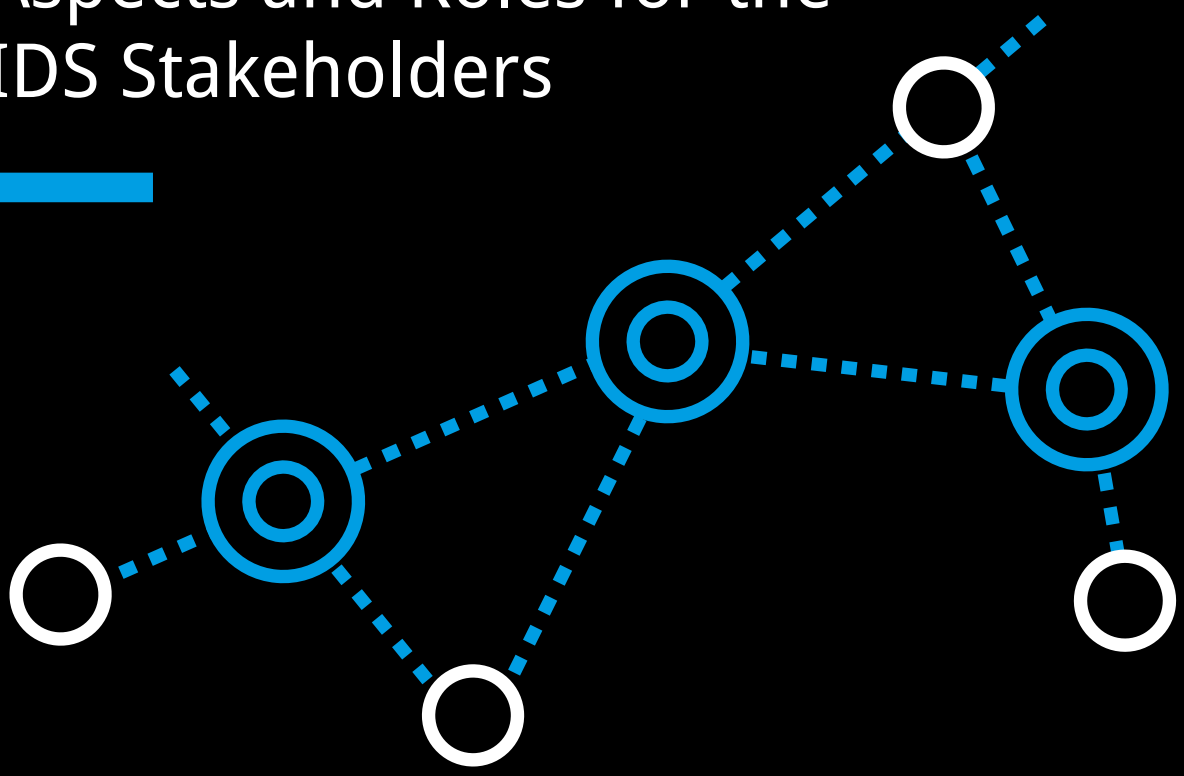
INTERNATIONAL DATA SPACES ASSOCIATION

Position Paper | Version 0.1 | August 2021

Governance for Data Space Instances

Aspects and Roles for the IDS Stakeholders



- (●) 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

TNO innovation for life

Publisher

International Data Spaces Association
Anna-Louisa-Karsch-Str. 2
10178 Berlin
Germany

Editor

Sebastian Steinbuss,
International Data Spaces Association

Cite as

Steinbuss S. (2021): Governances for Data Space Instances – Aspects and Roles for the IDS Stakeholders. International Data Spaces Association.
https://doi.org/10.5281zenodo.7376587

Authors & Contributors

Harrie Bastiaansen (TNO)
Mike de Roode (TNO)
Anil Turkmayali (IDSA)
Sebastian Steinbuss (IDSA)
Olaf-Gerd Gemein (OASC)

Contents

1 Introduction

1.1 The European Data Strategy: towards federated data spaces

"Data is a key strategic asset in our times.
Data sharing is a means for valorization".

Sharing of organizational data can optimize business ecosystems and supply chains, help the advancement of research, improve the functioning of government agencies and spur the economic and strategic position of countries and even regions.

Therefore, data and data sharing are key ingredients that are clearly on the radar of the European Commission. The commission has recently released its European Data Strategy [1], paving the way for data sharing in accordance to the European values. Moreover, its release of the Data Governance Act [1] and the additional input sought on data spaces through OPEN DEI [3] point to the importance that the EU attribute to data and data sharing for our society and economy.

Many specific data sharing initiatives already exist. These are often focused on a specific sector or domain. Additionally, also several generic data sharing initiatives exist such as GO FAIR [4], iSHARE [5] and IDS. They provide overarching principles, standards or functionalities which can be used in new and existing data sharing initiatives.

In view of the ambition as expressed in the European data strategy, the goal is to build upon these existing data sharing initiatives to strengthen them in unlocking the value of data sharing in and across their domain. A federation of data spaces is aimed for. A similar ambition is currently pursued by the Data Sharing Coalition [7].

1.2 Data spaces in the context of the European Data Strategy

Data spaces are key to realising the European data strategy. As stated in the European Data Strategy [1]: '*Data spaces should foster an ecosystem (of companies, civil society and individuals) creating new products and services based on more accessible data*'.

A data space has been defined by the European OPEN DEI initiative [6]as a '*decentralized infrastructure for trustworthy data sharing and exchange in data ecosystems based on commonly agreed principles*' and providing three types of building blocks

1. building blocks such as data platforms, providing support for effective data sharing and exchange as well as for engineering and deployment of data exchange and processing capabilities;
2. building blocks such as data marketplaces, where data providers can offer and data consumers can request data, as well as data processing applications;
3. building blocks ensuring data sovereignty, i.e., the ability for each stakeholder to control their data by making decisions as to how digital processes, infrastructures, and flows of data are structured, built, and managed, based on an appropriate governance scheme enabling specification of terms and conditions.

Within a data space, participants can share (potentially) sensitive data in a trusted and secure manner.

1.3 Role of IDS and IDSA

IDS and the IDSA have a major role to fulfil in the development and deployment of data spaces, and the federation and interoperability thereof. As such, the work of IDSA is key for realizing the European data strategy and the full exploitation of the potential of data sharing.

As indicated in the previous sections, it is to be realized that the role of IDS and IDSA is to be fulfilled (1) within the broader landscape of existing data sharing initiatives and (2) the ambition of a federation of interoperable data spaces. This implies that IDSA has to consider (the governance of) its development and deployment initiatives in the broader context of both:

1. striving for intra data space interoperability such that IDS can be positioned for being smoothly embedded and providing a gradual migration path within a single data space instance or data sharing initiative, and
2. preparing for inter data space interoperability between multiple data space instances or data sharing initiatives to pave the way towards the federation of interoperable data spaces as pursued by the European data strategy.

As such, also the Data Governance Act [1] recommends both an intra data space (domain) governance authority and an inter data space (central) governance authority. As cited from [6],

'The recently proposed Data Governance Act [1] confirms the notion of a governance structure constituted by multiple entities. For European data spaces, it is recommended to have a (domain) governance authority for each data space and a central governance authority overseeing all aspects in connection with interoperability of data spaces, i.e. the de-facto 'soft infrastructure'. This central authority will interact with all data space specific authorities'.

It is to be realized that a data space is more than merely its technical capabilities and the interoperability thereof. The (twelve) building blocks of a data space have been identified and described in the OPEN DEI position paper on design principles for data spaces [6]. Similarly, systematic approach for addressing the various levels of data space capabilities and the interoperability thereof is provided by the new European Interoperability Framework [8] as developed by the European Commission. The framework distinguishes four interoperability levels: technical, semantic, organizational and legal interoperability under overarching integrated governance. Each of these levels needs adequate governance to realize both intra and inter data space interoperability.

1.4 Goal of this report: governance on development and deployment

The goals of this report are to identify the topics requiring adequate governance in the broader context of both intra data and inter data space interoperability as described in the

previous sections and to detail the associated roles and responsibilities for the main IDS-stakeholders in jointly providing the governance for developing and deploying data space instances.

As such, this report extends upon the OPEN DEI data space design principles [6], the IDS Reference architecture Model [10] for data spaces and the IDSA Rule Book [11].

1.5 Report structure

The chapters in this report subsequently address:

- the governance challenges on both intra data space interoperability and inter data space interoperability for developing and deploying a federation of interoperable data spaces (chapter 2),
- the IDSA integrated governance approach for both intra data space interoperability and inter data space interoperability, for the main IDS stakeholders (chapter 3), and
- the concluding remarks (chapter 4).

In addition, the report has an appendix containing a glossary for the terms as used in this report.

2 Topics for intra and inter data space governance

As stated in the introduction, there is an important role to fulfill by IDSA and the main IDS-stakeholders in jointly providing the governance for developing and deploying data space instances in the broader context of

1. the introduction of new or migration / evolution of existing data sharing initiatives, i.e. intra data space interoperability, and
2. the embedding thereof within the European ambition of a federation of interoperable data spaces i.e. inter data space interoperability.

