CSBO SYTADEL : SYNCHROMODAL PROTOTYPE FOR DATA SHARING AND PLANNING

D 4.3 Data space governance principles

June 14, 2025

CONTENT

1 Introduction

Federated logistics data space is emerging as a solution for sharing data across multiple organisations in the supply chain while preserving each participant's autonomy and data sovereignty. Unlike centralised platforms, a federated data space allows logistics stakeholders such as shippers, carriers, ports, and regulators to exchange information on a peer-to-peer basis under a common set of standards and agreements. This approach is getting attention in Europe through initiatives like the International Data Space Association (IDSA) and GAIA-X, which focus on enabling secure, sovereign data collaboration aligned with values of privacy and trust. However, simply establishing the technical ability to connect systems is not enough. A robust governance framework is needed to ensure that data sharing in such a federated environment remains interoperable, trustworthy, valuable, and well-administered. In other words, governance provides the "rules of the game" that make participants comfortable sharing data and that keep the ecosystem fair and efficient.

Developing a governance framework for a logistics data space means addressing a combination of technical, organisational, and legal considerations. It involves setting policies for data access, usage, and security, defining roles and responsibilities, and aligning with regulatory requirements. Indeed, an effective framework spans multiple interconnected layers, such as technical, semantic, organisational, and legal, which work together to support data sovereignty, interoperability, security, and collaboration among stakeholders. The remainder of this report presents a comprehensive governance framework developed for a federated logistics data space, focusing on four primary governance pillars: Interoperability, Data Sovereignty and Trust, Data Value Creation, and Administrative Governance. Each pillar addresses a critical dimension of governance needed to manage data sharing in a complex, multi-actor logistics network. We draw on insights from the SYTaDel project and desk research to illustrate how this framework can be implemented in practice. The SYTaDel case serves as a running example, demonstrating how the governance principles translate into practical tools, rules, and processes.

Before diving into the pillars, we outline key considerations in designing the framework. We discuss each pillar of the framework with clarity and authority, explaining what it entails and how to implement it. Then we include understanding the context in which data is shared (e.g., whether data is at rest or in transit). Finally, we discuss lessons learnt, which offers actionable guidance for industry practitioners and academics looking to implement similar governance structures in their own data space.

2 Designing a Governance Framework: Key Considerations

Developing a governance framework for a federated data space requires a structured approach. It is helpful to start by breaking down the problem into fundamental questions:

What specific governance actions are required? Who is responsible for governing at each point? And What governance needs arise in each pillar? Addressing these questions up front ensures that the framework will be comprehensive and context-aware.

2.1 Defining the pillars of the governance framework

Developing a governance framework for a logistics data space means more than just setting rules for data. It also involves managing the processes that ensure data is used securely, efficiently, and collaboratively. In a federated setup, where many different actors are involved, this becomes especially important. A solid starting point for this is to look at the core design principles behind data spaces. As proposed by Nagel and Lycklama (2021), these principles offer a clear structure for building environments that support trusted, interoperable, and sovereign data exchange. Nagel and Lycklama (2021) grouped these principles into four key areas: Data Interoperability, Data Sovereignty and Trust, Data Value Creation, and Data Space Governance (Administrative Governance).

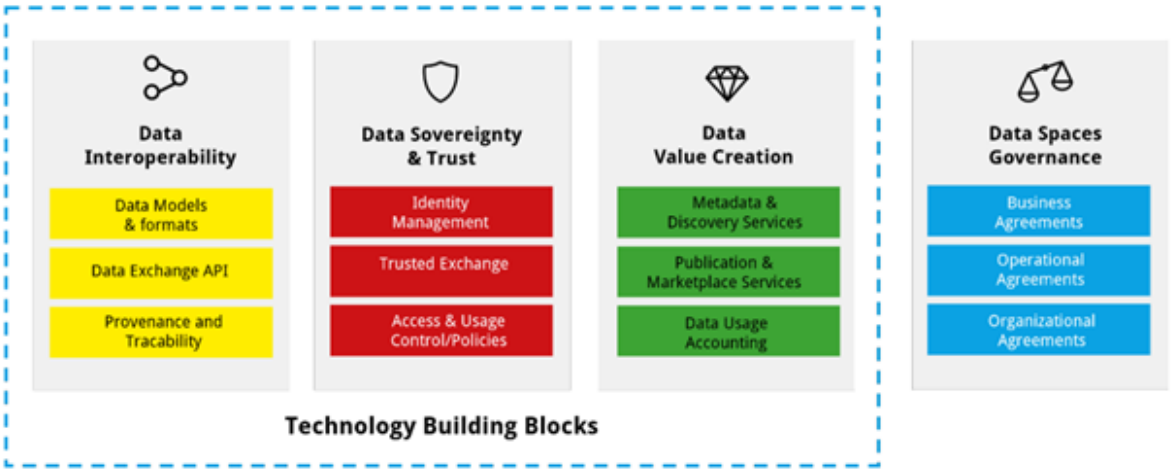

Figure 1: Data space design principles (Nagel and Lycklama, Open DEI, 2021)

Although these domains mainly provide the technical foundation for putting a federated data space into practice, especially in the logistics sector, they demand that governance mechanisms be integrated into each of them. This is essential to ensure trusted collaboration, data sovereignty, interoperability, and long-term value among diverse stakeholders. In this research, the design principles put forward by Nagel and Lycklama (2021) are used as the starting point for shaping the governance framework. Each principle is approached as a distinct governance pillar, requiring clear decision-making authority, accountability mechanisms, and operational rules to support a secure, scalable, and resilient data-sharing environment tailored to logistics. The framework also draws on the preliminary research

outlined by Vadhe and Boute (2023), which is further refined here to address the broader operational complexities of federated logistics data space.

