beyond civic

Data Space Playbook

Governance Guideline

Author: *Beyond Civic AG*
Version: *v0.9 / 28.03.2025*

Table of content

1 Introduction 6

1.1 Purpose of Data Space Governance 6
1.1.1 Data security and privacy 6
1.1.2 Trust and collaboration 6
1.1.3 Standards and interoperability 6
1.1.4 Access and usage rights 6
1.1.5 Accountability and compliance 6
1.1.6 Sustainability and further development 6
1.2 Data Governance and Data Space Governance 7
1.2.1 Data governance 7
1.2.2 Data space governance 7
1.3 Governance Perspectives 7
1.3.1 Technical perspective 7
1.3.2 Legal perspective 8
1.3.3 Organizational perspective 8
1.3.4 Ethical perspective 8
1.3.5 Economic perspective (expanded) 8
1.3.6 Trust and communication perspective (expanded) 8

2 Scope of Data Space Governance 8

2.1 Stakeholder Alignment 8
2.2 Sponsorship / Authority 9
2.2.1 Neutrality and Advocacy 9
2.2.2 Transparency and Accountability 9
2.2.3 Inclusivity and Collaboration 10
2.2.4 Adaptability and Expertise 10
2.2.5 Interoperability and Standards Development 10
2.2.6 Ethical Stewardship and Privacy Focus 10
2.2.7 Sustainability and Long-Term Vision 10
2.2.8 Further development over time 10
2.3 Business Model Implication 11
2.3.1 Revenue Streams 11
2.3.2 Cost Management 11
2.4 Decision tree to establish a Data Space 11

3 Multi-level Governance 13

3.1 Federated services and policy 13
3.2 Cross-border adaptation 13
3.3 Governance Levels 14
3.3.1 Organizational Level 15
3.3.2 Legal Level 15
3.3.3 Semantic Level 15
3.3.4 Technical Level 16
3.4 Ecosystem orchestration with Ostrom Principles 16
3.4.1 Introduction 16

3.4.2 Clearly defined boundaries 16
3.4.3 Rules adapted to local conditions 17
3.4.4 Collective-choice arrangements 17
3.4.5 Effective monitoring 17
3.4.6 Graduated sanctions 17
3.4.7 Conflict-resolution mechanisms 17
3.4.8 Minimal recognition of rights to organize 17
3.4.9 Nested enterprises 18
3.4.10 Conclusion 18

4 Organizational form 19

4.1 Preliminary remark 19
4.2 Data Space Governance Authority as a legal entity 19
4.3 Data Space as a legal entity 19
4.4 Possible Legal Bodies 19
4.4.1 Organizational forms of international law 19
4.4.2 Organizational forms of national public law 20
4.4.3 Organizational forms of national private law 20
4.5 Possible organizational forms of national private law 20
4.5.1 Capital-related companies 20
4.5.2 Person-related companies 20
4.5.3 Which personal form of organization 21
4.6 Association requirements 21
4.7 Reasons against a cooperative as a Data Space Governance Authority 21
4.8 Characteristics of an optimal Data Space Governance Authority 22

5 Governance Authority and Operations 22

5.1 Integration of operations as a task of the Governance Authority 23
5.1.1 Advantages: 23
5.1.2 Disadvantages: 23
5.2 Separation of governance authority and operating company 23
5.2.1 Advantages: 23
5.2.2 Disadvantages: 23

6 Rulebook Overview 24

6.1 References 24
6.1.1 Current developments 24
6.1.2 SITRA Rulebook 24
6.1.3 IDSA Rulebook 25
6.1.4 DSSC Blueprint 25
6.2 Ambition and Goals 26

7 Data Ecosystem Rulebook 27

7.1 Preliminary Remarks 27
7.2 Structure 27
7.3 Rulebook: Ecosystem Reference Documents 27
7.3.1 General Terms & Conditions 27