To fulfill this role adequate governance by IDSA and the main IDS-stakeholders on a range of development and deployment topics. These topics are identified and elaborated in this chapter. For identifying the governance topics, the following section lays the foundation by considering the data space structure in more detail and describing the scope of both the intra and inter data space interoperability perspective. The section thereafter elaborates the topics requiring adequate governance for both these perspectives.

2.1 Data space structure: building blocks, functional levels and interoperability

2.1.1 Data space building blocks: authority, data processing and data sharing

The OPEN DEI design principles for data spaces [6] identify and describe a soft infrastructure stack with 12 building blocks that provide the basic capabilities for a data space. How these are mapped on a data space structure is depicted in Figure 1.

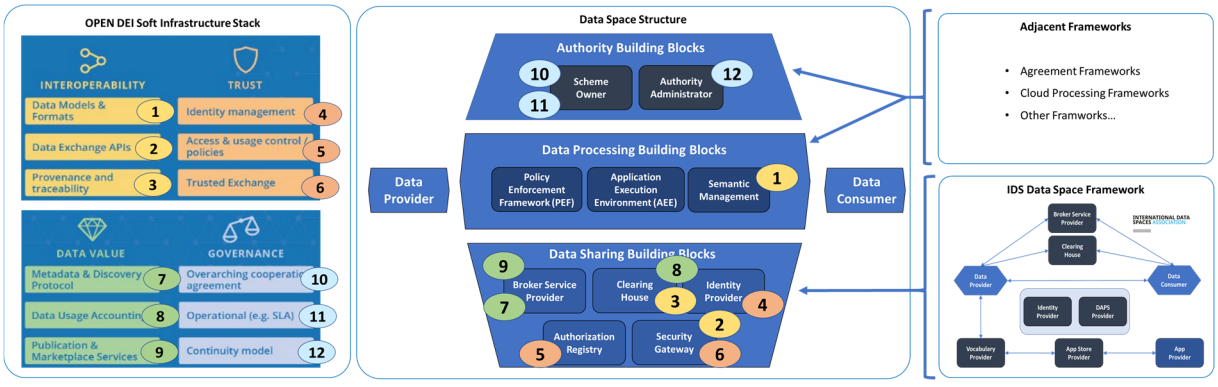


***Figure 1**. Data space structure (m) including mapping of the 12 building blocks in the OPEN DEI soft infrastructure stack (l) and the constituting capabilities provided by the IDS data space framework and adjacent frameworks (r).*

The figure shows that the structure of a data space has a categorization of the building blocks into 'data space authority' building blocks, 'data processing' building blocks and 'data sharing' building blocks:

1. The data space authority building blocks provide the functions associated to the 'agreement framework' as depicted in Figure 1, which are sometimes also referred to as the 'trust framework'. The scheme owner provides the data space governance framework for managing the commonly agreed upon procedures within the data space, e.g. on legal agreements and, conditions certification, applicable standards and architecture and the certification policy. The 'data space authority administrator' provides the supporting functions to manage participating entities in the data space, including the onboarding and accession criteria and processes, management of the identities and attributes of participants.
2. The data processing building blocks provide edge processing (computing) capabilities for data apps, e.g. for data apps for managing semantics (format conversion or mapping) or for locally executing AI-algorithms based on Federated Learning or secure Multi-Party Computation. Cloud integration could provide the manner for implementation thereof, with GAIA-X potentially being a good match. Moreover, data control and data sovereignty are enabled through integration with the Policy execution Framework (PEF).
3. The data sharing building blocks provide the hardware and software components to enable controlled data sharing with data sovereignty between data providers and data consumers. They are based on the roles as defined in the IDS Reference Architecture Model (IDS RAM [10], [12]).

The glossary for the building blocks as depicted in the figure is provided in appendix A.

This structure of a data space reflects the role of the (IDS) data space framework approach in relation to the already broadly used data sharing agreement framework approaches emerging (cloud) processing framework approaches, as depicted in the right side in Figure 1:

1. In a *data sharing agreement framework* approaches, a joint (legal) data sharing agreement is agreed upon between data providers and data consumers, possibly including an authorization function for defining and enforcing usage contracts on the specific access and usage control conditions for individual data sharing transactions. An agreement framework may be used within a single instance of data space, for example within a sector.
2. A *data space approach* provides value adding functions as part of a broader system approach including the supporting functions for data sharing transactions and for data processing and enrichment functions. IDS is currently gaining major European interest as data space approach.
3. In a *data processing framework approach*, (cloud) processing services are offered for outsourcing (large) data processing tasks, providing adequate levels of data sovereignty.

The agreement framework approach, the data space framework approach and the data processing framework approach for a major part pursue similar goals in realizing a federated data sharing architecture with a 'full-stack' of data control and data sovereignty capabilities. Nevertheless, these frameworks are complementary. An agreement framework's main focus is on the rules that data sharing partners agree upon. The data space framework adds features for data sharing support and functional extensibility, still requiring a firm grounding in

legal agreements. The data processing framework provides the needed data processing capabilities.

As example implementations, the iSHARE agreement framework approach [5] that provides the data space authority building blocks, providing an overarching scheme for managing onboarding, legal agreements and agreements for data access authorization. For the data processing framework, the current European GAIA-X initiative [9] may offer major potential.

2.1.2 Data space functional levels and relation to OPEN DEI soft infrastructure stack

An approach to systematically address and govern the interoperability challenges is provided by the new European Interoperability Framework as developed by the European Commission [8] and depicted in Figure 2.

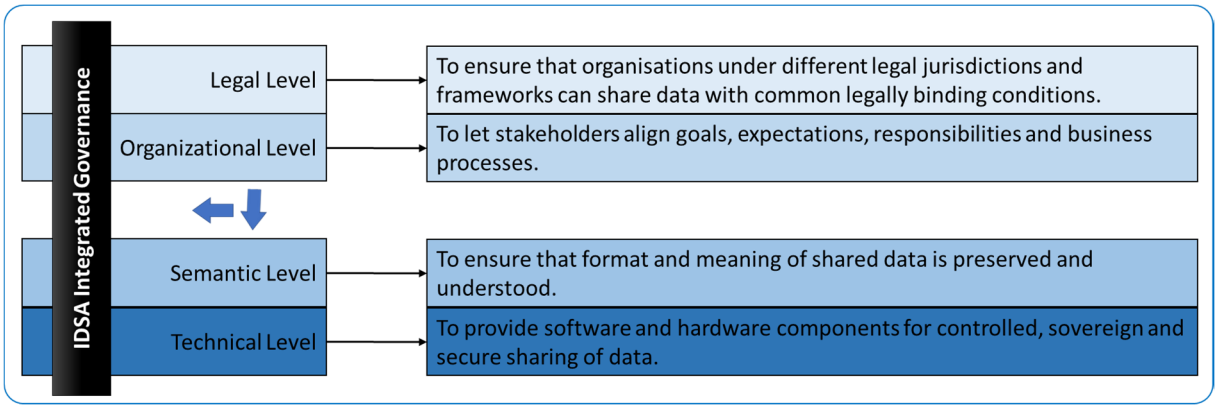


***Figure 2**. Layered functional model as aligned with the New European Interoperability Framework [8].*

As Figure 2 shows, the framework distinguishes four functional levels under an overarching integrated governance approach:

- Technical level, to provide software and hardware components for controlled, sovereign and secure sharing of data.
- Semantic level, to ensure that format and meaning of shared data is preserved and understood.
- Organizational level, to let stakeholders align goals, expectations, responsibilities and business processes.
- Legal level, to ensure that organizations under different legal jurisdictions and frameworks can share data with common legally binding conditions.

For each of the four functional levels, the topics to be governed are identified in the following section. The next chapter elaborates the governance thereof as part of the overarching IDSA integrated Governance approach.

2.1.3 Development lines: intra and inter data space interoperability

For the governance on the topics as identified in the previous section, a distinction is made on their applicability for two development lines for data space instances:

- *Intra data space interoperability,* between the data space authority, processing and data sharing building blocks within a single data space instance.
- *Inter data space interoperability,* between multiple data space instances at each of the functional levels as distinguished in the framework depicted in Figure 2.

Both intra and inter data space interoperability development lines are illustrated in Figure 3.

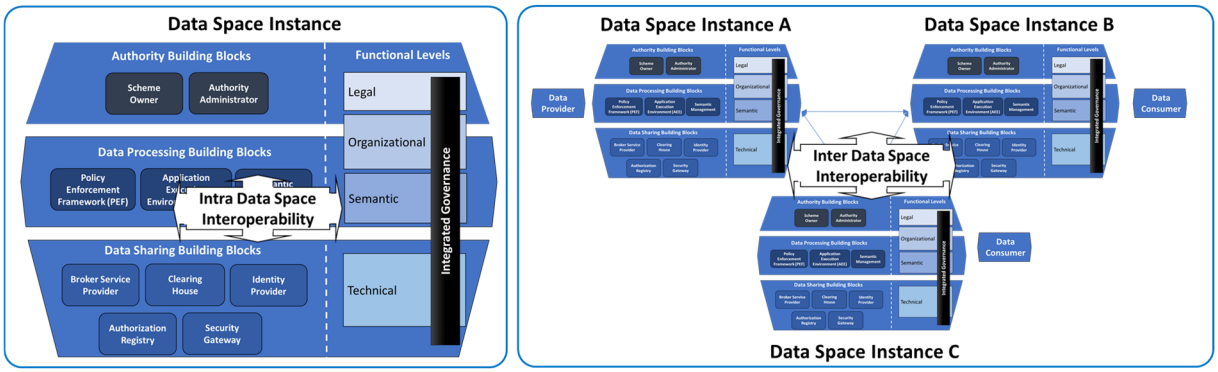


***Figure 3**. Intra data space interoperability (l) and inter data space interoperability (r) development lines.*

2.2 Topics requiring governance

To enable interoperability between data spaces, each of the functional levels as indicated in Figure 2 contains topics that require adequate governance. For each of the levels, these topics are identified in the following paragraphs subsequently. Their governance aspects are addressed in the next chapter.