With this foundation in place, we can now elaborate on the governance framework's four key pillars and show how they are implemented. Each pillar represents a critical aspect of governance that must be addressed to enable a secure and effective federated logistics data space.

2.1.1 Pillar 1 – Interoperability

Interoperability is the ability of different systems, organisations, and data sources to work together seamlessly. In a federated logistics data space, interoperability is the technical backbone that enables participants to actually exchange and use each other's data. Without interoperability, data-sharing efforts can falter. For example, if one port's system produces data in a format that a carrier's system cannot parse, or if there is no common reference for what a "shipment" or "location" means in data, the collaboration breaks down. Thus, interoperability is a cornerstone of effective data space, as it *"enables seamless data sharing and integration across diverse systems."* By ensuring that data can be easily understood and processed by different stakeholders' IT systems, interoperability facilitates collaboration and increases the overall uptake and usefulness of the data space within the ecosystem.

Achieving interoperability in a data space involves both technical standards and semantic alignment. On the technical side, the framework should promote standardised data exchange mechanisms. For instance, common APIs, data formats, and communication protocols. Participants should agree on using certain interface standards (such as REST/JSON APIs or specific event messaging formats) so that connecting a new data provider or consumer is plug-and-play. In the SYTaDel project, we leveraged the IDSA reference architecture as a foundation for interoperability, which provided predefined communication patterns and protocols for data exchange. Using a reference architecture that is recognised ensures that all parties followed a compatible method for connecting and transferring data. Key technical components included a federated catalogue service and standardised connector interfaces, which together established a common "language" for systems to request and send data. Additionally, the use case incorporated open-source middleware: for example, an Orion Context Broker (compliant with the FIWARE NGSI standard) was deployed to manage and share context information in real-time. This context broker acted as a hub where data (such as vessel positions, estimated arrival times, etc.) could be published and subscribed to in a uniform way. The Orion broker, along with a time-series database (for historical data), ensured that applications from different stakeholders could retrieve data using the same queries and data models. By relying on industry-accepted, open-source components, the project maximised technical interoperability and avoided vendor lock-in.

Equally important is semantic interoperability, a shared understanding of data definitions and structures. In logistics, different actors might have their own terminology or formats (one system's "ETA" might be formatted differently in another system). The governance framework should thus establish common data models or ontologies for key domain concepts. In the SYTaDel data space, an existing ontology from FIWARE for marine transport was extended to include vessel data, creating a standardised representation of information like barge identifiers, routes, and statuses across all participants. This meant that when a barge operator shared data about a vessel's position or cargo, the port terminal and shipper systems could interpret that data unambiguously. Harmonising data schemas and definitions (units of measure, date/time formats, location references, etc.) prevents miscommunication and errors. The framework can provide canonical data models or translation mappings as part of interoperability guidelines.

Another facet is data provenance and traceability. While often discussed under trust, provenance is also an interoperability concern in that any data item should carry metadata about its source and history in a standardised way. This allows systems that ingest data to know where it came from and how it's been processed. Including provenance metadata (timestamps, source IDs, etc.) for each data exchange can be part of the interoperability standards. This not only helps with data quality and auditability but also aids in integrating data from multiple sources (for example, if a delivery status is derived from several data points, traceability helps link them together).

In practice, governance for interoperability means the framework will enforce or encourage the use of these common standards. It might, for example, mandate that *"All participants must publish data through the data space using the agreed standard APIs and ontology. Data not conforming to the schema may be rejected or transformed by the data space operator to fit the common model."* During the onboarding of a new participant, there could be a checkpoint to map their data formats to the standard model. The SYTaDel project addressed interoperability challenges by performing an onboarding data mapping; when a data provider joined, its data format was mapped to the common model so that afterwards sharing with any new consumer was straightforward. Over time, maintaining interoperability may involve a governance process for updating standards (e.g., if the ontology needs to evolve) through a committee of experts drawn from the member organisations (this touches on Pillar 4, Administrative Governance, where change management for standards would be handled).

The benefits of this pillar are clear: with high interoperability, the data space can integrate systems from many logistics stakeholders, enabling richer datasets and more efficient operations. In SYTaDel, for instance, once interoperability was established, the data space could combine a barge's real-time AIS location data and an external route optimisation service, something previously very difficult when each party's data was siloed in incompatible systems. By harmonising data formats and exchange protocols across actors, the governance

framework lays the groundwork for all other pillars to function on top of a seamless data-sharing layer.

2.1.2 Pillar 2 – Data Sovereignty and Trust

The second pillar of the governance framework is Data Sovereignty and Trust, or simply Trust, which encompasses data sovereignty, security, and accountability in the data space. Establishing trust means that participants have confidence that sharing their data will not expose them to undue risk and that all parties will behave according to agreed rules. In a federated logistics data space with multiple independent actors, trust is absolutely crucial. Without it, companies will be reluctant to share valuable or sensitive information. This pillar addresses how to create a secure environment and clear rules so that each participant retains control over their data and can trust others in the ecosystem.