7.3.2 Code of Conduct (CoC) 28
7.3.3 Glossary 28
7.3.4 Statutes / Articles of Association 28
7.3.5 Membership Application / Accession Agreement 28
7.4 Rulebook: Data Space Reference Documents *28*
7.4.1 Data Network Description 28
7.4.2 Interoperability Specifications 28
7.4.3 Data Sharing Agreement (DSA) 29

8 References 30

Executive Summary

The governance guideline is for all initiators of Data Spaces and data ecosystems. It serves as an orientation aid, offering inputs and starting points. Readers should have a certain prior knowledge of the principle of Data Spaces and decentralized data sharing.

The Governance Guideline establishes a clear framework for establishing, operating, and developing a data space or ecosystem. This framework addresses both cross-border data collaboration and cross-sector collaboration between the private and public sectors. The resulting governance is designed to enable a secure, efficient, and compliant data exchange while fostering trust and interoperability. These ecosystems will function as digital infrastructures that enable organizations from different sectors to exchange and use data in a controlled and transparent manner.

Data protection and security are obviously a priority, but trust and collaboration are also key. Clear rules are established to promote collaboration between stakeholders. By defining standards and interoperability, the derived guidelines will enable seamless data sharing across different sectors. It also clearly defines the logic for access and usage rights, outlining who can use data and under what conditions. Additionally, it enhances accountability and compliance, thereby mitigating risk and ensuring ethical data practices. The governance framework is designed to ensure the long-term development and sustainability of data spaces by emphasizing technological and regulatory adaptability.

Data space governance must be considered from various perspectives, including technical, legal, organizational, ethical, and economic aspects. A strategy for involving stakeholders is also necessary to align the interests of various public and private institutions. In this context, the Data Space Governance Authority (DSGA) plays a central role as a neutral and transparent instance responsible for compliance with ethical, legal, and operational regulations. It is the governing body of Data Spaces and establishes a governance model that pursues a federated approach to policies and responsibilities. This enables participating organizations to collaborate while maintaining autonomy over their data.

It also highlights several legal and business models for structuring governance authorities. An association-based governance model is clearly the preferred option because it provides the necessary flexibility and inclusivity while ensuring long-term sustainability. The guideline definitively outlines a comprehensive set of rules that will be codified in a data space rulebook. This rulebook integrates best practices from international governance models, such as the SITRA framework, IDSA standards, and DSSC draft, while also incorporating Elinor Ostrom's commons principles to ensure sustainable and fair data sharing.

1 Introduction

1.1 Purpose of Data Space Governance[1]

Data space governance is essential for managing, securing, and effectively exchanging data in a data space. A data space is a digital infrastructure that enables companies and organizations to share and use data securely and efficiently, often across different sectors. Governance is a set of rules that guarantee compliance with standards and ensure transparency and trust among the parties involved. Data space governance is necessary for the following reasons:

1.1.1 Data security and privacy

Clear governance is essential for protecting and processing sensitive data in accordance with applicable data protection laws (such as the GDPR). This is crucial to ensure the confidentiality and integrity of the data.

1.1.2 Trust and collaboration

Trust and collaboration are essential in a data space, where different stakeholders share data with each other. Governance is essential for ensuring everyone involved adheres to the same standards. Governance establishes clear rules for the handling and exchange of data, ensuring trust.

1.1.3 Standards and interoperability

Uniform standards and interoperability are essential for seamless data exchange between different systems and players. Defining common standards and protocols is crucial for this. Governance defines these standards and ensures the interoperability of the various platforms.

1.1.4 Access and usage rights

Governance defines who may use which data and under what conditions. It regulates access rights, both for the exchange and analysis of data, and ensures that these rights are transparent and traceable.

1.1.5 Accountability and compliance

Good governance ensures that everyone involved knows their responsibilities and complies with them. It ensures compliance with legal and regulatory requirements and minimizes the risk of misconduct or legal problems.
Data quality and management: Governance ensures data quality by establishing rules for data collection, processing, and validation. High-quality data is essential for companies and organizations.

