN)
Marc Titulaer (KPN)
Rutger Borst (KPN)
Akira Sakaino (NTT)
Masaru Dobashi (NTT)
Sven Löffler (T-Systems)
Christoph Schlüter-Langdon (T-Systems)
Aleksander Kelecevic (T-Systems)
Lena Matsela (T-Systems)

Table of Content

Executive Summary	3
Introduction	4
1. Interoperability	7
2. Enabling cross-ecosystem commerce – A perspective by NTT and T-Systems	12
2.1 Data ecosystems need to support global supply chains	12
2.2 Federated identity and trust management	13
2.3 Lessons learned – Blueprint for the next continent?.....	14
3. Sharing experiences on interoperability by KPN	16
3.1 Interoperability	18
3.2 Lessons learned	19
4. Conclusion and outlook: IDSA Telco Provider Community perspective on international interoperability frameworks	20
4.1 The transformative impact of telcos on data economy.....	20
4.2 Better solutions by listening to the customer	21

List of Figures

Figure 1: The European Interoperability Framework	7
Figure 2: 3-layer model of a data ecosystem's software stack	8
Figure 3: Technical interoperability from an IDSA perspective with some examples	10
Figure 4: Technical interoperability between two data spaces via protocols.....	11
Figure 5 Cross-jurisdictional data transaction scenario with federated identities and trust anchors	14

Executive Summary

This paper, written by the IDSA Telecommunication Provider Community, outlines the important role of telecommunication providers (telcos) in advancing global data space networks. With the strong position of telcos in the field of communication networks and development of international standards, they are in a good position to drive the development of service offerings in for data spaces. These data spaces are key enablers for trustworthy and sovereign data exchange across all industries, fostering innovation and digital transformation. Key points of the paper are:

Role of telcos in data spaces

- Telcos have a century long expertise in managing global networks and thus creating interoperability in secure and reliable communication and data ecosystems.
- The telecommunication infrastructure can be used as a foundation for the soft infrastructure required by data spaces, so data sharing can become as seamless as mobile telephony.

Lessons from GSM

- The Global System for Mobile Communication (GSM) is an example of how the collaboration of telcos can lead to standardized interoperability.
- The same principles applied to data spaces can help the success of the adoption and enable cross-border data sharing in a sovereign way.

The Interoperability framework

- The paper presents a multi-layer model for interoperability of data spaces, starting with a general view, addressing technical, semantical, organizational, and legal interoperability aspects.
- Technical layer is further detailed into a 3-layer model of a data ecosystem's software stack: Data space networks, data products, and super-apps.
- The data space networks layer is further decomposed into trust anchors, trust services, and data space core services including the Dataspace Protocol (DSP).

Case studies and international collaborations

- Concrete implementations of KPN, NTT Communications, NTT DATA, and T-Systems illustrate the practicability of data spaces.
- These collaborations showcase the importance of mutual recognition of trust anchors and a strong alignment on the other interoperability layers as well.

The IDSA Telco Provider Community aims at providing interoperable data space solutions on a global scale and is open to new members who want to support these efforts.

Introduction

Currently, only a low percentage of the data that companies have at their disposal is accessible to others. When more data becomes available, it can create value for organizations. Better access to data leads to innovative solutions. It is essential that the data owner has autonomy over their data and can determine with whom and under what conditions access to that data is granted.

Data spaces represent a secure means of providing data access, with the data owner in control granting full data sovereignty. Many organizations today are engaged in designing and developing standards and technologies to bring the concept of data spaces into practice. However, the application of required standards and technologies to operate or access a data space is a complex challenge for companies, especially for small and medium sized companies.

Telecommunication providers (telcos) have extensive experience in managing complex networks and developing international standards. Moreover, telcos have the expertise to develop user-friendly services that allow users to benefit from complex networks and applications with minimal integration effort. The goal of telcos in the IDSA telco provider community is to offer data space functionality as seamlessly as mobile telephony, enabling large-scale adoption of data spaces.

Telcos have been connecting people and businesses for over a hundred years. They are experts at creating networks that are reliable, interoperable, secure and easy to use. And they bring interesting qualities to the table which underline this point:

- **Connect the world:** Telcos run global networks that make communication possible, from phone calls to the internet. They follow strict privacy laws, like GDPR, to ensure they only provide connections and do not listen in on conversations or take a look at the contents of your data.
- **Keep things secure:** Telcos protect critical systems from cyberattacks and make sure networks stay up and running, even during emergencies.
- **Make technology affordable:** Telcos invest, develop and build open networks (like 4G, 5G, and fiber) that work for everyone, not just for a specific group. This helps lower costs and ensures many different people and businesses can use them.

This experience positions telcos as crucial players in building data spaces by offering data space services. Telcos have strategically positioned themselves at the nexus of global data connectivity and technological advancement across key sectors. Not only do they enable other industries by providing critical technological foundations and capabilities, but they also utilize these advancements within their own industry to enhance operational efficiencies and customer experiences. This dual role is crucial in boosting connectivity and the capabilities necessary for digital transformation in vital industries such as automotive, manufacturing, mobility, energy, and healthcare.

Lessons from GSM

The Global System for Mobile Communications (GSM) is one of the great examples of how telcos can solve big problems by working together. Before GSM, countries had different

mobile systems that couldn't connect. GSM created a single, shared standard that made it easy for people to use their phones across borders and extended its success beyond Europe.

The success of GSM also provides valuable lessons for developing data spaces. Data space creators can leverage advanced and specialized expertise, resources, and engineering capabilities to build data spaces. Collaboration with telcos can drive the success of data spaces in several ways:

1. **Collaboration and standards:** GSM worked because telcos and governments created a single, highly scalable system that worked across borders. For data spaces, telcos can help industries like healthcare, manufacturing, transport, and finance share data by creating clear rules and standards everyone can follow and to build cross-border interoperable data spaces for customers to use worldwide.
2. **Trust and security:** GSM used secure systems (e.g. SIM card) to protect calls and messages. Telcos can do the same for data spaces by ensuring shared data stays private and follows strict rules, like protecting personal information. This helps everyone feel safe using the system.
3. **Toolchains:** GSM brought together networks, devices, and services to make mobile technology work everywhere. Telcos can do the same for data spaces by offering things like fast connections, data storage, and tools to analyze data. This makes it easier for companies to share and use data.
4. **Business impact:** GSM opened new opportunities, like mobile internet and apps. In data spaces, Telcos can offer services like data analysis, ID wallets, data connectors and secure hosting, so companies do not have to build these on their own. This makes it cheaper and easier for smaller businesses to join and innovate.
5. **Keep improving:** GSM kept evolving (2,5G, 3G, 4G, 5G) to remain useful. Data spaces need to do the same by adapting to new technologies like AI and edge computing. Telcos can help drive these changes and make sure data spaces remain relevant and stay ahead of future challenges.