A core concept under this pillar is data sovereignty, which is the idea that data providers retain control over how their data is used, even after it leaves their hands. The governance framework must ensure that each organisation's rights and policies travel with the data. Practically, this is achieved through usage control policies and technical enforcement. In SYTaDel, for example, data providers could specify usage restrictions (like "this data can only be shared with particular entities and not be forwarded elsewhere"), and those policies were attached to the data via standardised formats. The framework integrated a Policy Execution Framework so that whenever data was requested or exchanged, the usage rules were checked and enforced. The use of the Open Digital Rights Language (ODRL) was one solution for encoding these data usage policies in machine-readable form, allowing automated policy enforcement in the data connectors (Akaichi et al., 2024).

Another key aspect is identity management and access control. The data space needs to ensure that only trusted, authenticated parties can participate and access data. This often means establishing a federated identity system. In our case, each participant was issued a digital identity. The SYTaDel project used walt.id, which is a wallet technology for decentralised identity to issue GAIA-X-compliant organisation identities and managed them using Keycloak (an open-source identity and access management service). Each participant (e.g., a logistics company or an authority) had to authenticate via this system to prove who they were. The governance framework thus included an onboarding process where organisations are vetted and provided with these credentials. By having strong identity verification, the data space guarantees that when data is shared, the receiver is a known, trusted party with a valid identity. Additionally, authentication and authorisation protocols (such as OAuth2 with JWT tokens, etc.) were in place for every data access request. Only parties with the right credentials and permissions (as determined by the data owner's policy) could retrieve or view data.

Security measures underpin trust as well. All data exchanges in the space were secured end-to-end. For instance, the Eclipse Dataspace Connector (EDC) acted as a secure gateway for each participant. The EDC connectors established secure communication channels and also handled the negotiation of data-sharing contracts between parties. This means that if company A wants to get data from company B, their connectors first authenticate, then A's connector sends a usage contract proposal (specifying what data, what purpose, and how long it will be used), B's connector evaluates it (checks if it aligns with B's policy), and once agreed, data flows through. This automated contract and transfer process was aligned with IDSA's recommended protocols for data exchange. The governance framework defined these interaction rules so that every exchange goes through certain phases with checks. Concretely, the SYTaDel use case implemented a three-stage data sharing process: Initiation (data owner registers the dataset and usage policy in the catalogue), Verification (data consumer requests access and must agree to the terms; the system verifies the consumer's credentials and intent), and Transfer (secure transmission of data only after terms are accepted). For example, if a barge operator offers its real-time AIS data, it would publish that offering along with conditions (e.g., "only accessible to registered port or shipper users, not to be stored beyond 24 hours"). When a shipper tries to access it, their identity is checked, and they must accept those conditions; only then does the data stream start. If any policy condition fails (say an unapproved party attempts access, or the usage time window expires), the system will deny or cut off access. These mechanisms ensure that data is only shared with authorised parties under agreed conditions, reinforcing trust.

In summary, the Trust pillar of the governance framework establishes a secure and controlled environment for data sharing. By combining strong identity management, fine-grained access control, usage policy enforcement, auditing, and legal compliance, the framework ensures that every data exchange is transparent and within agreed bounds. Participants maintain sovereignty over their data, where they know *who* is accessing it and *for what purpose*, and they have the power to allow or revoke access as they see fit. In the federated logistics space, this pillar was evidenced by the successful implementation of a trust architecture: companies that were initially hesitant to share data (like a barge company sharing exact locations) were willing to do so once they saw that the system would enforce their restrictions (e.g., only the port authority and a particular shipper could see it, and only for the duration of a voyage) and that all parties had been vetted. The result is an environment where stakeholders can trust both the infrastructure and each other in a collaborative data ecosystem.

2.1.3 Pillar 3 – Data Value Creation

Sharing data in a federated space is only worthwhile if it creates value for the participants. The Data Value Creation pillar focuses on ensuring that the data being shared is used in ways that generate tangible benefits and that there are mechanisms to capture this value fairly. It

also covers the governance of data usage by making sure that data is used according to agreed terms (overlap with the Trust pillar) and that usage is tracked and can be accounted for.

A key component here is establishing a data ecosystem that provides services or insights on top of raw data. In the SYTaDel logistics data space, merely exchanging data was the first step; the real value came from integrating that data and feeding it into decision-support tools. For instance, the project integrated external services such as the Euris ETA Service (which calculates ETA for barges) and the PILL Route Planner (which suggests optimised intermodal routes) into the data space. By doing so, participants who contributed data immediately got value in return (e.g., better ETAs for their shipments, optimised plans). Another example was Dockflow's APIs that provided real-time track-and-trace across the supply chain. These services *"significantly enhance the functionality of the data space."* Stakeholders can optimise operations using the insights, which in turn motivates them to keep sharing data. The governance framework should encourage the inclusion of such value-added services and possibly govern how they plug in. For example, there might be rules on how third-party services can access the data (to ensure they also abide by usage policies) and how any commercial arrangements are handled.

Another aspect is maintaining a federated catalogue or marketplace for data assets. Governance should ensure that data providers publish descriptions of their datasets (metadata) so that potential consumers can discover what's available. This improves discoverability. So, instead of bilateral agreements hidden from view, everyone in the data space can see a kind of inventory of data offerings (subject to access permissions). The governance rules might require that *"All shared data assets must be catalogued with clear metadata, including data definitions, update frequency, owner, and usage terms."* This transparency not only helps find data but also avoids misunderstandings about what the data represents or how current it is.

In some data spaces, especially those expected to become self-sustaining, a data marketplace mechanism is established. This could involve pricing of data or exchange of services. For logistics, one could imagine a model where, for example, a barge operator could charge a fee for providing high-precision location data or where a third-party analytics provider sells an ETA prediction service to others on the platform. In SYTaDel's case, direct pricing was not implemented in the pilot, but the framework allowed *"local freight forwarders to define data pricing rules"* as an option, and an opt-in model for data monetisation was considered theoretically.