1.1.6 Sustainability and further development

Clear governance ensures the data space remains functional in the long term and continues to develop. It ensures the continuous improvement of the infrastructure so that it can keep pace with technological and market-related changes.

[1] (European Commission, n.d.)

Data space governance is necessary to enable the secure, efficient, and compliant exchange of data while promoting trust, responsibility, and collaboration between the various stakeholders.

1.2 Data Governance and Data Space Governance

1.2.1 Data governance [2]

Data governance is the set of internal policies and processes that an organization uses to manage data properly. It includes defining responsibilities for data usage, protecting sensitive information, ensuring data quality, and complying with relevant legal regulations, such as data protection laws. Data governance dictates who has access to which data, how it is stored, processed, and used, and guarantees that data is consistent, correct, and trustworthy.

1.2.2 Data space governance[3]

Data space governance is the management and organization of data exchanged between organizations in a digital space or network. The aim is to enable secure and transparent data exchange between different players. Data space governance ensures that all participants can work together in a trustworthy and interoperable manner, taking into account legal, technical, and data protection requirements. It governs how data is shared, which access rights apply, and how the integrity and security of data is guaranteed throughout the network.

Data governance focuses on internal management and control of data within an organization. Data space governance goes a step further, relating to collaboration and data exchange across organizational boundaries. Data space governance ensures the efficient and secure exchange of data between different partners while safeguarding their individual interests and legal requirements.

1.3 Governance Perspectives[4]

Data space governance perspectives refer to various viewpoints and aspects that must be taken into account when designing and implementing governance in a data space. These perspectives relate to technical, legal, organizational, and ethical issues. These issues are necessary to enable the secure, transparent, and efficient exchange of data between different stakeholders. Here are the key perspectives:

1.3.1 Technical perspective

The technical perspective focuses on the infrastructure and systems that enable data exchange and interoperability between the various participants in the data space. This involves choosing the right technologies, protocols, and standards to ensure that data can be transferred securely and efficiently. This also includes mechanisms for data backup, encryption, and protection against unauthorized access.

---

[2] (ITU, The World Bank, 2024)

[3] (European Commission, n.d.)

[4] (European Commission, n.d.)

1.3.2 Legal perspective

The legal perspective addresses the legal framework and compliance with data protection regulations, such as the General Data Protection Regulation (GDPR). It clearly regulates the rights and obligations of participants in the data space, how access to data is controlled, and how the use of data is ensured in accordance with the applicable laws. This perspective is crucial to avoid legal risks and conflicts between participants.

1.3.3 Organizational perspective

The organizational perspective examines the governance structure and the distribution of roles within the data space. It defines who assumes which responsibilities, how decisions are made, and how collaboration between the various players is organized. This perspective definitively defines how the flow of data between participants is coordinated and who is responsible for the quality, security, and protection of the data.

1.3.4 Ethical perspective

The ethical perspective is more than legal and technical. It asks how to design the exchange of data according to ethical principles like transparency, fairness, and justice. The goal is clear: prevent the misuse of data and ensure that the exchange of data does justice to the interests of all participants. This perspective is crucial for fostering trust among participants and preventing ethical dilemmas when handling sensitive or personal data.

1.3.5 Economic perspective (expanded)

The economic perspective emphasizes the value of data exchange and the economic benefits that all participants can derive from collaboration. It relates to issues such as the monetization of data, the creation of added value through data access, and the fair balance between the various stakeholders. Governance must ensure that all parties can benefit from participating in the data space without unfair or one-sided advantages.

1.3.6 Trust and communication perspective (expanded)

Trust is a crucial factor in any data space. This perspective examines how trust is established and maintained among participants through clear governance rules. This includes defining transparent processes, open communication channels, and responsibility for the use of data. Governance must ensure that all stakeholders can track and monitor the use of their data.