As key partners in the international data space ecosystem, telcos can play an essential role in addressing the challenge of creating interoperability across diverse industries in the data economy, to unlock the value of data.

The role telco providers played in the adoption of past technological pushes, like GSM, is a great example of how they can make new technologies accessible and usable for a broad range of companies and people. This is why the International Data Spaces Association (IDSA) founded the IDSA Telco Provider Community in 2024¹. The vision of this community is to establish a unified, sovereign, and open digital infrastructure that not only fosters innovation and drives digital transformation but also protects data sovereignty. We envision a future where scalable, secure, and interoperable services enhance critical applications and foster the development of innovative business models across various industries. By championing open standards, embracing sustainable technologies, and fostering collaboration among diverse stakeholders, we aim to develop a resilient, interconnected, and competitive digital data-economy.

¹ <https://internationaldataspaces.org/new-global-telecom-community-launched-by-idsa-a-step-towards-trusted-international-data-spaces/>

Key Strategic Pillars

1. **Enabling a Technological Foundation and Data Roaming:** Telcos manage critical infrastructure, including cell towers, data centers, network hardware and software, which are essential for advanced technology deployment and global data roaming. This infrastructure enhances sustainable, automated services and meets the growing demand for interoperability on a global scale.
2. **Supporting Seamless Deployment and Interoperability:** Through international partnerships and adherence to global standards set by organizations like the International Telecommunication Union (ITU), operators ensure flexibility and interoperability across different vendor networks. This facilitates seamless technological deployment within industries and guarantees international roaming without disruptions.
3. **Empowering Key Sectors with Advanced Technologies:** Telcos lead in integrating cutting-edge technologies and innovative business models into critical sectors. They enable smart manufacturing through IoT and AI, support the development of connected vehicles and smart transportation systems, manage distributed energy resources via smart grids, and enhance telemedicine with secure connectivity.
4. **Leveraging Network Capabilities for Industry Enablement:** Telcos will utilize existing initiatives to enable seamless access to enhanced telco network capabilities, such as those offered by 5G. These capabilities, exposed through APIs, are partly available in 4G but are significantly more powerful in 5G networks. They allow for the extraction of information from and configuration of the network, transforming operator networks into service enablement platforms. This on-demand, secure, and controlled exposure is key to delivering enhanced and service-tailored customer experiences in the 5G era.

As enablers of the data economy and architects of robust data ecosystems, telcos are indispensable to the evolution towards an interconnected and technologically sophisticated future. Their extensive involvement in infrastructure management, commitment to ensuring interoperability, and their role in enabling various sectors through advanced technologies underscore their foundational status in building a secure, connected, and reliable digital landscape. By fostering a trusted environment for data exchange and enhancing roaming services, they reinforce global connectivity and security. Dedicated to this strategic vision, we are at the forefront, driving the transformation that links current capabilities with future possibilities, thereby catalyzing the growth of a dynamic global data ecosystem.

This paper presents the achievements of the members of the IDSA Telco Provider Community and puts it into perspective of interoperability on a global scale.

Therefore, chapter 1 provides the reader with an introduction to interoperability in context of data spaces providing an interoperability framework on different levels of abstraction. This framework provides guidance and orientation to data space solution providers.

Chapters 2 and 3, give deeper insights into the existing work of T-Systems, NTT DATA, NTT Communications, and KPN making this publication practical relevant for users of data spaces.

Finally, chapter 4 provides the reader with a conclusion of this document and an outlook with a perspective for telecommunication providers and users of data spaces as well.

1. Interoperability

From a general perspective the topic of interoperability is elaborated on in the IDSA Rulebook² with a dedicated chapter called “Interoperability in Data Spaces”. Here the four main levels of interoperability are described as follows (cf. Figure 1):

- **Technical interoperability** refers to the physical and logical connections between systems and data sources, such as protocols, interfaces, and formats. This includes syntactic interoperability which refers to the structure and syntax of the data exchanged, such as schemas, models, and vocabularies.
- **Semantic interoperability** refers to the meaning and interpretation of the data, such as concepts, relationships, and ontologies.
- **Organizational interoperability** refers to the processes, policies, and governance of data sharing, such as roles, responsibilities, and agreements.
- **Legal interoperability** refers to the acceptance of legal equivalence of contracts and contractual clauses between different data ecosystems. These ecosystems can have differences on multiple dimensions, based for example on industry regulations, or national laws but also contractual statements with identical wordings might have diverging interpretations in different data ecosystems.”