Crucially, to measure value, usage accounting is needed. The framework put in place tools for tracking how data is used. For example, counting the number of times a dataset was accessed or logging what queries were run. This serves multiple purposes: it can feed into billing or credits if a marketplace is involved, and it provides feedback to data providers about the

demand for their data (which can justify their effort/cost in sharing it). In SYTaDel, this was done through Grafana (a dashboarding tool we used to visualise the logs) showing each provider how many times their data was queried. This kind of transparency can incentivise data sharing by demonstrating its impact. The governance framework can specify that *"The data space operator will provide regular reports to data providers on the usage of their data, including who used it and under what terms,"* which ties back into trust and accountability as well.

From a data value creation governance perspective, Pillar 3 overlaps somewhat with Pillar 2, but with a different emphasis: while Pillar 2 (Trust) ensures no misuse, Pillar 3 ensures productive use. The governance framework should encourage practices that maximise data's utility. For instance, promoting data quality improvement (garbage data has no value), encouraging data enrichment (combining datasets to create new insights), and facilitating feedback loops (letting data consumers report issues or improvements back to providers). In the case study, as data started to flow, stakeholders realised that by combining their data, they each gained a better situational picture. The framework supported this by not only allowing direct sharing but also by orchestrating those three main stages of secure data sharing (initiation, verification, and transfer) that we described.

In summary, the Data Value Creation pillar ensures the governance framework is not just about control but also about value generation and sustainability. It guides how the shared data is turned into improved operations, new services, or even financial benefits, and it ensures that usage is tracked and fair. By embedding mechanisms like data catalogues, usage policies, and accounting, the framework helps maintain a balance where providers feel rewarded (or at least see the benefit) for sharing data, and consumers get reliable, useful data to drive efficiencies. This pillar is vital for keeping participants engaged; if stakeholders see concrete returns (better ETAs, optimised routes, fewer delays, etc., as tested in scenarios in SYTaDel) from the data space, they are more likely to continue contributing data, creating a virtuous cycle of data sharing.

2.1.4 Pillar 4 – Administrative Governance (Data Space Governance)

The fourth pillar, Administrative Governance, deals with the overarching management and coordination of the data space. While the first three pillars focus on specific domains (technical interoperability, security trust, and data usage value), this pillar is about the *institutional arrangements;* the policies, processes, and organisational structures that keep the data space running smoothly and resolve issues as they arise. In many ways, Administrative Governance provides the glue that binds the other pillars together and ensures that there is a clear governance process for things like onboarding new members, making decisions about the data space's rules, and handling conflicts or changes.

A key element is defining the governance structure or bodies. Federated data space often establish a governance board or committee comprised of representatives of the participants. Another aspect is the division of administrative functions into core and extended domains. In our framework design, we distinguished between a Core Domain of administration and an Extended Domain. The Core Domain includes the foundational processes needed to start and maintain the data space's daily operations. These are things like participant onboarding, like how new companies or entities join the data space. The framework should have a clear onboarding procedure to ensure new members meet the requirements and understand the rules. It also includes establishing each member's identity in the system (linking to Pillar 2's identity management) and setting the standard terms and conditions that all participants agree to. These terms likely cover liability, data usage rights, confidentiality, etc., forming a kind of baseline contract for members of the data space. The core domain would also handle routine governance tasks like maintaining a registry of members, ensuring that certificates or connectors are up to date, and coordinating any central services (like the catalogue or identity provider).

The Extended Domain of administrative governance builds on that to cover more advanced or escalated governance needs. For instance, dispute mediation mechanisms fall here, like if two participants have a conflict (maybe one accuses another of misuse of data, or there's a disagreement on data quality), the framework should have a defined process to resolve it. This could involve the governance board as arbitrator or a predefined arbitration process. Another extended function is managing semantic translation or interoperability bridging beyond the core standards. As new data types or external data space come into play, governance might need to oversee how to integrate or translate between them (ensuring that the data space can nest or interoperate with other data space, which relates to the *nested enterprises* principle).

From an operational perspective, Administrative Governance also covers setting up monitoring and enforcement processes for the rules. Pillar 2 discussed automated enforcement for data usage; Administrative Governance includes human oversight too. There might also be a defined process for updating the governance framework itself. E.g., an annual review where all members can propose changes, which are then voted on. This ensures the framework stays living and can adapt to new challenges (technology changes, new types of data, etc.). Administrative governance should also address community management: fostering a collaborative culture among participants. Although less tangible, the framework can encourage information sharing about needs and benefits, host periodic meetings or innovation workshops, and so on, under the governance umbrella. This soft governance can be crucial in logistics, where trust between companies (some of whom might even be competitors) needs to be cultivated beyond just the technical and legal measures.

In the SYTaDel case, the administrative governance pillar was partially exercised through the project consortium itself (which acted like a proto-governance board), making decisions on data sharing agreements and technical standards during the implementation. The other aspects of the administrative governance were considered from a theoretical perspective. As the data space moves beyond the pilot, formalising that structure will be key, likely setting up an independent governing association or expanding the mandate of an existing logistics industry body to oversee the data space. By having a strong administrative governance pillar, the federated data space can remain organised, fair, and adaptable, ensuring longevity.