2 Scope of Data Space Governance

2.1 Stakeholder Alignment

Stakeholder alignment in an ecosystem refers to the coordination and harmonization of the interests, goals and expectations of all relevant stakeholders within a particular system. An ecosystem can take many forms, e.g. an economic, social, ecological or technological ecosystem. Stakeholders in this context are all parties that are affected by or influence the activities and results of this ecosystem, such as companies, organizations, governments, communities, investors and customers.
Important aspects of stakeholder alignment are listed below, although these are certainly not exhaustive.

- Define common goals. It is essential to develop a clear vision and common goals that are supported by all stakeholders.
- Create transparency. An open and honest exchange of information is crucial to build trust and avoid misunderstandings.
- Promote collaboration. Stakeholder alignment is key to more effective collaboration. Stakeholders who bring different perspectives and resources to the table will achieve more effective results.
- Conflict resolution is simple: clarify interests at an early stage to minimize or resolve potential conflicts.

Stakeholder alignment is particularly important as it is crucial for the functioning and prosperity of an ecosystem. The following is a summary of some of the concrete effects.

- Align interests and goals to bundle and use resources efficiently. This will create synergies that increase value creation within the ecosystem.
- Promoting innovation is as easy as building a coordinated ecosystem. This ecosystem makes it easier to develop ideas and innovations because all stakeholders work towards a common goal and contribute their expertise.
- Avoid conflict. Stakeholder alignment is essential for avoiding tensions and conflicts that hinder collaboration and progress.
- It is essential to ensure sustainability. Coordinated action is the key to developing long-term strategies that balance economic, environmental, and social goals.
- Increase competitiveness. In a dynamic market environment, the ability of an ecosystem to respond to challenges and exploit opportunities together is a decisive competitive advantage.
- Integrate goals and values. Stakeholders who are aligned will find it easier to incorporate shared values and principles into decision-making processes. This will increase acceptance among all participants.

2.2 Sponsorship / Authority

A Data Space Governance Authority (DSGA)[5] is a pivotal entity that serves as both a sponsorship body and a regulatory facilitator. It ensures the effective establishment, operation, and sustainability of a data-sharing ecosystem. Its overarching purpose is to create a trusted and inclusive environment where data can be securely accessed, exchanged, and utilized for mutual benefit while upholding ethical standards and compliance with regulations.
The DSGA fulfills its purpose by embodying several key roles and characteristics. These enable it to balance the diverse needs of stakeholders.

2.2.1 Neutrality and Advocacy

The DSGA operates as a neutral and impartial body. It champions the creation and maintenance of the data space by securing financial, technical, and policy support. This neutrality guarantees fair decision-making and fosters trust among participants, enabling collaboration across governments, private entities, non-profits, academia, and individuals.

2.2.2 Transparency and Accountability

Transparency is central to the DSGA's operations. It communicates policies, governance decisions, and performance metrics openly to build trust and ensure accountability. Clear

[5] (Data Space Support Centre, 2024)

mechanisms are established to resolve disputes, address grievances, and manage non-compliance. This reinforces the authority's role as a trusted steward of the data space.

2.2.3 Inclusivity and Collaboration

The DSGA actively encourages the participation of a diverse range of stakeholders, ensuring equitable access and representation across sectors and regions. It fosters partnerships and promotes co-creation of policies and standards, serving as a collaborative platform that brings together data providers, users, and intermediaries to drive innovation and mutual benefits.

2.2.4 Adaptability and Expertise

The DSGA is committed to staying relevant in a rapidly evolving digital landscape. It regularly updates its frameworks to align with new technologies, regulatory changes, and stakeholder needs. Its operations are guided by a high level of expertise in legal, technical, and organizational aspects, ensuring robust governance and authoritative leadership.