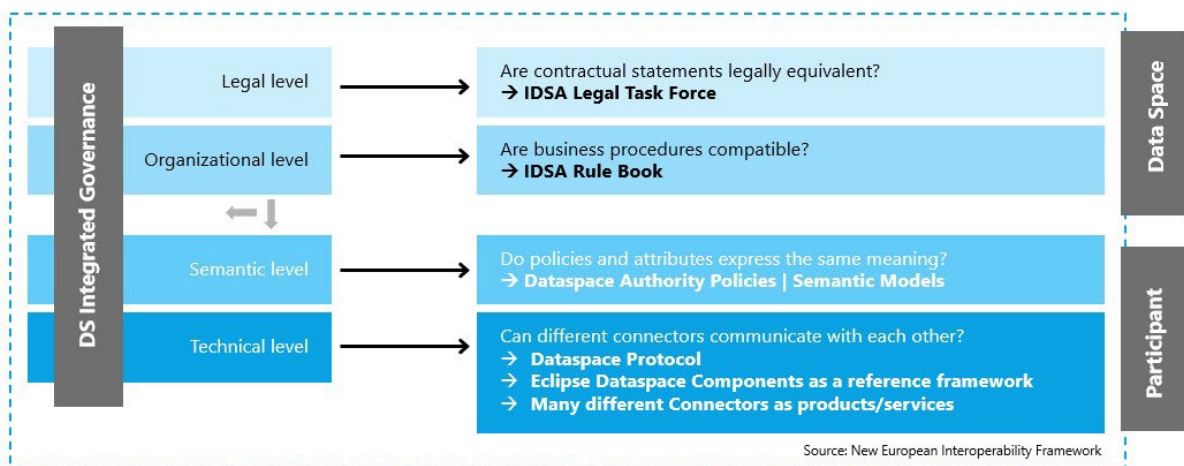


Figure 1: The European Interoperability Framework

As outlined in the IDSA Rulebook the four-layer model based on the European Interoperability Framework can be clearly mapped to the 5 facets of Interoperability as described in ISO/IEC 19941:2017 Information technology – Cloud computing – Interoperability and portability³. This international standard, which is currently under revision, is the common foundation for interoperability of services in international collaboration. Data Portability as key aspect in Data Spaces is defined subsequently in this standard as a combination of syntactical, semantic, and policy portability. ISO/IEC CD 20151 Information technology – Cloud computing and distributed platforms – Dataspace concepts

² <https://docs.internationaldataspaces.org/ids-knowledgebase/idsa-rulebook>

³ <https://www.iso.org/standard/66639.html>

and characteristics⁴ bases its work on interoperability in Data Spaces and between Data Spaces on ISO/IEC 19941.

When zooming into the technical layer, the 3-layer model of system software stacks reveals which is a helpful framework to orchestrate existing software stacks and identify remaining gaps in the IT infrastructure of companies who want to become a participant in data spaces. The following part will give better insights into this model.

Maturity of data ecosystems: A 3-layer model of the system software stack

Data ecosystems may seem complex, but technology has matured to simplify their adoption. Businesses can now seamlessly connect, leverage their capabilities, and stay focused on solving problems for faster results and measurable benefits.

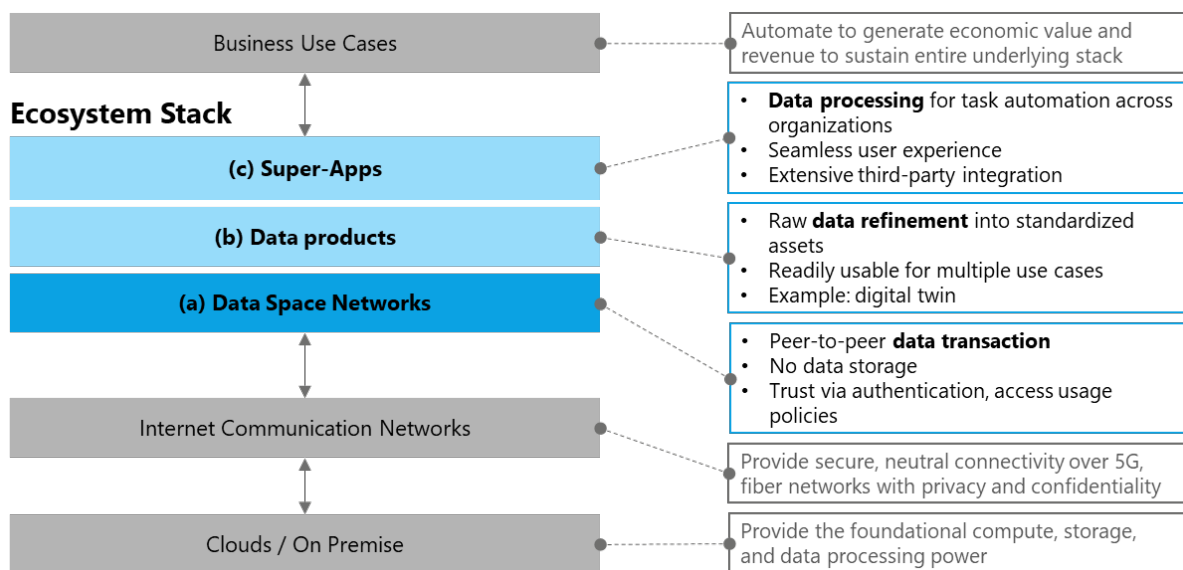


Figure 2: 3-layer model of a data ecosystem's software stack^{5,6}

Figure 2 illustrates how a data ecosystem seamlessly integrates into your existing IT landscapes by operating atop cloud or on-premises hardware and communication networks to support the automation of your business use case. Drawing on established conceptualizations of information systems⁷ – including the abstraction layers of the Open Systems Interconnection (OSI) model, a reference framework by the International Organization for Standardization (ISO/IEC 7498-1:19948)—it has been established how three

⁴ <https://www.iso.org/standard/86589.html>

⁵ Guggenberger, T. M., C. Schlueter Langdon, and B. Otto. 2025. "Data Spaces as Meta-Organisations. European Journal of Information Systems, January, doi:10.1080/0960085X.2025.2451250: 1–21, <https://www.tandfonline.com/doi/full/10.1080/0960085X.2025.2451250>

⁶ Schlueter Langdon, C., and K. Schweichhart. 2022. Dataspaces: First Applications in Mobility and Industry. In: Otto, B. et al. (eds.). Dataspaces – Part IV Solutions & Applications. Springer Nature, Switzerland: 493–511, https://link.springer.com/chapter/10.1007/978-3-030-93975-5_30

⁷ See for example: Turban, E., L. Volonino, G. R. Wood, and R. D. H. Watson. 2022. Information technology for management: Advancing sustainable, profitable business growth. Wiley 12th ed. Hoboken, NJ

⁸ ISO/IEC 7498-1:1994. Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model (Ed. 1, 1994; last reviewed and confirmed in 2000)

key layers can be distinguished^{5,6}. The three-layer model of a data ecosystem software stack consists of:

1. Dataspace network: Peer-to-peer data transactions
2. Data products: Raw data refinement
3. Super-apps: Data processing across traditional boundaries

This model further illustrates that, similar to the Internet, the network layer of the data space is industry-agnostic, whereas data products and applications are tailored to specific industries or even individual companies.