2.3.1 Technical level

The technical level covers the software and hardware components for controlled, sovereign and secure sharing of data. It consists of five sub-levels with topics that require adequate governance:

- Handshake

  The handshake protocol as implemented by an **IDS connector** handles aspects such as secure peer-to-peer connectivity, identification and authorization and remote attestation, as well as the meta-data message information model. For IDS, the communication between the IDS-connectors uses the IDS Communication Protocol (IDSCP). IDSCP allows remote attestation and uses the **IDS information model**.

From a Data Providers perspective, it is noted that not for all sharing of data with Data Consumers a same and high level of security will be required. Supporting various handshake protocols can make his data available in an easy manner to a larger set of Data Consumers. For instance, when open data is shared or when data has been anonymized it may already be used by a broad set of Data Consumers without all 'heavy-weight' control and security measures of IDSCP and an IDS trusted connector being required. A 'light-weight' handshake protocol may be sufficient for being allowed to access the data. Therefore, a **hybrid connector** is to be supported allowing for various handshake protocols to be used.

- Identity and authentication

  Within a data sharing domain, identification and authentication are done at two levels:

  - As legal identities, to identify and authenticate natural persons, organizations, or software components as legal entities.
  - As data space members, to administer and to continuously check that the identified and authenticated legal entities are actually registered as member of a specific data space, and as such adhere to the legal agreements as agreed upon within the data space.

- Authorization

  This encompasses the definition of access and usage control policies, the registration of access and usage control policies and the enforcement of access and usage control policies. The access control policy states which individuals, roles or systems are allowed access to the data provided. The usage control policy states which individuals, roles or systems are allowed access to the data provided. The access and usage control policies express the data provider's internal (business) data sharing policies and the external (regulatory) policies.

- Data, processing and service brokering

  Data, processing and service brokering entails registering and managing metadata on the data, processing and service resources available in individual data sharing domains to make these registered resources searchable and available within and across data spaces. As such, a '**federated catalogue**' approach is required. The federated catalogue consists of a federation of different catalogues of resources which are joined in a standardized method, virtually acting as a single overarching data, processing and service broker across data spaces. The federated catalogue must be aligned with the concept of the federator as currently being developed within GAIA-X initiative [9].

- App enabling

To enable ease of deployment of (third party) data apps an **Application Execution Environment (AEE)** as part of the IDS-connector is needed for app and data flow initiation and orchestration function. The orchestration function should interwork with the Policy Execution Framework (PEF) in order to validate data usage policies during the data sharing process.

The AEE can be seen as edge processing (computing) capability with capabilities for advanced data control and data sovereignty. **Cloud integration** could provide the manner for implementation thereof, with GAIA-X potentially being a good match to provide the required functionality.

2.3.2 Semantic level

At the semantic level, it may be obvious that a shared and **common semantic data model** to be jointly used by Data Providers and Data Consumers has major advantages in minimizing complexity for interconnection and collaboration. However, such a jointly used common semantic data model will appear to be an utopia. Therefore, mechanisms for semantic conversion need to be supported in the data space architecture. Enabled by the (Application Container Management Layer of the) IDS-connector (security gateway) architecture as recently standardized [12], this may be taken care of by means of semantic management data apps. **Semantic management data apps** may be developed for specific semantic conversions or for enabling easy-to-use mapping between semantic models.

2.3.3 Organizational level

The organizational level refers to the way in which the agreements, expectations and processes are aligned to achieve the common goals for controlled data sharing. This includes the **onboarding and certification** (according to common and accepted criteria), **aligned service level agreements** (for realizing overarching expectations and quality control) and aligned **operations and customer processes** (for improved operating efficiency and enhanced customer experience).

2.3.4 Legal level

The aspect of legal interoperability between data sharing domains presents a major challenge. Currently, legal aspects are mainly dealt with within a single data space by pre-defining the set of muti-lateral legal agreements to which individual Data Providers and Data Consumers are bound to adhere to when signing up for joining the domain. However, this provides interoperability challenges on the legal aspects in case a Data Service Provider and a Data Consumer are member of different (or even none) data sharing domains, with varying multilateral legal agreements. To address this challenge, a **joint legal agreement** is required, which at run-time is supported by a process for **verification of legal status for data transactions**.

3 IDSA integrated governance for data space instances

The IDSA integrated governance for data space instances addresses the IDSA governance role and approach on the two development lines as described in the previous chapter:

- intra data space interoperability development line between data space authority capability and the data space intermediary infrastructure capabilities within a single data space instance, and
- inter data space interoperability development line between multiple data space instances at each of the functional levels.

3.1 Applicability: intra and inter data space interoperability

Not all the governance on the topics as identified in the previous section are applicable to both intra data space interoperability and inter data space interoperability. This is indicated in the applicability matrix in Table 1.

Table 1: Applicability Matrix: Intra and Inter Data Space Interoperability
(A = Applicable, NA = Not Applicable)

			Intra Data Space Interoperability	Inter Data Space Interoperability
Technical level				
	Handshake			
		IDS information model	A	A
		IDS connector	A	NA
		Hybrid connector	A	A
	Identity and authentication			
		Legal identities (Identity Provider)	A	NA
		Data space membership (DAPS, ParIS)	A	A
	Authorization			
		Definition of access and usage control policies	A	NA
		Registration of access and usage control policies	A	NA
		Enforcement of access and usage control policies	A	A
	Data, processing and service brokering			

		Findability & Accessibility (Broker & DAPS)	A	A
	App enabling			
		Application Execution Environment (AEE)	A	NA
		Data Apps	A	NA
		Cloud integration (GAIA-X)	A	NA
Semantic level				
		Common semantic data model	A	NAA
		Semantic management data apps	A	NA
Organizational level				
		Onboarding and certification	A	NA
		Service level agreements and quality control	A	NA
		Operations and customer processes	A	NA
Legal level				
		Joint legal agreement	A	A
		Verification of legal status for data transaction	NA	A

3.2 IDSA integrated governance: stakeholders and instruments

The IDSA has considered various governance instruments for the integrated governance of data space instances over the various IDS stakeholders. The IDSA governance instruments and the various IDS stakeholders are described in the following paragraphs of this section.

3.2.1 IDS Stakeholders

The International Data Spaces Association is a large network organization (community) with over 100 members. Currently, the IDSA manages the IDS Standard. On its turn, these standards are being deployed by IDS-users, including IDSA members. In addition, other organizations are developing implementations of various IDS components conforming to the IDS standards. Finally, there are (commercial) initiatives who use the IDS concepts and implementations in their product offering.

In the IDSA Open Source Strategy [13] the following stakeholders have been identified:

- **Data Space Instance (DSI),** i.e. a domain specific instance of and (IDS) data space, in which a data space is defined as a data ecosystem, defined by a sector or application, whereby decentralized infrastructure enables trustworthy data sharing with commonly agreed capabilities (data sovereignty and roles) [6].
- **International Data Spaces Association (IDSA)***,* as chair of the IDS initiative and organizing body for the IDSA community, guardian for the IDS standards and leader / coordinator in the development and deployment of IDS over the various stakeholders.
- **International Data Spaces Support Organization (IDS-SO)** being the, proposed, chair of the software developments for the IDS standard.
- **International Data Spaces Certification Body (IDS-CB)** is a single entity which manages and monitors the certification process and is in charge of certifying Evaluation Facilities.
- **Service Provider (SP),** being IT solution provider integrating IDS as part of their product offering for End-Users and Domain Specific Communities which are certified by the Evaluation Facilities. They help IDS End-Users and Domain Specific Communities in realizing the value add that IDS brings to their business or community.
- **End-user (EU)**, being the actual users of the IDS-based services. The End-users might be connected via a Service Provider or directly with an own connection.
- **Evaluation Facility (EF)** which evaluates and certifies IDS implementations of third-parties.
- **Contributor (C)**, being an organization that contributes to the software development of IDS. Often these types of organizations are either RTOs, Service Providers, or Domain-specific communities that develop IDS-components, e.g. for IDS-connectors or for IDS intermediary roles.

Figure 4 provides an overview of the relationships (with cardinalities) for these IDS-stakeholders. There are certain centralized roles as part of the cross data spaces governance, and roles specific for data spaces instances. Moreover, the figure specifies two types of service providers: (1) provider of essential IDS services (e.g. Broker, Identity Manager, Clearing House), and (2) provider of IDS-based services. The former group may have DSI as customer, while the latter group focusses on interconnecting End-users.