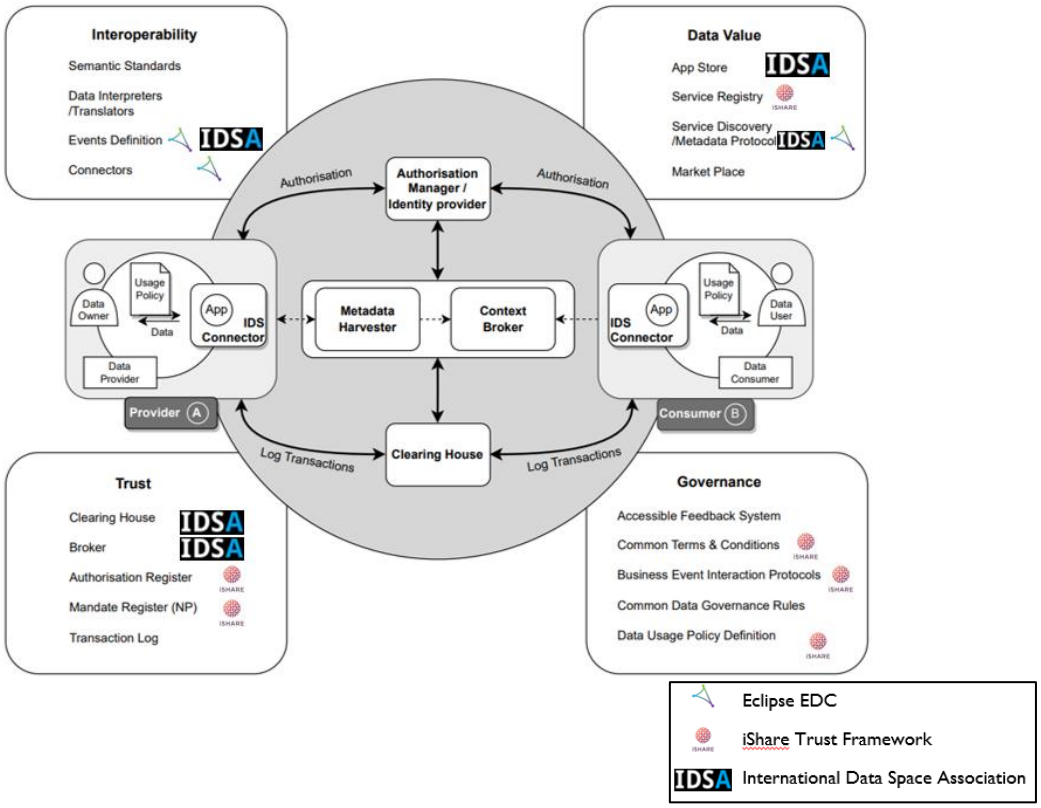

Figure 2: Overview of the governance framework

To summarise the four pillars: Interoperability provides the technical connectivity and common language for data; Trust provides the security, control, and confidence for participants to share; Data Value Creation ensures the sharing produces mutual benefits and that usage is properly governed; and Administrative Governance provides the institutional framework to manage and sustain the data space. These pillars are interdependent, and weakness in one can undermine the others. Therefore, a holistic governance framework needs to balance and integrate all four.

2.2 Define the clear state of data

In a logistics data space, data will exist in different states: primarily *at rest* (when stored in a database or system) and *in transit* (when actively moving between systems). Each state has distinct characteristics and risks. Data at rest refers to information being stored, for example, a container status record kept in a port terminal's database or shipping documents in a cloud repository. Data in transit refers to information in motion, such as real-time GPS signals streaming from a truck to a shipper's system or customs data being sent to authorities. Clearly delineating these states is important because governance measures must be tailored to the context: protecting a static database is different from securing a live data stream.

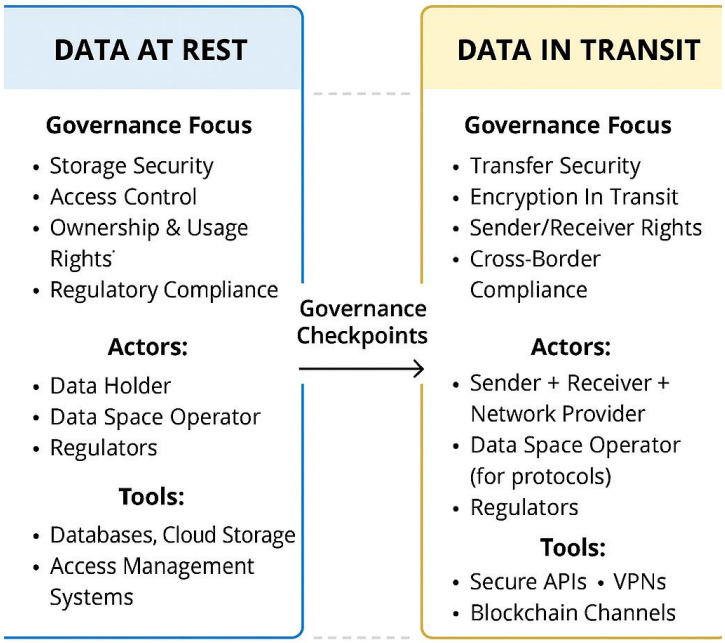

Figure 3: Summary of governance focus areas, actors, and tools for data at rest vs. data in transit in a federated logistics data space.

As Figure 3 illustrates, the governance focus shifts between data at rest and data in transit. For data at rest, the priorities include storage security (protecting databases or data lakes through measures like encryption at rest and backups) and access control within the organisation holding the data. Ensuring clearly defined ownership and usage rights is critical—who is allowed to access or share the stored data, under what conditions—as is compliance with regulations on data storage and privacy (e.g., GDPR's data residency rules). By contrast, for data in transit, the emphasis moves to secure data transfer across networks (encryption in transit, secure communication protocols) and managing sender/receiver rights—in other words, agreeing on what each party can do with data while it's being exchanged and ensuring

compliance with cross-border data transfer laws. In a federated setting, data might cross national or organisational boundaries during transit, so governance must address jurisdictional rules and liabilities during data exchange.