In addition to this 3-layer model Figure 3 extends or combines some of the layers to put a stronger focus on the data space itself. Compared to Figure 2 we see a more detailed view of the data space network layer differentiating between trust anchors, trust services, and data space core services. At the same time the two layers of data products and super-apps are combined into the data usage layer. The new view on the layers from bottom to top looks as follows:

1. Clouds/on-premise & internet communication network: Provides the required infrastructure for the soft services of data spaces
2. **Trust Anchors (Identity Management)**: Organizations need decentralized identity providers that allow for cross-border identity verification. This ensures that users and devices can be authenticated globally without compromising data sovereignty, enabling trusted interactions across different regulatory landscapes.
3. **Trust Services**: The implementation of trust registries is critical for establishing a verifiable and secure data-sharing ecosystem. Adopting industry-recognized standards, such as Gaia-X trust frameworks or the iShare trust framework, ensure that participants meet stringent security and compliance requirements.
4. **Data space core services**: Based on the trust infrastructure participants need to be enabled to negotiate data contracts based on access and usage policies. Also, discoverability of data and super-apps, providing of vocabularies and semantic models, and observability are elementary things which are provided on this layer. The required specifications for these functions are defined by the IDSA community.
5. Data usage: Data refinement and data processing
6. Business use cases: Generate economic value and revenue

By reinforcing identity and trust mechanisms, the data space network layer can overcome existing barriers to global data interoperability, fostering secure, trusted, and scalable data ecosystems.

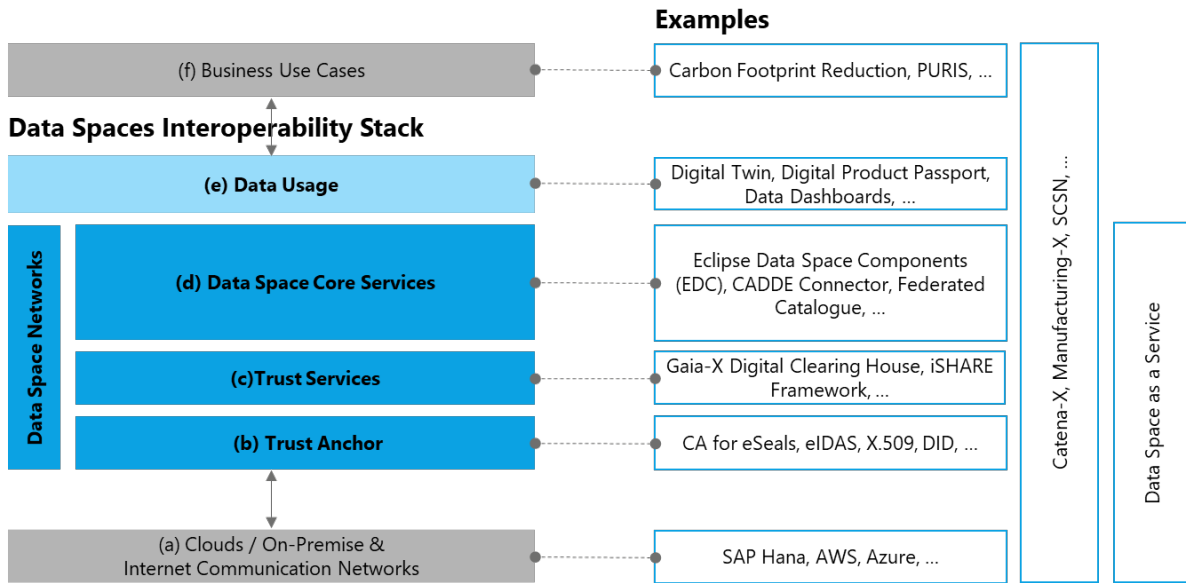


Figure 3: Technical interoperability from an IDSA perspective with some examples

On the right side of Figure 3 some examples for each layer are given. Of course, there are many more examples for each layer. In the case of the elements on the data spaces core service layer, connectors are a fundamental part of the solution, here with the Eclipse Data Space Components project (EDC) and CADDE connector. More examples can be found in the Data Connector Report created by IDSA⁹.

Also, on the side of the examples, two blocks cover almost all layers, one being about data space projects, like Catena-X, Manufacturing-X, or SCSN – the Smart Connected Supplier Network. An overview of further data spaces and use cases can be found on the webpage of the Data Spaces Radar¹⁰.

The other one, which is labeled with “Data Spaces as a Service” refers to technical infrastructure that is enabling data usage and business use cases but does not provide the usage-oriented solutions right away. It refers to those offerings which allow a company to join a data space without having to take care of the underlying infrastructure.

Two participants from the same or two different data spaces are only interoperable when interoperability is given on all layers of the stack. This requires international mutual recognition on the level of trust anchors (see also Data Free Flow with Trust – DFFT¹¹), the Decentralized Claims Protocol¹² on the trust service layer, the Dataspace Protocol¹³ for the data space core services, and one of the many existing protocols for the actual sharing of data. Even though the Dataspace Protocol (DSP) is located on the data space core service layer, it has an impact on the other layers as well by ensuring the right level of security, hardware trust, digital identities, credentials, and usage policies. The DSP leads to trust and

⁹ Data Connector Report: <https://internationaldataspaces.org/download/36320?tmstv=1741270071>

¹⁰ Data Spaces Radar: <https://www.dataspaces-radar.org/>

¹¹ DFFT: <https://www.oecd.org/en/about/programmes/data-free-flow-with-trust.html>

¹² Decentralized Claims Protocol: <https://projects.eclipse.org/projects/technology.dataspace-dcp/governance>

¹³ Dataspace Protocol: <https://internationaldataspaces.org/offers/dataspace-protocol/>

interoperability by defining the required schemas and protocols for cataloging the data and negotiating contracts as well as usage agreements.