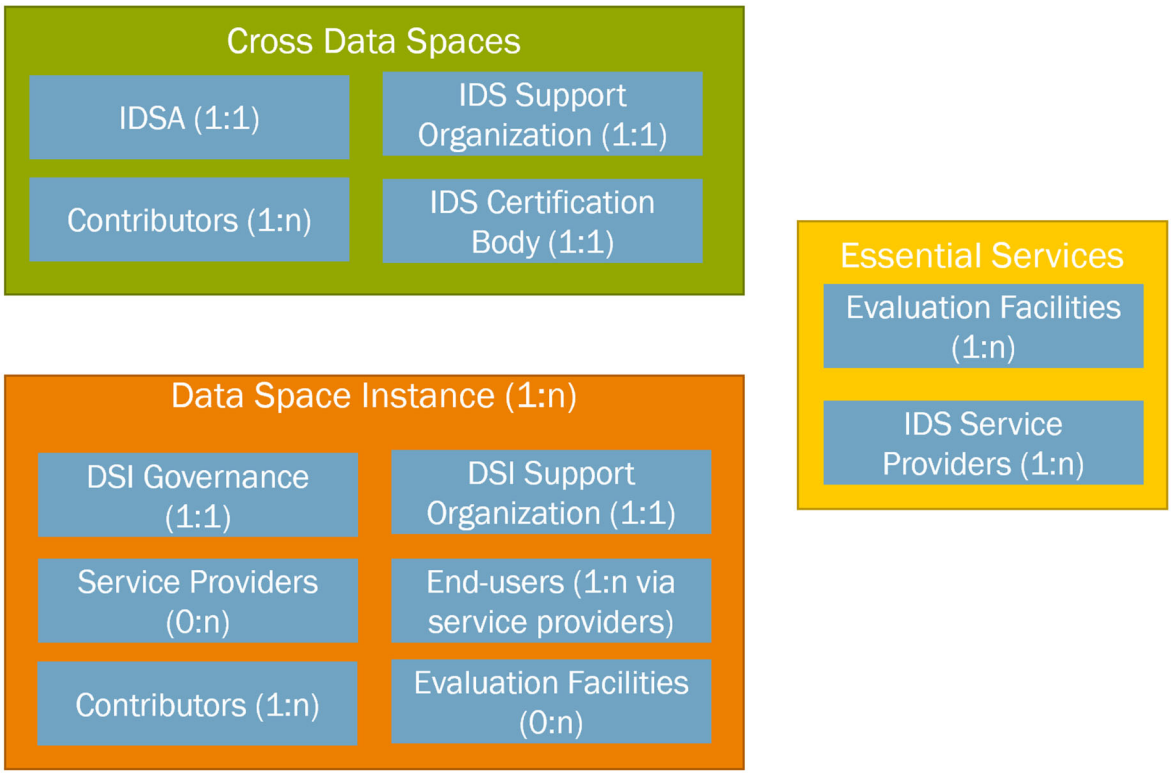


***Figure 4**. Relationships with cardinalities for the IDS-stakeholders.*

3.2.2 Governance instruments

The various governance instruments that may be considered by the IDSA are enumerated in Table 2. These governance instruments each describe a different aspect of a certain activity and are used in the next section to provide a multidimensional overview of the intra- and inter-data spaces governance.

Table 2: IDSA governance instruments

Governance Instrument	Governance instrument description
Standardization	Ensuring that the tasks, processes, and guidelines around this activity are formalized, documented, and aligned between data spaces instances and the IDSA. The standardization efforts can generally be used as a blueprint or as starting point for the stakeholders.
Certification	Validate that stakeholders act according to the standardized way of working. Certification can be divided in component certification (i.e. the certification of technical/software components) and organizational certification (i.e. organizational and legal processes).
Development	The activity may require (software) development tasks as part of the realization, which should be conform the standardization activities and preferably followed by a certification.
Operations	The operations are about the exploitation and usage of the developed components. The operations can be certified as part of the organizational certification.

Communication	The dissemination of the activity is an important aspect which might include the awareness of the standardization and certification, but also contains the marketing aspects.
Support	The support activities include the structured help of stakeholders involved in the operation, development, certification, and communication activities.

3.3 Governance for intra data space interoperability

Intra data space interoperability aims to ensure optimal functional alignment between the data space authority capability and the data space intermediary capabilities within a single data space instance as described in the previous section. The following table describes which stakeholders are responsible for the governance activities within a single data space.

For the topics on intra data space interoperability that are relevant for IDSA governance as identified in the previous paragraph the IDSA integrated governance approach is enumerated in Table 3 and elaborated in the remainder of this paragraph.

Table 3: IDSA integrated governance approach for intra data space interoperability

			Standardization	Certification	Development	Operations	Support	Communication
Technical level								
	Handshake							
		IDS information model	IDSA	EF	IDSSO		IDSSO	IDSA
		IDS connector	IDSA	EF	SP, C	SP	SP, IDSSO	IDSA
		Hybrid connector			SP, C	SP		IDSA
	Identity and authentication							
		Legal identities (Identity Provider)	DSI, IDSA	DSI		DSI, SP	SP, DSI	IDSA
		Data space membership (DAPS, ParIS)	IDSA	DSI	IDSSO	DSI, SP	SP, IDSSO	IDSA
	Authorization							
		Definition of access and usage control policies	IDSA		IDSSO		IDSSO	IDSA

		Registration of access and usage control policies	DSI	DSI	SP	DSI, SP	DSI	DSI
		Enforcement of access and usage control policies	DSI	DSI	SP	SP	SP	DSI
	Data, processing and service brokering							
		Findability & Accessibility (Broker)	IDSA	EF	SP, C	SP	SP, IDSSO	DSI
	App enabling							
		Application Execution Environment (AEE)	IDSA	EF	SP, C	EU, SP	SP, IDSSO	IDSA
		Data Apps	IDSA	EF, DSI	DSI	EU, SP	DSI	DSI
		Cloud integration (GAIA-X)	IDSA	EF	SP	SP	SP	SP
Semantic level								
		Common semantic data model	DSI	DSI	DSI		DSI	DSI
		Semantic management data apps	DSI	DSI	SP	SP	SP	SP
Organizational level								
		Onboarding and certification	DSI, IDSA	DSI		SP	SP, DSI	DSI
		Service level agreements and quality control	DSI, IDSA	DSI		SP	SP, DSI	DSI
		Operations and customer processes	DSI			SP	DSI	DSI
Legal level								
		Joint legal agreement	DSI, IDSA			DSI	DSI	DSI
		Verification of legal status for data transaction	DSI			DSI	DSI	DSI

The above table provides a comprehensive summary of which stakeholders are responsible and involved in the various activities. The table below further elaborates on this summary by providing a more detailed description of how the different stakeholders might interact per activity.

Table 4: Elaboration per topic of the IDSA integrated governance approach for intra data space interoperability as enumerated in Table 3.
Technical level
Handshake
IDS information model The Information Model is an RDFS/OWL-ontology covering the fundamental concepts of the International Data Spaces, i.e. the types of digital contents that are exchanged by participants by means of the IDS infrastructure components. This model is used as top-level ontology and describes generic functionality relevant for all types of data space instances. The data spaces instances enrich this model with domain-specific additions, which is part of the semantical activities. The **standardization** of the Information Model is chaired by the IDSA and is **supported** and **developed** by the IDSSO. Moreover, the DSI and SP use and integrate this model in their applications and may be **certified** by the Evaluation Facilities, including compliance to the IDS information model. These stakeholders may all contribute to the **development** of the IDS Information Model, but the IDSA is in charge of its overall management.
IDS connector The IDS Connector provides a generic and standardized interface into IDS-based data spaces. The Connector contains generic IDS-functionality which is mandatory for all IDS stakeholders and data space instances to use. The IDS Connector is **standardized** by the IDSA as it is part of the IDS-RAM and **supported** by the IDSSO. There are various implementations of the IDS Connector, **developed** by contributors. IDS Service Providers offer IDS-based services on top of this Connector implementation and thus **operationalize** the connector. The Service Providers are therefore also the first-line of **support** for the usage of the Connector, but are supported by the IDSSO as second-line of support on specific aspects. The various Connector implementations are **certified** by the Evaluation Facility, under supervision of the IDS Certification Body.
Hybrid Connector • See the topic of the hybrid connector as described for inter data space interoperability in Table 6.
Identity and authentication
Legal identities (Identity Provider) Before new End-users can join a domain-specific data space instance, their identity should be verified. This includes the authentication of natural persons, organizations or software components as legal entities and consists of both technical and organization steps. First of all, the identity of the End-user should be verified by using standardized processes, such as eIDAS or manual checking of official identification documents. When the identity has been confirmed, the Identity Provider can provide a Digital Certificate which End-users can use to proof their identity. The **standardization** or guidelines of the identification requirements or process within a DSI is chaired by the DSI itself. However, the IDSA can provide some generic guidelines for structuring this process. The identification is **operationalized** by the Service Providers as they perform the identity check, and the quality of this service is **certified** by the DSI. The Service Providers act as a first-line support for this process and are supported by the DSI as a second-line of support.
Data space membership identities (DAPS, ParIS) When the identity of End-users has been confirmed (see previous activity), the Identity Provider can provide a Digital Certificate which End-users can use to proof their identity, which is part of the next