2.2.5 Interoperability and Standards Development

The DSGA's core role is to establish and enforce technical, legal, and ethical standards that promote interoperability across platforms, systems, and jurisdictions. These standards guarantee seamless data exchange while maintaining data integrity, security, and privacy.

2.2.6 Ethical Stewardship and Privacy Focus

The DSGA's governance framework is built on two foundational principles: ethics and privacy. It ensures fairness, transparency, and respect for privacy in all policies and processes, encouraging responsible data usage and safeguarding against misuse. The authority aligns with global data protection laws, such as GDPR, and implements measures like encryption and anonymization to enhance data security.

2.2.7 Sustainability and Long-Term Vision

The DSGA's primary responsibility is to ensure the long-term viability of the data space. It will diversify funding sources, foster public-private partnerships, and promote sustainable practices. This will create a resilient ecosystem that will deliver societal, economic, and environmental benefits over time.
The DSGA governs the data space effectively and serves as its primary advocate, facilitator, and enabler. The DSGA achieves this by striking the perfect balance: innovation meets ethical and regulatory considerations. This creates an ecosystem where data is leveraged responsibly to unlock value and drive collective progress.

2.2.8 Further development over time

After its establishment, the DSGA embarks on a path of continuous development to adapt, scale, and sustain its operations while maintaining stakeholder trust and relevance. The DSGA starts by focusing on consolidating its internal processes, refining governance frameworks, and enhancing technical infrastructure to address early-stage challenges. Simultaneously, it fosters collaboration through stakeholder engagement, onboarding programs, and transparent communication to build trust and ensure alignment among participants.
The DSGA is expanding its scope by tailoring governance models for specific sectors, enabling cross-border collaboration, and adapting policies to emerging regulations. We

integrate advanced technologies like AI, blockchain, and privacy-preserving methods to enhance operational efficiency, security, and scalability. The DSGA ensures long-term sustainability by diversifying its funding, aligning with environmental and social goals, and implementing robust risk management strategies.
The DSGA is committed to continuous improvement, with regular feedback loops, performance audits, and iterative policy updates that keep it responsive to technological, legal, and societal changes. The DSGA has established a global presence through thought leadership, participation in international forums, and certification programs. This solidifies its reputation as a trusted leader in data governance, setting benchmarks for ethical, secure, and inclusive data-sharing ecosystems.

2.3 Business Model Implication

Developing a sustainable and adaptive business model is essential for governing the data space effectively over the long term.

2.3.1 Revenue Streams

There are various conceivable sources of revenue, although these can also be combined. Some of the most common models are mentioned below:

- Membership fees: Charging organizations for participation based on size, usage, or sector.
- Service Fees: These fees are used to monetize specialized services like compliance certifications, technical support, or premium access to resources.
- Public-Private Partnerships: Secure funding from government grants and private investments to support development and operations.
- Data Transactions: Collecting share of fees from data exchanges or licenses.

2.3.2 Cost Management

The Operational Costs cover expenses for staff, technology infrastructure, legal frameworks, and outreach programs. It is essential to design systems and policies that can scale efficiently as the data space grows.

2.4 Decision tree to establish a Data Space

The establishment of a data space commences with the identification of shared data-sharing needs among organizations, leading to the formation of a data space initiative. Initially, members reach basic agreements on their commitment, targeted sectors, and collaboration approach. These agreements can be informal. The group then develops a business model for the data space, addressing key organizational questions, such as its permanence, legal status, profit orientation, headquarters location, and member involvement in management and operations. This foundational process ensures clarity and alignment for the data space's future establishment.
With the Decision Tree, the DSSC offers a tool that can at least be used as a guide.