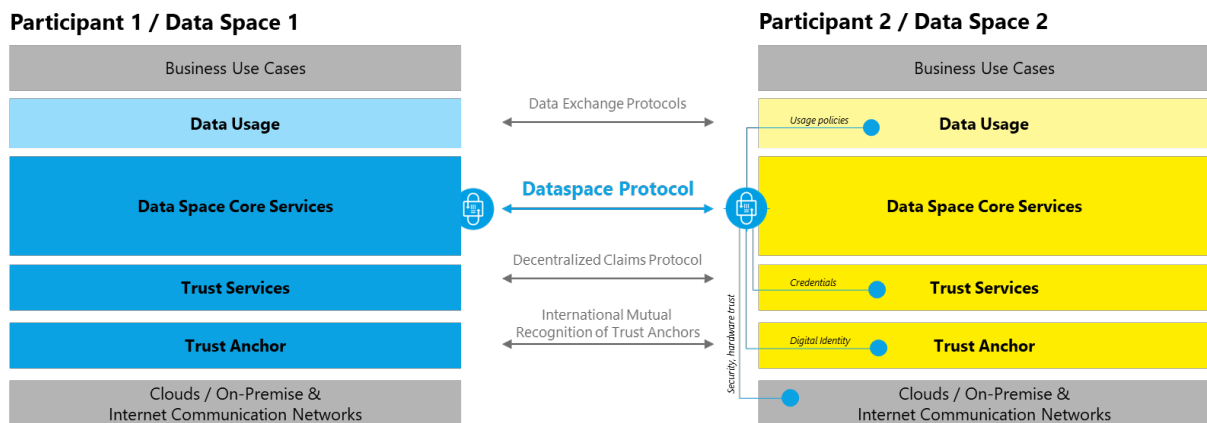


Figure 4: Technical interoperability between two data spaces via protocols

Solving interoperability on the technical layers at the end will not be enough. As the European Interoperability Framework makes clear, there are also other layers which must be considered: referring to semantic, organizational, and legal interoperability. As we can see in the data space network layer the fact that it also contains the negotiation of usage policies leads to overlays with the organizational and legal layer of the EIF. Aligning data-sharing policies with international regulations is essential for ensuring legal and regulatory compliance. Frameworks such as GDPR, CCPA, and industry-specific governance models provide the necessary structure to enable seamless, lawful data exchange across borders.

The following chapters will introduce the groundwork on solving the technical interoperability challenges that have been done by the IDSA Telco Provider Community and reflect on the lessons learned to generate impulses to improve the state of play.

2. Enabling cross-ecosystem commerce – A perspective by NTT and T-Systems

This chapter will reflect on the solution which was crafted jointly by NTT and T-Systems. First by presenting the given challenge and then drafting the solution for an international data exchange.

2.1 Data ecosystems need to support global supply chains

In a data ecosystem, the data space network layer enables data transactions across organizations. The data space network layer has matured to provide mechanisms for identity, trust, and governance, which ensure that data can be shared securely across organizations with data sovereignty so that a data provider remains in control of the rights to its data. However, today's supply chains are global in nature, crossing continents, which requires data transactions to follow across continents and jurisdictions.

Dataspace transactions are often compared with phone calls, where a provider is facilitating peer-to-peer communication with privacy and confidentiality protection. Telecommunication carriers provide solutions so that callers can verify each other's identities, ensure secure connections, and prevent unauthorized interception. The data space layer would need similar capabilities.

The ability to exchange data seamlessly across ecosystems and jurisdictions remains a major challenge for organizations. Differences in regulatory environments, varying standards for identity and trust, and technical fragmentation hinder the development of scalable, interoperable data-sharing solutions. Organizations that operate globally, such as logistics companies, financial institutions, or healthcare providers, struggle with fragmented regulatory landscapes and incompatible trust frameworks when attempting to share data across continents.

For example, consider a multinational company that needs to securely share supply chain data between its European and North American branches while ensuring compliance with both GDPR and U.S. data protection regulations. Without a unified framework for identity verification, trust management, and governance, achieving secure, sovereign, and compliant data exchange is nearly impossible.

Carriers can use their Digital Network Architecture and advanced security frameworks to facilitate trusted data exchanges within data spaces. Telecommunications operators play a pivotal role in this ecosystem by providing the foundational infrastructure required for secure data exchange. Their contribution includes enabling interoperability through standardized APIs, supporting trusted digital identities with identity verification and authentication services, and ensuring cross-border regulatory compliance through governance frameworks that align with global data protection regulations.

2.2 Federated identity and trust management

Identity and trust services are fundamental to the data space network layer, ensuring secure and sovereign data exchange. As described in the previous chapter, the data spaces network layer can be further broken down into three sub-layers: trust anchor, trust service, and data space core components. However, for data ecosystems to scale globally, current identity and trust mechanisms must be extended, and mutual agreements are required to support cross-continental interoperability.

To illustrate the impact of these solutions, consider a pilot initiative where a European-based automotive manufacturer collaborates with a North American supplier. The goal is to exchange real-time sensor data for predictive maintenance while adhering to EU data protection regulations and U.S. compliance standards. By leveraging a data space framework with integrated identity and trust mechanisms:

- The supplier and manufacturer authenticate their systems using a federated identity provider, ensuring that only authorized entities can access the shared data.
- Trust anchors validate each participant, providing digital certificates that confirm compliance with agreed-upon security and regulatory standards.
- Data usage policies embedded in smart contracts can enforce sovereignty rules, ensuring that the provider retains control over how its data is accessed and processed.

This approach mirrors the evolution of global telecommunications, where international roaming agreements allow phone users to connect seamlessly across networks while adhering to local regulations. Just as telecom operators provide the infrastructure for trusted, cross-border communication, they are now positioned to enable trusted cross-border data exchange within data spaces.

Exactly this scenario was the driving force behind the recent collaboration between T-Systems and NTT Communications, which partnered to introduce a data space test environment specifically designed for Japanese users. This strategic alliance merges the expertise of two digital service leaders, aiming to expedite the adoption of data spaces and ensure smooth interoperability between European and Japanese data ecosystems. High-level overview of the interaction of two environments can be seen on Figure 5.