		activity. Within the IDS-RAM, two main components are identified which support the technical process of identifying technical components (IDS-connectors), namely (1) the Identity Provider (IdP) to create, maintain, manage, monitor, and validate identity information of either technical components (IDS-connectors) or participants of the data space and (2) the Dynamic Attribute Provisioning Service (DAPS) for managing the dynamic attributes of the participants and continuously checks the trustworthiness of End-users including dynamic claims (e.g. certification). In addition, recently the (3) Participant Identity Service (ParIS) has been added to identify participating organizations. The IDSA is responsible for the **standardization** of the DAPS and ParIS components. For the DAPS, an API for usage has been defined, not (yet) for management and onboarding. For ParIS, the definition of its functionality (w.r.t. participant attribute status and /or participant brokering) and API's is in development. The IDSA is supported by the IDSSO and Contributors for the development of the components. The Service Providers offer DAPS/IdP/ParIS services to the data spaces instances and are therefore responsible for the **operationalization** of the components. Therefore, the Service Providers again act as a first-level of **support**, whereas the IDSSO act as a second-line of support. For IDSA the follow-up actions are suggested: • Define a management and onboarding API for the DAPS component. • Define and formalize the functionalities and API's for the ParIS component. • Define a strategy and roadmap on additional identities to be supported as part of the IDS architecture, e.g. on professional identity (physician, CFO, …), national identity, …
	Authorization	
		Definition of access and usage control policies The Access and Usage Policies (AUP) are a technical and legal way of describing how data consumers may use the provided data. The specific content of the policies might be domain- and user-specific. The individual DSI's are each themselves responsible for defining the domain-specific Access and Usage Policies applicable for their use-case. However, in order to ensure interoperability these policies should be described in a generic and **standardized** way, for which IDSA is responsible. The AUP is part of the IDS-RAM.
		Registration and management of access and usage control policies The DSI is responsible for **development** of the specific policies applicable within its data space and therefore also acts as **support** partner. The End-users and Service Providers have to apply these domain-enriched policies in their use-case and are therefore in charge of the **operationalization** of the AUP. The associated **development** and associated **support** activities are chaired by the IDSSO. The registration and management of AUP's is generally done by means of an Authorization Registry (AR) component. An AR is not part of the IDS ecosystem model in the current IDS RAM v3. Hence, for IDSA the follow-up actions are suggested: • As the AR is part of the regular interaction flows for data transactions, the relation of the IDSA to the functions of the AR should be (re-)considered. • Define and formalize the functionalities and API's for the ParIS component. Finally, the DSI might monitor the registration process of AUP policies and can therefore act as **certifier** for the End-users and Service Providers.
		Enforcement of access and usage control policies The UAPs have to be enforced, i.e. they have to be executed in practise. The Service Providers are responsible for the **operationalization** of these policies, in other words: they have to ensure that the IDS

		components and back-end systems are compliant with these policies. The Service Providers therefore also act as **support**. Moreover, to ensure that the AUP policies are enforced, the DSI can **certify** the Service Provider implementations. The IDSA can **communicate** (e.g. by means of tutorials and reference implementations) on how to realize policy execution.
	Data, processing and service brokering	
		Findability & Accessibility (Broker) When an End-user joins a DSI, being findable and accessible is an essential service to get to know the relevant participants within a data space. There are two components defined within the IDS-RAM which contribute to the findability and accessibility of participants, namely: The Broker and the Participant Information Services (ParIS). The broker is a service for data source registration, publication, maintenance, and query, based on an index. The ParIS manages additional meta-data about participants. Both components are st**andardized** by the IDSA as they are part of the IDS-RAM and **developed** by Service Providers which aim to **operationalize** these components as a service. The Service Providers therefore act as a first-line of **support** and the IDSSO as a second-line of **support**. Moreover, the Broker and ParIS services are **certified** by Evaluation Facilities, ensuring that the components are compatible with the IDS-RAM and interoperable.
	App enabling	
		Application Execution Environment (AEE) The AEE is part of the IDS Connector and enables to enrich the Connector with Data Apps (see next activity). Similar to the IDS Connector itself, the AEE is **standardized** by the IDSA as it is part of the IDS-RAM and **supported** by the IDSSO. There are various implementations of the AEE, each of them **developed** by an IDS Service Provider which might aim to offer IDS-based services on top of this AEE implementation and thus **operationalize** the connector. The Service Providers are therefore also the first line of **support** for the usage of the AEE, but are supported by the IDSSO as second-line of support for questions transcend implementation-specific questions. The various AEE implementations are **certified** by the Evaluation Facility, under supervision of the IDS Certification Body. For IDSA the follow-up actions are suggested: • Data apps are developed and provided by App Providers. When installing a data app within an IDS-connector, its input and output data flows may need to be controlled by the IDS-connector's UAP policy execution framework (PEF). Hence, IDSA should develop and standardize an interface on the PEF to be used by data apps for instantiating and enforcing the required PEF capabilities.
		Data Apps Data Apps contain domain-specific data handling logic and enrich the IDS-Connector interface (as provided by the IDS-G [14]) with organizational and technical requirements on top of the IDS Connector. The Data Apps concept is **standardized** by the IDSA as part of the IDS-RAM. The domain-specific Data Apps are **developed** by the DSI, and **operationalized** by the Service Providers and End-Users. The interoperability of the Data Apps with the IDS-RAM is certified by the Evaluation Facilities and the domain-specific logic is certified by the DSI.

		Cloud integration (GAIA-X) The final technical activity touches upon the cloud and hardware layer of the IDS-service offerings. This topic is highly related with GAIA-X Cloud Interoperability concepts. For IDSA the follow-up actions are suggested: • API definition for interfacing with data processing environment, e.g. the GAIA-x environments. • Define a strategy and roadmap on 'full-stack' integrity, i.e. for realizing sovereignty across both the data processing and data sharing capabilities.
Semantic level		
		Common semantic data model The IDS Information Model is the basis semantic model for IDS-based data spaces (see activity Information Model). Each data space might have to enrich the Information Model with domain-specific information, which is not part of the Information Model. The DSI is responsible for **standardizing** and **development** the common semantic data model within the data space instance. The Service Providers **implement** the domain specific model in the related Data App (as part of the IDS Connector), and this implementation is **certified** by the DSI. Finally, the DSI is responsible for **support** on the domain-specific data models.
		Semantic management data apps The Semantic Management Data Apps are used within data space instances to map different semantic models to the agreed upon common semantic data model (see previous activity). In order to integrate End-users, a semantic mapping between the End-users back-end systems and the common semantic data model is required. This mapping might be **standardized** and **certified** by the DSI and is **developed** by the Service Providers. The Service Providers facilitate the connection of the End-users and therefore are also the main **support** contact point.
Organizational level		
		Onboarding and certification When new End-users want to join the data space instance, they have to be onboarded and certified. The onboarding process consists of various organizational activities besides the technical onboarding, such as the identification and authorization (which are covered earlier) and contractual agreements. This onboarding and certification process is an data space instance-specific process, as requirements may change across data spaces. Therefore, the DSI is responsible for the **standardization** within the data space (i.e. ensuring that all participants are onboarded in a similar way), while the IDSA provides generic rules and guidelines for onboarding new participants as part of the IDSA Rule Book. The Service Providers **operationalize** the process by performing the actual onboarding and is **supported** by the DSI. Moreover, the DSI might **certify** the onboarding process of the service providers associated with the data space.
		Service level agreements and quality control Important aspects of the organizational contractual agreements between the different stakeholders in a data space is Service Level Agreement (SLA) and general quality control. The SLA provides a legal set of requirements for the service offering and aims to maintain a certain level of quality. The DSI is responsible for **standardizing** the SLAs within a data space, while the IDSA provides generic reference agreements which may be used by the DSI. The SLA is **operationalized** by the Service Provid-

		ers. Therefore, the Service Providers act as the first-line of **support** and the DSI as second-line of support. Moreover, the DSI is responsible for the continuously monitoring of the SLAs and quality control and can **certify** the service providers which meet all requirements.
		Operations and customer processes The final organization process defined in this overview is about the actual operations of the data space. In practise, the service providers are the facilitators of the IDS-based connections and therefore are responsible for the **operationalization** and **support** from the perspective of the End-user. The DSI might provide **standardize** the operational processes as part of the domain-specific enrichments of the dataspace.
Legal level		
		Joint legal agreement The various stakeholders of a data space might require an array of different joint legal agreements as a legal basis for the collaborations through the data space, examples being the Service Level Agreement and the Data Processing Agreement. The DSI is responsible for **standardizing** the agreements within the data space, while the IDSA provides generic reference frameworks for structuring these agreements. Moreover, the DSI is also chairing the **support** around the legal agreements.
		Verification of legal status for data transaction This activity is only relevant for the inter-data spaces governance interoperability and is therefore discussed in the next section.