3 Application of the governance framework in SYTaDel

To ground the discussion, we reflect on the implementation of this governance framework in the SYTaDel project. In SYTaDel, we developed a prototype data space for the synchromodal freight transport domain, connecting various stakeholders along a transport corridor (including inland waterway barges, port terminals, logistics service providers, and authorities). The goals were to improve coordination and efficiency in multimodal transport by sharing data such as vessel locations (AIS data), terminal slot timings, and shipping documents in a controlled, federated manner. This also connects with other recent research of federated data spaces in inland waterway logistics, which demonstrate how modular architectures can support operational coordination through standardised data flows (Pulido et al., 2025).

3.1 Framework application and implementation challenges

During implementation, several governance challenges arose, which the framework helped address:

3.1.1 Heterogeneous Systems (Interoperability Challenge)

Stakeholders had different IT systems and data formats, making data exchange initially difficult. For example, barge operators used one format for AIS messages, terminals had another format for their schedules, etc. Without a common standard, integrating these was nearly impossible. The framework's interoperability pillar resolved this by establishing standard data models and APIs. The use of the FIWARE-based ontology and the Orion context broker (mentioned earlier) essentially created a translation layer so that each system could feed into and retrieve from a unified data layer. The initial mapping of each participant's data to the common model (done at onboarding) proved valuable, and once completed, it enabled data exchange thereafter. This was demonstrated when a new data service was added: since the common APIs were defined, integrating an ETA prediction service was straightforward; it subscribed to the broker and published results in the same format that others could consume. Thus, the interoperability governance not only overcame the heterogeneity but also future-proofed the data space for additional services.

3.1.2 Data Sovereignty (Trust Challenge):

Some of the data involved (like vessel tracking) could be sensitive. For instance, if it revealed business patterns or involved personal data of operators. Small family-run barge companies were particularly concerned about sharing data that might be misused or violate privacy rules. The governance framework enforced strict data protection measures to ensure compliance

and build trust. Every data transaction required a valid purpose and was logged; no personal data was shared unless necessary, and even then only under consent or contractual necessity. Integrating identity and access control (Keycloak) assured participants that *only* authorised entities (e.g., the specific port authority or a specific shipper) could access their data. Moreover, usage policies (ODRL) were applied so that, for example, a shipper accessing AIS data could not re-share it or use it beyond the agreed purpose (like it couldn't be used to analyse a competitor's performance). GDPR compliance was thus woven into the technical fabric. Data was only shared if there was a lawful basis and for the duration necessary. These measures alleviated participants' fears: one barge operator commented that having the detailed audit logs and control over access made them *"far more comfortable sharing data than in previous projects without such safeguards."* In essence, the trust pillar's implementation transformed a blocker into an enabler.

3.1.3 Enable Collaboration Among Stakeholders (Cultural Challenge):

Beyond technical and legal facets, there was natural wariness among some companies about collaborating. This is a common issue in logistics, which is that the competitive and commercial pressures can make companies hesitant to share information. The governance framework helped by providing clear rules and neutral ground. The presence of an independent governance board, or at least the project consortium acting in that capacity, signalled that this was a joint effort with equal footing. Over the course of the project, trust grew as parties saw the system working: data was exchanged without leaks, and each participant involved within the LivingLabs got useful outcomes. The framework's emphasis on collective governance (everyone having a say in the rules) also meant stakeholders felt a sense of ownership rather than feeling dictated to. This case underscores that establishing trust isn't just about technology but also about governance transparency and fairness, which our framework aimed to provide.

3.1.4 Demonstrating Value (Usage Challenge):

Early on, some questioned whether the benefits of sharing would justify the effort. The framework's Data Value pillar ensured that from the get-go, value-add features were integrated. For example, as soon as data was flowing, the ETA service and route planner were giving insights that individual companies couldn't easily compute alone. The governance framework's role here was ensuring that such metrics could be collected (with respect for privacy) and shared and that participants had the freedom to innovate with the data to create value (within the allowed usage scope). In SYTaDel's evaluation, they found the framework effectively balanced control with utility, and it aligned with broader goals of transparency, efficiency, and security in logistics.

By the end of the SYTaDel pilot, the governance framework had been applied and tested through several iterations of data-sharing scenarios. The evaluation noted that the framework

maintained data integrity, security, and privacy even as operational conditions changed, demonstrating adaptability. This suggests that the framework can scale and generalise beyond this specific corridor to other logistics contexts or geographies.

3.2 Onboarding process

Establishing a clear, secure, and scalable onboarding process is essential for trustworthy participation in any federated data space. Onboarding is more than a procedural step; it serves as the first gate through which governance principles become operational. It is where participants are verified, certified, and granted access under shared rules. In the SYTaDel project, the onboarding process was inspired by the International Data Space Association (IDSA) framework but tailored through the use of the Eclipse Dataspace Connector (EDC) to meet domain-specific and technical flexibility requirements.

The IDSA Reference Architecture Model outlines a structured, multi-stage onboarding process that ensures only verified and policy-compliant organisations are permitted to participate in a data space (IDSA, 2022). Figure 4 shows the onboarding workflow for a data space with the key steps involved. This onboarding workflow ensures that all data space actors are known, accountable, and technically aligned from the beginning.