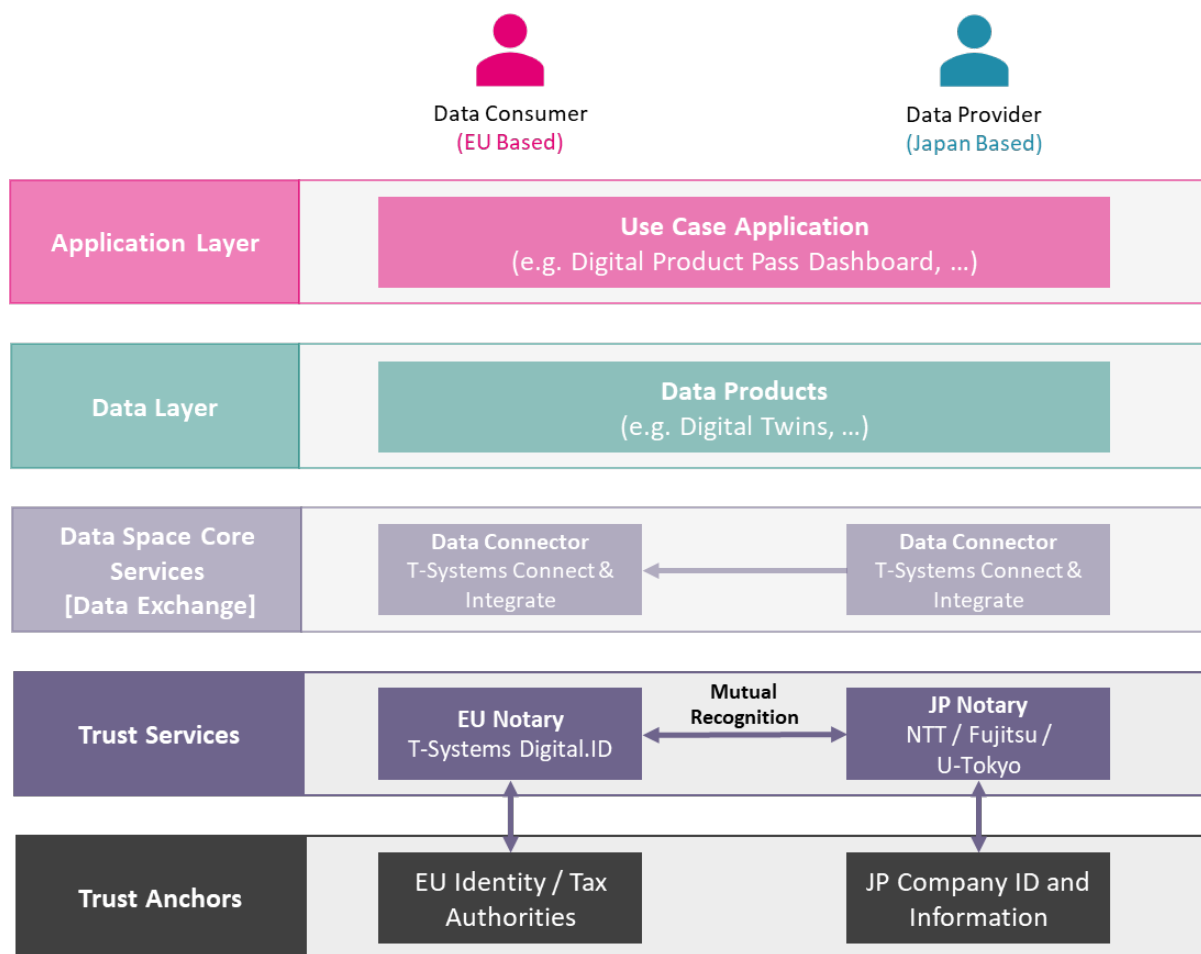


Figure 5 Cross-jurisdictional data transaction scenario with federated identities and trust anchors

This collaborative endeavor has thus become a foundational experimental “network of networks” that aims to achieve interoperability among diverse ecosystems, which are built on varying business practices, concepts, and specifications. By bringing together a wide array of international stakeholders, the initiative facilitates the convergence of different technological standards, ultimately driving the seamless integration of global data space ecosystems. In addition, and as part of realizing cross-regional and organizational federations, NTT DATA is collaborating with The University of Tokyo to conduct international connection experiments using data space connectors, such as the EDC Connector or the CADDE connector. NTT DATA and The University of Tokyo have already completed connection experiments with several countries in Asia and Europe.

2.3 Lessons learned – Blueprint for the next continent?

The challenge of enabling cross-continental data sharing is being addressed through advancements in the data space network layer, particularly in identity and trust services. Telecommunication operators, as key enablers of digital infrastructure, are instrumental in developing solutions that facilitate interoperability, regulatory compliance, and trusted data exchange. By adopting these principles, organizations can unlock the full potential of data-driven collaboration, fostering innovation across industries and jurisdictions.

Immediate Business Benefits: Closing the data space/trust anchor gap enables seamless global applications such as Digital Product Passports (DPPs), which rely on standardized data models for interoperability. With common trust frameworks and governance mechanisms in place, businesses can securely exchange product lifecycle data across industries and jurisdictions. As organizations and ecosystems drive global standardization of digital twin models, companies can leverage these frameworks for enhanced supply chain transparency, regulatory compliance, and circular economy initiatives. This fosters efficiency, innovation, and new data-driven business models across sectors.

Outlook: To fully realize these benefits, more trust anchors will be required to support scalable, cross-border, and multi-industry data spaces. The expansion of federated trust frameworks, digital identity solutions, and compliance mechanisms, e. g. enabled via the DSP, will be crucial in enabling trusted and frictionless data transactions. As governments, industry consortia, and technology providers continue to align on global standards, we can expect a broader adoption of secure and sovereign data-sharing ecosystems, driving new opportunities for collaborative innovation and digital transformation.

3. Sharing experiences on interoperability by KPN

KPN, telco incumbent in The Netherlands has been facilitating data exchange since 2018. At various abstraction levels, KPN facilitates the exchange of data. Below examples of applications:

- Data exchange platform Data Services Hub facilitates governance on data sharing. Sovereign and secure data sharing, designed to execute the exchange of high volume (streaming) data between organizations.
- Hosting central components of a federated data spaces:
 - SCSN – hosting central IDSA components such as the DAPS (Dynamics Attribute Provisioning Service) and SCSN specific address book.
 - DVU – hosting central iSHARE components such as the Participant Register, also known as iSHARE Satellite.
- Providing Federated Identity & Access Management to enable organizations to comply with the Data Act regulation.

The role of KPN differs in each of the abovementioned data sharing activities. Hereafter, some additional context about the different roles.

Data Services Hub platform

The KPN Data Services Hub is a platform-as-a-service that enables the exchange of (streaming) data. The cloud agnostic platform is multi-tenant, secure by design and developed to safeguard data sovereignty to data owners.