3.4 Governance for inter data space interoperability

There will not be a single data space. Individual sectors or communities are expected to develop their own data space instances. Being able to seamlessly share data over these data space instances yields clear advantages. It extends the reach and scope of accessible data and allows new business models and services to be developed across sectors and regions. Therefore, interoperability between data space instances adds major value, resulting in a federation of interoperable data spaces as depicted in in the right part of Figure 3.

3.4.1 Interoperability architecture considerations

3.4.1.1 Harmonization

The Data Sharing Coalition is an open and growing, international initiative in which a large variety of organizations have collaborated to drive cross-domain data sharing at scale. Its results on cross-domain data sharing have recently been published in the 'Data Sharing Canvas' [7].

In the 'Data Sharing Canvas', a comparison has been made between various harmonization options. Full Harmonization of data spaces, in which existing data spaces adjust their implementations to follow a common, cross data space design, is the ideal solution to achieve multilateral interoperability. However, it impacts all data space participants, requiring significant investments and will therefore not be adopted. Bilateral Harmonization of data spaces, in which individual data spaces bilaterally organize custom interoperability are dependent

on individual participants implementing specific harmonized solutions and will therefore limit large scale cross data space data sharing. As alternative Partial Harmonization, in which a new role 'Data Space Proxy' is introduced, overcomes these limitations of Full and Bilateral Harmonization. The Proxy absorbs the complexity of harmonization for data spaces and its participants as much as possible by implementing all harmonization requirements. This enables a data provider in one data space to share data with a data consumer in another data space, while limiting impact for both existing data providers and data consumers. The proxy model for partial harmonization is depicted in Figure 5.

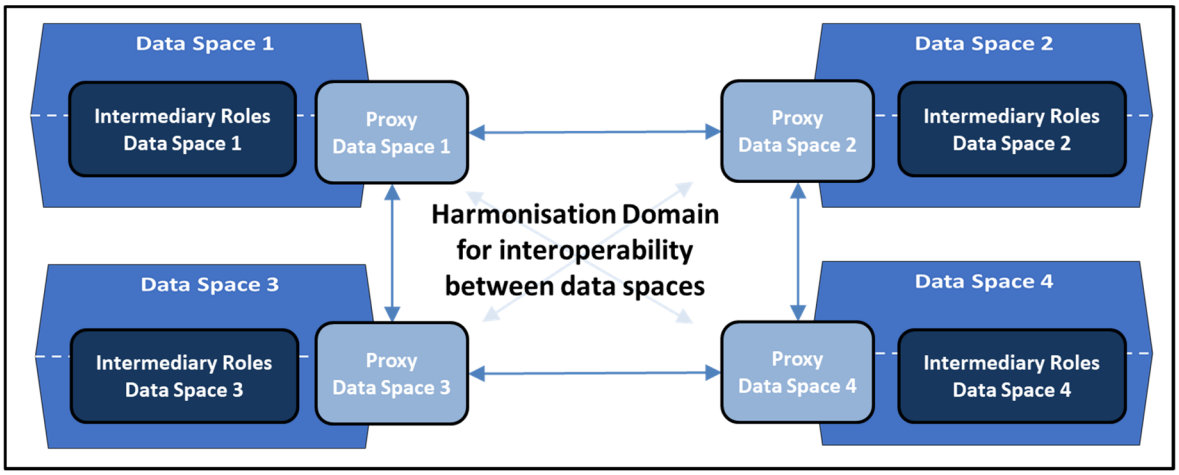


Figure 5. The proxy model for data space harmonization [7].

The main functionality of the proxies is to translate data space specific transactions to their harmonized equivalents:

- Proxies will translate data space specific language to a harmonized language in the Harmonization Domain to enable multilateral end-to-end Interoperability,
- Proxies will facilitate Trust across data spaces by conforming to the rules and agreements of the Trust Framework,
- Proxies will enable the discovery of data providers across data spaces.

The Proxies implemented by all data spaces form a network, the Harmonization Domain, which enables each data space to share data effortlessly with other data spaces.

3.4.1.2 Interaction topologies

For interoperability between data space instances, the intermediary roles of these data spaces will have to interact and to exchange (meta)data. These interactions may be designed through various 'Metadata Role Interaction Topologies (MRIT)'. The implementation decision for a specific type of MRIT will result in a governance role for the IDSA and / or other IDS stakeholders their development or deployment. They are illustrated in Figure 6.

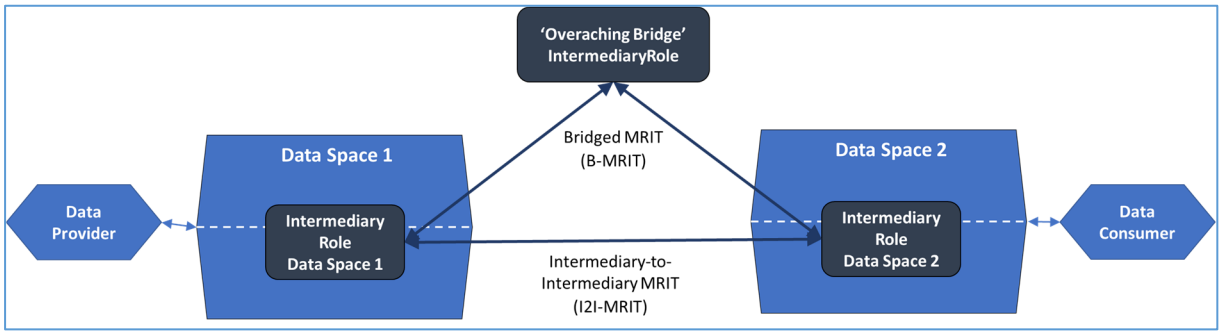


Figure 6. Two basic types of 'Metadata Role Interaction Topology' (MRIT).

The two basic types of MRITs which are applicable for exchanging (meta)data between intermediary roles from different data space instances as depicted in the figure, are:

- Intermediary-to-Intermediary MRIT (I2I-MRIT), in which the exchange of (meta)data between the intermediary roles of the various data space instances is on bilateral, peer-to-peer basis.

An example may be the broker service provider that bilaterally exchange metadata on available data sources.

- *Bridged MRIT (B-MRIT),* in which the exchange of (meta)data between the intermediary roles of the various data space instances uses an overarching bridging function.

An example may be the legal framework with associated participant registry for managing that data spaces instances and its participants are legally adhering to an overarching legal framework.

For interoperability for the various data space capabilities, different interaction topologies may be most suitable, requiring different governance role for IDSA in developing or deploying these topologies.

3.4.2 Governance topics: elaboration

Inter data space interoperability has to ensure seamless functional and technical alignment between multiple data space instances for the topics on each of the functional levels as depicted in Figure 2 and described in section 2.1.

For these topics, Table 5 enumerates the IDSA integrated governance approach for inter data space interoperability in terms of both the governance instruments to be used and the associated IDS stakeholders.

Table 5: IDSA integrated governance approach for inter data space interoperability							
		Standardization	Certification	Development	Operations	Support	Communication
Technical level							
	Handshake						
	IDS information model	IDSA		IDSSO			IDSA
	IDS connector						
	Hybrid connector			SP, C	SP		IDSA
	Identity and authentication						
	Legal identities (Identity Provider)						
	Data space membership (DAPS, ParIS)	IDSA	IDS-CB	C	SP	SP, IDSSO	DSI
	Authorization						
	Definition of access and usage control policies						
	Registration of access and usage control policies						
	Enforcement of access and usage control policies	IDSA					IDSA
	Data, processing and service brokering						
	Findability & Accessibility (Broker)	IDSA					IDSA
	App enabling						
	Application Execution Environment (AEE)						
	Data Apps						
	Cloud integration (GAIA-X)						
Semantic level							
	Common semantic data model						
	Semantic management data apps						

Organizational level								
		Onboarding and certification						
		Service level agreements and quality control						
		Operations and customer processes						
Legal level								
		Joint legal agreement	IDSA			IDSSO		IDSA
		Verification of legal status for data transaction	IDSA		IDSSO	IDSSO		IDSA

For the topics at each of the technical levels, the results as provided in the table are further elaborated in the following paragraphs.