The SYTaDel project followed the conceptual logic of the IDSA onboarding process but implemented it through the Eclipse Dataspace Connector (EDC) instead of the official IDSA connector. This allowed for greater modularity and flexibility while still maintaining trust and policy control. The steps included:

- **Identity and Credential Setup**: Instead of relying on centralised identity providers, the EDC used decentralised identity (DID) frameworks and verifiable credentials to register participants. Each organisation obtained a GAIA-X-compliant digital identity, often anchored in a federated identity service such as Keycloak.
- **Connector Deployment**: Each participant hosted their own instance of the EDC. These instances were configured to establish secure communication channels, enforce data usage policies, and exchange contract offers in line with governance rules.
- **Policy Enforcement Configuration**: Usage rules were attached to datasets through machine-readable languages such as ODRL. The EDC connectors were responsible for enforcing these policies in real time during data transfer requests.
- **Access Testing and Readiness Verification**: Prior to full access, each connector instance underwent basic functional tests, including security checks and validation of policy enforcement logic, to ensure operational compliance.

This tailored setup preserved the core objectives of trust, compliance, and interoperability while providing a more adaptable solution aligned with the logistics ecosystem's needs.

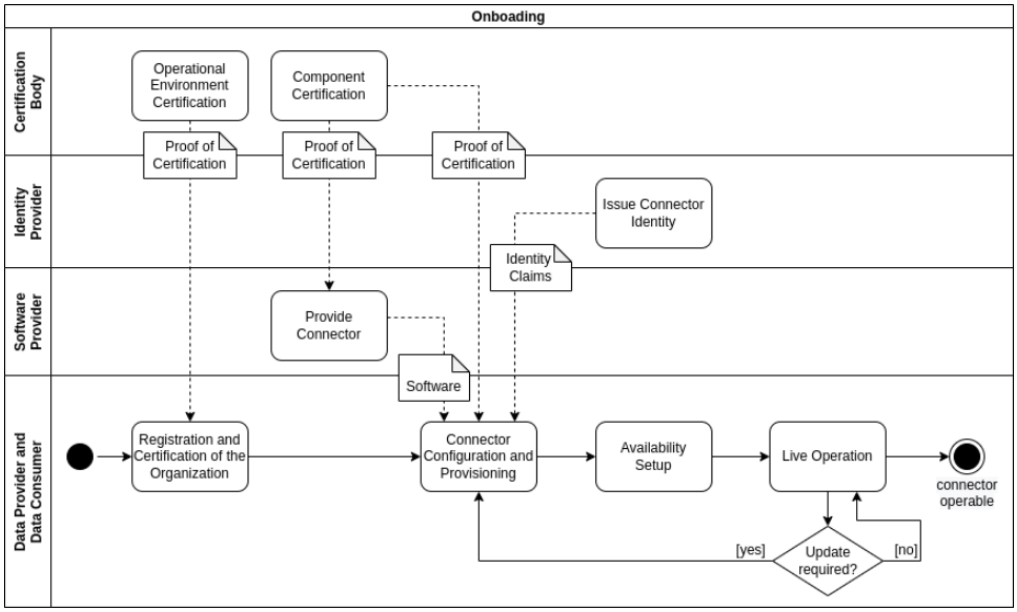

Figure 4: IDSA Onboarding Workflow for Data Space *Referred from IDSA Knowledge Base (IDSA, 2022). The visual outlines the process from registration and verification to connector activation and trusted participation.*

From a governance perspective, onboarding is the crucial checkpoint where policy, identity, and operational control converge. In SYTaDel, this process did not rely on centralised gatekeeping. Instead, it embraced a federated trust model where each participant retained their autonomy but committed to shared rules enforced via technology. Governance actions—such as identity verification, role allocation, policy validation, and enforcement setup—were embedded into the onboarding flow. The decentralised architecture, using EDC, ensured that the process was scalable and tamper-resistant. Equally important, onboarding became the first assurance point for data sovereignty. Only after completing onboarding could a participant expose datasets, and all shared data carried the participant's policies with it. Logs of these actions were retained by the data space operator, providing traceability and auditability. In this way, onboarding acted not just as a technical precondition but as a critical act of operationalising governance in a federated, trusted, and legally aligned data-sharing ecosystem.

4 Lessons Learned

In this section, we share key lessons learnt and actionable insights from a governance perspective, gathered during the SYTaDel Project. This can be useful for both researchers and practitioners who are exploring the data space solution for data sharing

- **Orchestrator for data ecosystem—A common goal:** In a federated logistics data space, the presence of an orchestrator is essential, not as a central authority but as a facilitator that helps align the interests of diverse participants. This role involves supporting collaboration, maintaining a shared vision, and coordinating governance activities to ensure interoperability and sustained engagement. By anchoring the ecosystem around a common purpose the orchestrator can help foster commitment while allowing participants to retain control over their own data and operations.

- **Accessible and fair common rules**: For governance to be inclusive and effective, the rules guiding participation and data use must be easily accessible and clearly communicated. This means using language and formats that all stakeholders, regardless of their size, technical expertise, or role can understand and apply. Co-developing these rules with participants strengthens legitimacy and ensures they reflect operational realities. Fairness is further reinforced by encoding rules in technical components where possible, enabling consistent and impartial enforcement across the ecosystem.

- **Transparent governance**: Transparency is a cornerstone of data sharing. Participants need clarity not only about the rules but also about how decisions are made, how data is used, and how compliance is monitored. This includes maintaining open access to governance documents, providing visibility into data access logs, and regularly updating participants on changes or issues. Such transparency helps build trust among stakeholders, encourages responsible behaviour, and strengthens the perceived credibility of the data space as a whole.