The KPN Data Services Hub simplifies the way data is shared between organizations, people, and 'things'. The platform allows organizations to connect data sources, devices, and systems that traditionally worked separately and can process millions of simultaneous connections. The Data Services Hub has functionalities that make it easy for both data holders and data consumers to exchange data. It offers a rich set of connectors for connecting data sources on one end and data consumers on the other. Additionally, the Data Services Hub has a powerful authorization mechanism, allowing the data holder to specify which data consumer can access each data source. Thus, the data holder always remains in control of what happens to their data sources. With registration and authorization via the Federated Identity & Access Management (FIAM) service of KPN based on the iSHARE Trust Framework, it is possible to connect to data sources on the Data Services Hub.

Smart Connected Supplier Network data space

The Smart Connected Supplier Network (SCSN) focuses on supply chains in the manufacturing industry, where success depends on exchanging large amounts of detailed information accurately and in an efficient manner. SCSN simplifies data sharing in the supply chain by automatically processing data between ERP systems. Some other benefits include:

- Automating manual processes saves labor and reduces the risk of errors.
- Standardized semantics ensure easy and error-free interpretation.
- Only one connection is needed. An SCSN participant registers once with an SCSN Service Provider to exchange information with all affiliated companies.

- Data sovereignty. The participant decides which data is shared with whom.

TNO, together with industry companies, developed and implemented the SCSN data sharing solution based on the IDSA reference architecture. It is now used daily by over 300 organizations. Due to this regular use, affiliated organizations rely on the SCSN Data Space and expect reliable and robust services. To ensure proper governance, an independent management organization was established: the Smart Connected Supplier Network Foundation. The Foundation contracted KPN to provide the technical (cloud) infrastructure for hosting the core components of the SCSN Data Space. This agreement gives participants a reliable technical foundation to scale. SCSN is an operational data space in which a delicate balance between day-to-day stability and fit for the future technology and functionality is important. Above all, the participating companies must be able to rely on optimal availability of the technical infrastructure. That does not mean, however, that there is no consideration being given to the future architecture of SCSN in the meantime.

Datastelsel Verduurzaming Utiliteit data space

Datastelsel Verduurzaming Utiliteit or DVU, was initiated by the Dutch Enterprise Agency. Buildings need to be made more energy-efficient to meet the climate goals of the Climate Agreement. This data system aims to provide faster and better insights into the actual energy use in commercial buildings in the Netherlands. The data system enables the structural comparison of energy consumption per square meter for different types of buildings. It is also being developed to make this data more accessible and shareable in a secure way. DVU is fully federated in terms of interface standards but starts with offering a combination of data reporting insights, an authorization register, and a registration process. DVU is built on the Trust Framework of iSHARE and the Participant Register is hosted by KPN.

Federated Identity & Access Management (FIAM) service

KPN introduces the Federated Identity & Access Management (FIAM) service to address the need of organizations in the role of data holder to become compliant with the Data Act. The Data Act mandates organizations to allow access to data to third parties after authorization provided by the data owners. FIAM provides compliance in an efficient manner, while ensuring the autonomy and privacy of the data owners. Furthermore, FIAM supports participation in a federative data ecosystem, making data sharing beyond current scopes more streamlined and effective. The FIAM service offers several key functionalities:

1. Identification and registration of third-party details.
2. Logging data owner authorizations for third-party data access.
3. Verification of third-party data access validity.
4. Monitoring and reporting of data request volumes and frequencies.
5. Publication for data exchange API endpoints discovery for third-party access.

The service offering is designed to be flexible and easy to use, so it becomes much less cumbersome for data holders to comply with Data Act regulations while being flexible to adapt to customer specific requirements. KPN's role as a Qualified Trusted Service Provider (QTSP) and its experience with the Data Services Hub, further strengthens the reliability and scalability of the FIAM service, making it a vital component in delivering high-quality data space solutions. By leveraging the iSHARE Trust Framework, FIAM enhances interoperability between data spaces. iSHARE provides a standardized framework that ensures compliance

and therefore provides trust and interoperability among participants within and between different data spaces.

In summary, KPN's FIAM service empowers businesses to navigate the complexities of the Data Act, fostering a secure, sovereign and collaborative data-exchange environment that enhances operational efficiency and innovation.

3.1 Interoperability

Testbed SCSN

There is significant progress being made on the technical building blocks for data spaces, which aligns with the current adoption phase of the European data strategy. KPN is working with TNO to explore the right technology stack for the next phase. Therefore, the parties have set up a testbed to test various building blocks. The goal of the testbed is to validate new functionality together with the participants in SCSN.

The testbed includes components based on the Dataspace Protocol. The Dataspace Protocol has been developed by IDSA to facilitate interoperable data sharing between entities governed by usage control and based on Web technologies. In addition, KPN and TNO investigate to what extent the iSHARE trust framework is suitable for SCSN.

Today, SCSN already offers value to its participants in the manufacturing industry on a daily basis and at the same time there is still a lot of potential for new use cases and new participants within the sector. In the future of SCSN, participants aim to establish cross-sector relationships. Making the network interoperable with other networks could be a suitable feature for the SCSN network and a natural step in its development.

The iSHARE Trust Framework

- iSHARE Foundation is a non-profit organization that provides and maintains a Trust Framework for data spaces. Data spaces utilizing the Trust Framework employ the Participant Registry for participant registration and discovery. Data sovereignty and trust is facilitated by the Authorization Registry providers and built upon Identity providers across Europe.
- The iSHARE framework ensures legal interoperability, giving parties real assurance that liability for breaches of confidentiality and usage licenses is well secured for everyone within the framework. The framework focuses on identification, authentication and authorization, using open standards such as OAuth 2.0, OpenID Connect, JSON Web Tokens (JWT), and eIDAS certificates.

Key benefits include:

- **Interoperability Across Data Spaces:** iSHARE supports trusted data sharing between multiple data spaces, facilitating both intra- and inter-data space interoperability. Achieving inter-data space interoperability is very important as this brings benefits to participants (easy onboarding into different data spaces, an option to create new value by combining data/insights) and to service providers (convergence in data space building blocks, improved maturity and scale).

- **Data Sovereignty:** Participants retain control over their data, deciding who can access it and under what conditions, thereby ensuring compliance with privacy regulations and internal policies.
- **Enhanced Security:** iSHARE ensures that only authorized parties can access specific data, maintaining confidentiality and integrity.
- **Trust and Compliance:** Through a structured certification process, iSHARE builds a network of trusted partners, reducing risks associated with data sharing and ensuring compliance with legal and regulatory standards.