Table 6: Elaboration per topic of the IDSA integrated governance approach for inter data space interoperability as enumerated in Table 5

Technical level		
	Handshake	
		IDS information model • See the topic of the IDS information model for intra data space interoperability in Table 4. **In addition:** IDSA should develop a vision and strategy for positioning (elements of) the IDS information model in the **development** of a harmonization model in the federated and interoperable data space architecture as depicted in Figure 5. In addition, semantic mappings on elements with adjacent information models in other data sharing domains can be developed.
		IDS connector See the topic of IDS-connector for intra data space interoperability in Table 4.
		Hybrid connector The introduction of IDS data spaces will be gradual. Not all data providers and data consumers will have all (or even any) IDS data space building blocks in place at the same time. Or in short: a 'big bang' introduction of IDS data spaces is a utopia. The data sharing landscape will be characterized by various data sharing environments with various sets capabilities and protocols. Nevertheless, this shouldn't prevent individual data providers and data consumers from sharing data. However, the extent to which sensitive data is shared may depend on the common capabilities they do have in place. To support such heterogenous data sharing relationships, a data provider can classify his data, distinguishing between open data and (various levels of) governed data. Data sharing decisions with specific Data Consumers are based upon the combination of the classification level of the data and the capabilities they have implemented, including: (1) being able to identify the data consumer, (2) Having a legal and / or usage contract with the data consumer and (3) having policy execution capabilities with the data consumer. This is enabled by a hybrid connector in which multiple protocols (in addition to the IDS protocol) are supported. The role for the IDSA in the development and deployment of hybrid connectors is limited, i.e. to **communication** of its possibilities as part of a migration and interoperability trajectory, e.g. by means of a

		vision paper. To support their customers with a portfolio of services, there is a role for Service Providers and Contributors in the **development** and for Service Providers in **operations** of the hybrid connectors.
	Identity and authentication	
		Legal identities (Identity Provider) Legal identities are only used within a DSI, not between DSI's. They are internally registered in the DAPS or the ParIS component. The IDSA can provide some generic guidelines for structuring this process.
		Data space membership identities (DAPS, ParIS) • See the topic of data space membership identities for intra data space interoperability in Table 4. **In addition:** Data space membership identities are used between DSI's to authenticate technical components or participants on specific DSI membership. To this end the IDSA should **standardize** the functionality and API's for both DAPS and ParIS for inter data space interactions and **develop** a vision and strategy for positioning DAPS and ParIS a spart of the harmonization model in the federated and interoperable data space architecture as depicted in Figure 5. The **development** thereof as part of a proxy should be done by Contributors whereas ist **operations** and **support** are done by Service Providers
	Authorization	
		Definition of access and usage control policies • See the topic of access and usage control policies for intra data space interoperability in Table 4.
		Registration and management of access and usage control policies • See the topic of registration and management of access and usage control policies for intra data space interoperability in Table 4.
		Enforcement of access and usage control policies • See the topic of enforcement of access and usage control policies for intra data space interoperability in Table 4. **In addition:** Enforcement of the AUPs between DSI's is a key design component of inter data space interoperability. It requires the implementation of the complete suite of IDS functions over each of the interoperability levels as depicted in Figure 3 (technical, semantic, organizational, legal). As such, it also has a relation with each of the topics as addressed in this table. The exchange of authorization (and enforcement) information between data spaces is key for retaining data sovereignty for individual data sharing transactions. An Authorization Registry (AR) component has an important role to play in this process. However, as stated in in Table 4 an AR is not part of the IDS ecosystem model in the current IDS RAM v3. For IDSA, the following follow-up actions are suggested: • Develop a vision and strategy for positioning enforcement of AUP's and the role of AR's therein in the development of a harmonization model in the federated and interoperable data space architecture as depicted in Figure 5. • Define an API for AR-components for inter data space interactions.

	Data, processing and service brokering
	Findability & Accessibility (Broker) • See the topic of findability and accessibility for intra data space interoperability in Table 4. **In addition:** Being able to seamlessly share data over individual DSI's yields clear advantages. It extends the reach and scope of accessible data allowing services and solutions to be developed across Hence, DSI's. Finding and accessing data across DSI's is needed. The Federated Catalogue acts as a Broker between DSI's. For IDSA, the following follow-up actions are suggested: • Develop a vision and strategy for positioning the IDS Broker Service Provider in the development of a harmonization model in the federated and interoperable data space architecture as depicted in Figure 5. • Define an API for the IDS Broker Service Provider for inter data space interactions. • Support the development of semantic data apps for converting / mapping the data source description format of the IDS information models into other, commonly used, description formats (e.g. DCAT 2.0).
	App enabling
	Application Execution Environment (AEE) • See the topic of the Application Execution Environment (AEE) for intra data space interoperability in Table 4.
	Data apps • See the topic of the Data Apps for intra data space interoperability in Table 4.
	Cloud integration (GAIA-X) • See the topic of cloud integration for intra data space interoperability in Table 4.
Semantic level	
	Common semantic data model • See the topic of common semantic data model for intra data space interoperability in Table 4.
	Semantic management data apps • See the topic of semantic management data apps for intra data space interoperability in Table 4. **In addition:** The (semantic management) data apps will execute in an Application Execution Environment (AEE) of an IDS-connector. Therefore, also the topic in the App Enabling category in both Table 4 and this table are applicable.

Organizational level		
		Onboarding and certification • See the topic of onboarding and certification for intra data space interoperability in Table 4. As stated in Table 4, the onboarding and certification process is a data space instance-specific process, as requirements may change across data spaces. The DSI is responsible for the standardization within the data space
		Service level agreements and quality control • See the topic of Service level agreements and quality control for intra data space interoperability in Table 4. This is data space instance-specific process. The role for IDSA is limited to providing generic reference agreements which may be used by the data space instances.
		Operations and customer processes • See the topic of operations and customer processes for intra data space interoperability in Table 4. Also this is data space instance-specific process. The role for IDSA is limited to providing generic reference agreements which may be used by the data space instances.
Legal level		
		Joint legal agreement An overarching 'data space scheme' addressing (amongst others) the joint legal agreements between adhering data spaces will be pivotal in realizing data space interoperability. It provides an overarching legal framework, to which the individual data space instances (and their subscribers) agree to adhere. For IDSA, the following follow-up actions are suggested: The role of IDSA in fulfilling the role of overarching 'data space scheme owner' should be assessed and adequate governance on it should be provided for. It may imply that the IDSA will (have to) fulfil a continuous operational task in providing this role of overarching 'data space scheme'.
		Verification of legal status for data transaction For individual data transactions, the formal legal status of the data consumer (in relation to the data provider) has to be known, prior to sharing the (sensitive) data. As such, a metadata information flow including the (legal) status check at the overarching 'data space scheme' between adhering data spaces may be required, for which the IDSA or IDSSO may need to fulfil an **operations** task. For IDSA, the following follow-up actions are suggested: • The role of IDSA in providing the capability for the (legal) status check between adhering data spaces should be assessed, including the role of a role for the IDSSO in the **development** and **operations** of this capability.

4 Concluding remarks

A primary objective of this report has been to identify and detail the roles and responsibilities for the main IDS-stakeholder in jointly providing the governance for developing and deploying IDS and data space instances. As such, an extensive set of topics requiring adequate governance has been identified and elaborated, systematically categorized according to the interoperability levels of the new European Interoperability Framework as developed by the European Commission, under an overarching integrated governance approach: the technical level, the semantic level, the organizational level and the legal level. Moreover, a distinction has been made between governance topics for two development lines, i.e. the development line of intra data space interoperability and the development line of inter data space interoperability.

In conclusion, the following sections summarize the governance roles for the various IDS-stakeholders on the interoperability topics for both intra and inter data space interoperability and provide concluding remarks on both the intra and inter data space development lines, subsequently.

4.1 Summary of governance roles of IDS-stakeholder for intra and inter data space development

An extensive elaboration of the roles of the IDS-stakeholders on the various levels and topics of interoperability has been provided in chapter 3, both for the intra and inter data space development lines.

Table 7 summarizes its results with the main responsibilities per IDS stakeholder.

Table 7: Summary of governance roles of IDS-stakeholder for intra and inter data space interoperability development		
Data Space Instance (DSI)		
	Role in intra data space development	
		To coordinate the operational activities within the data space, ranging from providing technical support, to marketing, to legal aspects.
	Role in inter data space development	
		•
International Data Spaces Association (IDSA)		
	Role in intra data space development	
		To provide and to promote generic technical standards which can be used across the various DSI. Moreover, the IDSA can provide standardized processes and procedures to manage a DSI as well contribute to general marketing and communication activities, which can be an important input for setting up a DSI.

	Role in inter data space development
	•
International Data Spaces Support Organization (IDS-SO)	
	Role in intra data space development
	To support the (technical) integration of the provided standards as part of IDSA's responsibilities. The Support Organization is mostly concerned about providing support to (1) DSI, (2) EF, (3) Service Providers, and are therefore not directly concerned about the end-users.
	Role in inter data space development
	•
International Data Spaces Certification Body (IDS-CB)	
	Role in intra data space development
	To standardize the certification process of implementation in the DSI.
	Role in inter data space development
	•
Service Provider (SP)	
	Role in intra data space development
	To develop, integrate, deploy, and support the solutions developed in the DSI. The Service Providers are the main contact point for the End-users and facilitate the (technical) onboarding of the End-users in the DSI.
	Role in inter data space development
	•
End-user (EU),	
	Role in intra data space development
	To make use of the developed solutions.
	Role in inter data space development
	•
Evaluation Facility (EF)	
	Role in intra data space development
	To certify, under supervision of the CB, the usage and implementation of the solutions developed by the Service Providers and used by the End-users.