- **Adopt a multi-stakeholder approach from the start:** Involve representatives from all key stakeholder groups in designing the governance rules. This inclusive approach (e.g., joint working groups to define data standards or policies) ensures the framework has legitimacy and addresses real concerns. It also helps clarify roles, define early *who is responsible for what* in managing data and enforcing rules, and document these responsibilities clearly so everyone knows their duties.

- **Embed governance "by design" into the architecture:** Don't treat governance as an afterthought or merely a legal document; bake it into the technical architecture. Utilise platforms and connectors that can enforce policies automatically (for example, enforce access controls and usage restrictions at the data connector level). This way, compliance and security checks happen by default during data transactions, not manually or ad hoc.

- **No need to start from scratch:** Use existing frameworks like IDSA and GAIA-X to provide reference architectures and iShare and BDI for trust frameworks; adopt them or align with them to avoid reinventing the wheel. There are other service providers in the market that can be useful to help set up the data space governance.

- **Cultivate a culture of trust and collaboration:** Beyond formal rules, encourage relationship-building among participants. Host workshops or retrospectives on the data space usage, share success stories, and allow participants to voice concerns or suggestions. This human governance aspect will reinforce the formal framework. Participants who trust each other interpersonally are more likely to adhere to rules and share generously. The framework can mandate or recommend such meetings (for example, quarterly member forums) as part of governance processes.

By following these lessons learnt, organisations can improve their knowledge of establishing a successful federated data space. Governance is often the deciding factor in such collaborations. Strong technology can fail if governance is weak, while even moderate technology can succeed if governance is robust and accepted by all. Therefore, investing time and effort into building a sound governance framework is paramount.

5 Concluding Discussion

Building a governance framework for a federated logistics data space is a complex process. The framework presented in this report offers a structured approach, centred on the four pillars of Interoperability, Trust, Data Value Creation, and Administrative Governance, to cover the technical, ethical, economic, and organisational aspects of data sharing. The experience from the SYTaDel project illustrates that with the right governance in place, companies can overcome hesitations and collaboratively unlock efficiencies that were previously unattainable in siloed systems.

A well-designed governance framework provides clarity and assurance: it tells participants how data will be shared, protected, and used, and it establishes the mechanisms to manage this continually. For industry practitioners, this means data-sharing initiatives can be approached with confidence in security and fairness; for academics and system designers, it

offers a blueprint informed by both theory (such as Ostrom's principles and data space reference architectures) and practice. The federated approach to data in logistics—and other sectors—is still evolving, but governance will remain the linchpin of its success. As logistics networks become increasingly digital and interconnected, those that have strong governance frameworks will be able to adapt, scaling their data space while maintaining trust and interoperability across all parties.

In closing, the journey to build a federated data space is as much about governance as it is about technology. By systematically addressing interoperability, establishing trust, ensuring mutual value, and putting in place sound administrative oversight, stakeholders can create a data ecosystem that is resilient, inclusive, and innovative. The governance framework described here aims to serve as a guide for that journey, helping others to replicate and tailor the success seen in SYTaDel and paving the way for more intelligent and collaborative logistics networks in the future.

References

- Akaichi, I., Slabbinck, W., Rojas, J. A., Van Gheluwe, C., Bozzi, G., Colpaert, P., Verborgh, R., & Kirrane, S. (2024). *Interoperable and continuous usage control enforcement in dataspaces*. Institute for Complex Networks, WU Vienna & IDLab, Ghent University - imec.

- BDI – Basic Data Infrastructure. Federated Infrastructure for Secure and Sovereign Data Exchange in the Netherlands. Retrieved from https://www.basicdatainfrastructure.nl

- Eclipse Foundation. Eclipse Dataspace Connector (EDC). Retrieved from https://projects.eclipse.org/projects/technology.dataspaceconnector

- FIWARE Foundation. FIWARE Open Source Platform. Retrieved from https://www.fiware.org

- GAIA-X Association. GAIA-X: A Federated Data Infrastructure for Europe. Retrieved from https://www.gaia-x.eu

- International Data Spaces Association. (2022). IDSA Reference Architecture Model. Retrieved from https://internationaldataspaces.org

- iSHARE Foundation. iSHARE: Data Sovereignty and Interoperability in Data Spaces. Retrieved from https://www.ishareworks.org

- Keycloak. Open Source Identity and Access Management. Retrieved from https://www.keycloak.org

- Nagel, B., & van der Lycklama à Nijeholt, E. (2021). Data spaces design principles. Open DEI Project. Retrieved from https://www.opendei.eu

- ODRL – Open Digital Rights Language. Policy Expression Language for Usage Control. Retrieved from https://www.w3.org/TR/odrl-model/

- Orion Context Broker. FIWARE NGSI-LD Standard Implementation. Retrieved from https://www.fiware.org/developers/data-orion-context-broker/

- Pulido, J. M., Cardenas Barbosa, I., Carlan, V., Bergmans, T., & Vanelslander, T. (2025). Contributing to synchromodality through the implementation of a federated data space in Inland Waterway Transport. *Transportation Engineering, 21*, 100351. https://doi.org/10.1016/j.treng.2025.100351

- Vadhe, A., & Boute, R. (2023). *A data governance framework for a federated logistics data space.* Presented at IPIC 2023, Athens

- Walt.id. Digital Identity Infrastructure for Web3 and SSI. Retrieved from https://www.walt.id