The iSHARE Trust Framework offers a strong and practical way to build trust in data spaces. KPN has gained significant experience with the iSHARE Participant Register.

3.2 Lessons learned

The strength of a data space, a community without a dominant party, also requires extra attention to certain elements. Participating parties have the right insights to determine which functionalities are desired. The challenge is facilitating change within an ecosystem of parties that rely on the value proposition of a data space. These tasks are often assigned to a data space authority. It is important that this authority has sufficient resources, knowledge and mandate to initiate and organize such structural development. One consideration is that the authority outsources certain tasks to specialized parties.

Access to data is essential for business processes. Data spaces will become increasingly important for organizations in providing access to data. Therefore, it is logical that the technology stacks of data spaces are stable and reliable. With the Data Services Hub, KPN has been focusing for years on delivering high-quality data processing infrastructure. Providing access to data sources is still a primary service of KPN. In recent years, it has become clear that the control plane which is covered by the DSP is just as important. That is why KPN has invested heavily in the iSHARE Trust Framework and is now developing services for Data Act compliance.

KPN aims to deliver an enterprise-grade, secure and scalable solution that simplifies access to a federated data exchange. KPN has identified several opportunities of adopting data space technologies in key areas:

1. **Enhancing integration:** There is significant potential to create seamless interoperability between new technologies and existing infrastructure and KPN solutions, ensuring increased added value, seamless customer experience and minimizing disruptions.
2. **Building confidence:** By focusing on testing and collaboration, telecom operators can help emerging technologies prove their reliability and scalability for large-scale deployments while fostering strong partnerships with innovative initiatives.
3. **Strengthening regulatory and security compliance:** Emerging technologies offer a chance to shape solutions that provide new functionality. This new functionality must fit with the regulatory framework the telco operates in and must meet stringent security standards.

4. Conclusion and outlook: IDSA Telco Provider Community perspective on international interoperability frameworks

This paper presented different layer models for the topic of interoperability in data spaces starting with a general interoperability model which points to different kinds of interoperability – technical, semantical, organizational, and legal interoperability. All these levels must be addressed to be fully interoperable within and between data spaces.

With the ecosystem stack this paper presents a detailed view of the technical layer pointing to data space networks, data products, and super-apps as fundamental aspects for technical interoperability. Furthermore, we decompose the data space network layer even further into the data spaces interoperability stack by differentiating between trust anchors, trust services, and data space core services. Besides pointing to different examples for each layer we establish a view which clarifies how interoperability between two participants of the same or two different data spaces can be established and by this we create a coherent view on required technical components and protocols that are required to reach full interoperability on international scale – with the **Dataspace Protocol (DSP)** as important contribution by the IDSA community.

It is important for telecommunication providers around the world to work together and openly discuss the various aspects of interoperability – architectures, protocols, governance rules and trust frameworks for international data spaces are all important in this debate. Telecommunication providers need to consider all the presented aspects in their market offers to avoid the next level of data silos. This ensures that solutions are both practical and cost-effective and thus deliver real benefits for customers. The existing solutions and demonstrations by KPN, NTT, and T-Systems are presented in this paper and reflect on the lessons learned from each perspective.

Furthermore, the telco providers ensure benefits for the customer. The solutions developed are not merely interoperable for the sake of interoperability but also reduce costs at the data space participant side. By lowering the entry barrier to data spaces companies can benefit from the network effect – the more participants the better the data ecosystem. These benefits combined with the aspect of data sovereignty for those who share their data will lead to a flourishing data economy that overcomes the issue of data scarcity for application fields, like artificial intelligence or use cases like carbon footprint reduction.

The vision of the **IDSA Telco Provider Community** is to create interoperable solutions on a global scale by following the developed interoperability framework.

4.1 The transformative impact of telcos on data economy

Telecommunication providers should consider concrete methods, build data exchange network systems and conduct joint tests to ensure interoperability on international scale for data space participants. They play a key role to operate data spaces efficiently and securely, while not being the only potential provider of required infrastructure. Other technical

solutions providers are well equipped to provide services on the presented interoperability layers, which is leading to a whole variety of data space as a service offers.

To foster this discussion IDSA has founded the IDSA Telco Provider Community and started preparations for required actions together with KPN in the Netherlands, T-Systems in Germany and NTT in Japan with further telcos joining the community in 2025. IDSA will facilitate productive discussions in the community to achieve international interoperability based on the presented interoperability model, the IDS Reference Architecture Model, and the DSP as key enabler of interoperability in the data space core service layer. The work that has been done in the field of interoperability of data space offerings is presented in this paper.

This community is looking forward for many other telco carriers, including China Telecom, to join the discussion and work, to elaborate on additional perspectives of how data is structured and exchanged in a sovereign way in other parts of the world.

The collaboration of telco providers, further solutions providers, and users of data spaces will have a positive and transformative effect on global data economy.

4.2 Better solutions by listening to the customer

For companies who are interested in the application of the services described and who want to leverage the benefits, IDSA has founded the **IDSA User Group**¹⁴. To understand the topic of data spaces not only from the technical side, we welcome data space users to join the discussion from a different perspective. And the users-perspective will help to accelerate the discussion and identify requirements for improvements of international interoperable data spaces. Therefore, IDSA invites people to participate in the IDSA User Group.

The Telco Provider Community will work closely with the IDSA User Group to plan an international joint test project enabled by telco providers together with the users implementing real market requirements. And by this, we create a fruitful environment in which the existing data space services can mature and where the needs of the user will give the orientation for further development while at the same time business benefits for the user side are monetized.

You can read more about the business-related topics in the publication “Data Spaces Business Models”.¹⁵

¹⁴ <https://internationaldataspaces.org/idsa-user-group/>

¹⁵ <https://internationaldataspaces.org/download/49662/?tmstv=1741317225>

CONTACT

INTERNATIONAL DATA SPACES ASSOCIATION

Emil-Figge-Str. 80
44227 Dortmund | Germany

phone: +49 231 70096 501
mail: info@internationaldataspaces.org

WWW.INTERNATIONALDATASPACE.ORG



[@ids_association](https://twitter.com/ids_association)



[international-data-spaces-association](https://www.linkedin.com/company/international-data-spaces-association)