	Role in inter data space development	
		•
Contributor (C),		
	Role in intra data space development	
		To further contribute to the development of the DSI solution and to the IDS Reference Architecture Model.
	Role in inter data space development	

4.2 Concluding remarks on the intra data space development line

For the development line on intra data space interoperability, the following concluding remarks are made:

- The exact relations between the data spaces and the IDSA may differ between data space instances, but in general the IDSA can provide guidelines, frameworks, or policies on how processes are structured within a data space instance. The data s pace itself is responsible for executing this process.
  - A complete set of APIs for interactions with the various building blocks and capabilities of the data space structure (as depicted in Figure 1) should be identified and defined. This will be done under the responsibility of the IDSA Technical Steering Committee (IDSA-TSC) and reported on within the (future releases of the) IDSA Rule Book [11]. This may extend on the current scope of APIs being defined by the IDSA. Specific attention should (for instance) be given to:
  - An API for the Policy Execution Framework (PEF) to be used by data apps for using the PEF's data control and sovereignty features, as identified for the topic 'Application Execution Environment (AEE)' in Table 4.
  - APIs for managing and accessing data space membership identities (as provided by the DAPS and ParIS capabilities) to be used in the authorization flows for individual data transactions, as identified for the topic 'Data space membership (DAPS, ParIS)' in Table 4.
  - An API for accessing (cloud) processing capabilities for locally executing data apps, as identified for the topic 'Cloud integration (GAIA-X)' in Table 4.
  - …
- An adequate and future-proof governance process for managing the IDSA standards is needed. The IDSA standards need management and maintenance, including further development with backward compatibility of releases. Again, this process will be elaborated on within the (future releases of the) IDSA Rule Book [11].

4.3 Concluding remarks on the inter data space development line

For the development line on inter data space interoperability, the following concluding remarks are made:

- The proxy model in combination with a harmonization domain and protocols is currently suggested by the Data Sharing Coalition [7] as architecture to enable interoperability between data space instances, i.e. for inter data space interoperability as depicted in Figure 5. As the need for inter data space interoperability is rapidly growing, it is necessary for the IDSA to assess whether and how it impacts the development of (IDS-based) data spaces and on the role of IDSA in co-developing the data space proxy interfaces and harmonization protocols. The IDSA governance model for development and deployment of the inter data space architectures and standards is to be defined.
- Moreover, an overarching 'data space scheme' defining and implementing joint legal and operational agreements between adhering data spaces instances will be pivotal in realizing inter data space interoperability. Amongst others, it provides an overarching legal framework, to which the individual data space instances (and their subscribers) agree to adhere.

The role of IDSA in fulfilling the role of overarching 'data space scheme owner' should be assessed and adequate governance on it should be provided for. It may imply that the IDSA will (have to) fulfil a continuous operational task in providing this role of overarching 'data space scheme'.

The need for inter data space interoperability is rapidly growing. As such, this topic has been identified as relevant for various European research and development initiatives. For instance, the Data Sharing Coalition [7] and the OPEN DEI initiative (in the future releases of their 'Design Principles for Data Spaces' [6]) are expected to explicitly address these topic. An active role of IDSA and its stakeholders should be pursued in these European initiatives.

5 References

[1] European commission 2020. "A European Strategy for Data". Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions. URL: https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf.

[2] European Commission 2020. "Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act)". Communications 66. URL: https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-data-governance-data-governance-act.

[3] OPEN DEI. "Aligning Reference Architectures, Open Platforms and Large-Scale Pilots in Digitising European Industry". URL: https://www.opendei.eu/.

[4] GO-FAIR, "FAIR Principles", URL: https://www.go-fair.org/fair-principles/.

[5] Dutch Neutral Logistics Information Platform. "iSHARE Data Sharing Initiative". URL: https://www.iSHAREworks.org/en/.

[6] OPEN DEI. "Design Principles for Data Spaces – Position Paper". Version 1.0. April 2021, https://design-principles-for-data-spaces.org/.

[7] Data Sharing Coalition (2021). "Data Sharing Canvas - A stepping stone towards cross-domain data sharing at scale". URL: https://datasharingcoalition.eu/app/uploads/2021/04/data-sharing-canvas-30-04-2021.pdf.

[8] European Union 2017. "New European Interoperability Framework (EIF) – Promoting seamless services and data flows for European public administrations". URL: https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf.

[9] GAIA-X initiative 2021. "GAIA-X Architecture Document". URL: https://www.gaia-x.eu/sites/default/files/2021-06/Gaia-X_Architecture_Document_2106.pdf.

[10] International Data Spaces Association (IDSA) 2019. "International Data Spaces: Reference Architecture Model Version 3". URL: https://www.internationaldataspaces.org/wp-content/uploads/2019/03/IDS-Reference-Architecture-Model-3.0.pdf.

[11] IDSA (2020). "IDSA Rule Book", version 1.0, December 2020. URL: https://internationaldataspaces.org/wp-content/uploads/IDSA-White-Paper-IDSA-Rule-Book.pdf.

[12] DIN SPEC 27070, "Reference Architecture for a Security Gateway for Sharing Industry Data and Services". URL: https://www.beuth.de/en/technical-rule/din-spec-27070/319111044.

[13] International Data Spaces Association (IDSA) 2021. "IDSA Open Source Strategy – Version March 2021".

[14] International Data Spaces Association (IDSA). 'IDS-G on GitHub". URL: https://github.com/International-Data-Spaces-Association/IDS-G.

6 Appendix A: Glossary

This appendix contains a glossary for the terms as used in this report.

Where applicable, the terms as used within the glossary in this appendix adheres to the definitions as provided in the glossary of the OPEN DEI position paper on design principles for data spaces [6] and the terminology as provided in the recently standard for the reference architecture of a security gateway [12].

In the following tables, the glossary distinguishes between the terms used for:

- IDS stakeholder roles (Table 8),
- Data space authority building blocks (Table 9),
- Data space data sharing building blocks (Table 10), and
- Data space data processing building blocks (Table 11).

Table 8: Glossary for IDS Stakeholder Roles	
Term	Definition
Contributor(C)	Organization that contributes to the software development of IDS. Often these types of organizations are either RTOs, Service Providers, or Domain-specific communities that develop IDS-components, e.g. for IDS-connectors or for IDS intermediary roles.
Data Space Instances (DSI)	Domain specific instance of and (IDS) data space. In which a data space is defined as a data ecosystem, defined by a sector or application, whereby decentralized infrastructure enables trustworthy data sharing with commonly agreed capabilities (data sovereignty and roles) [6].
End-users (EU)	Actual user of the IDS-based services. The End-users might be connected via a Service Provider or directly with an own connection.
Evaluation Facilities (EF)	Evaluator and certifier of IDS implementations of third-parties.
International Data Spaces Association (IDSA)	Chair of the IDS initiative and organizing body for the IDSA community, guardian for the IDS standards and leader / coordinator in the development and deployment of IDS over the various stakeholders.
International Data Spaces Association Certification Body (IDS-CB)	A single entity which manages and monitors the certification process and is in charge of certifying Evaluation Facilities.

International Data Spaces Support Organization (IDS-SO)	The, proposed, chair of the software developments for the IDS standard.
Service Providers (SP)	IT solution provider integrating IDS as part of their product offering for End-Users and Domain Specific Communities which are certified by the Evaluation Facilities. They help IDS End-Users and Domain Specific Communities in realizing the value add that IDS brings to their business or community.

Table 9: Glossary for Data Space Authority Building Blocks	
Term	Definition
Authority Administrator	Verifies and manages applications and admitting parties to the scheme. This entails both checking the identity of the company, and its legal adherence to the rules. In addition, a technical compliance process may be required.
Scheme Owner	Manages the development of the data space itself, in which the scheme is a common set of multilateral agreements that facilitates standardized and decentralized data sharing directly amongst participants [6].

Table 10: Glossary for Data Space Data Sharing Building Blocks	
Term	Definition
Application Execution Environment, (AEE)	Provides an environment to execute data apps under (security) control of either a Data Service Provider or Data Service Consumer. It may be provided over a cloud infrastructure, e.g. as provided by GAIA-X.
Policy Execution Framework (PEF)	Enforces the conditions under which data is shared (as expressed by a usage contract) within the (security) domain of the Data Provider or Data Consumer.
Semantic Management	Provides the functions to manage the semantics of the data being shared, e.g. by means of semantic mapping or semantic conversion.

Table 11: Glossary for Data Space Data processing Building Blocks

Term	Definition
Authorization Registry (AR)	Manages Records of Authorization (and, if relevant, Records of Delegation) so that Participants in the Collaborative Solution can verify whether a Data Consumer is authorized to access a specific Data Asset [6].
Broker Service Provider	Mediates between data providers and data consumers [12]. Unlike brokers in common message based systems retrieving and distributing the data actually offered and required, the Broker as under stood here retrieves and distributes metadata about certain data and services.
Clearing House	Provides clearing and settlement services for all financial and data sharing transactions, including conflict resolution and support for data sharing transactions requiring non-repudiation.
Identity Provider	Offers services to create, maintain, manage and validate identity information for parties that share data within a collaborative solution [6].
Security Gateway	A network component connecting different network segments [12]. A Security Gateway is typically located at a company‘s logical border, defining its interfaces with external entities. This means that a Gateway can physically be implemented both at the company‘s premises and at the premises of a service provider.

CONTACT

Head Office

INTERNATIONAL DATA SPACES ASSOCIATION

Emil-Figge-Str. 80
44227 Dortmund | Germany

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

WWW.INTERNATIONALDATASPACES.ORG

@ids_association

international-data-spaces-association