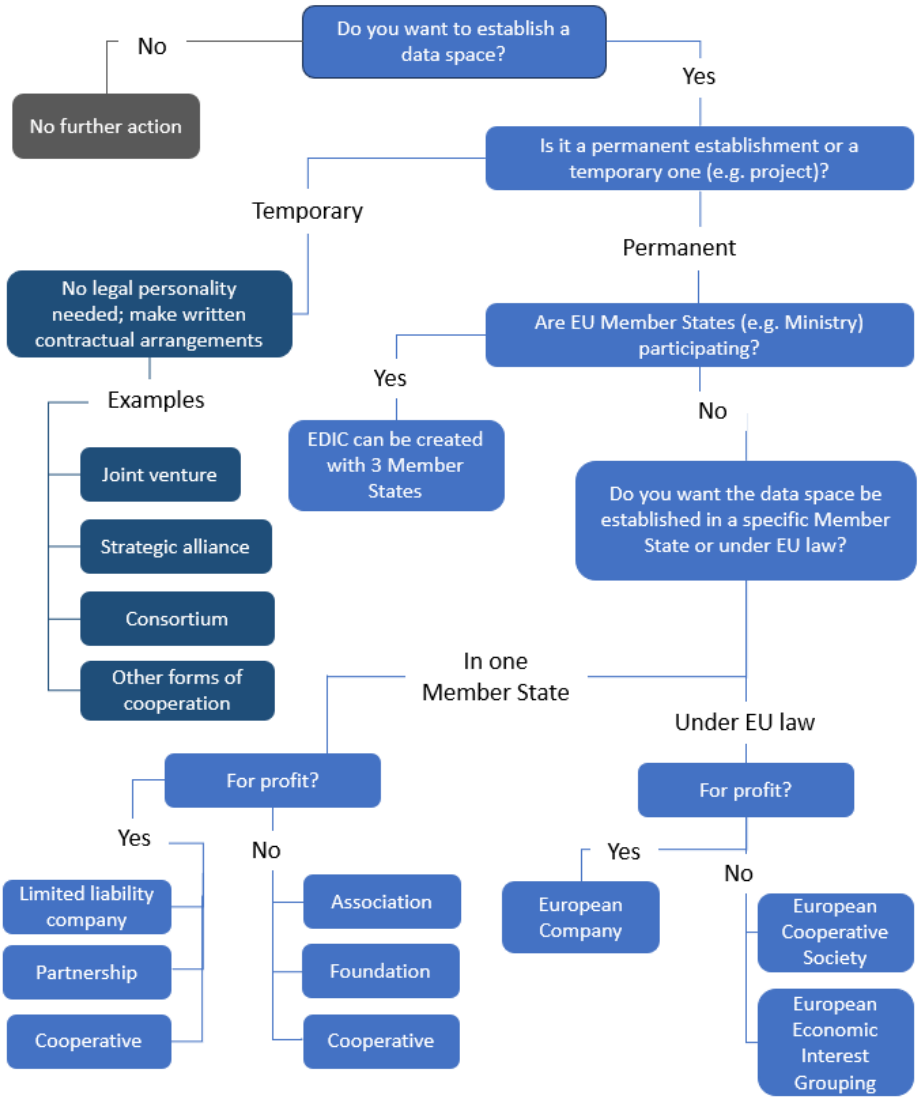

Figure 1: Decision tree including some of the core design choices for organizational form (Source: DSSC)

3 Multi-level Governance

3.1 Federated services[6] and policy

A federated policy in the context of data exchange and data spaces represents a governance model that allows independent organizations to collaborate and share data while maintaining control over their individual assets. This approach is based on the principles of decentralization, in which no single entity dominates the ecosystem. Instead, participants collaborate under a shared framework that ensures interoperability, trust, and adherence to legal and ethical standards.

Central to the federated guidelines is the concept of data sovereignty. Each organization retains ownership and control over its data and determines how it can be accessed, shared, or used. This autonomy is balanced by shared agreements that set the rules for collaboration and foster trust among participants. For example, standardized protocols and formats ensure that data can flow seamlessly between systems, while robust security measures – such as encryption and anonymization – protect sensitive information during exchange.

A federated approach also emphasizes compliance with regulations such as the GDPR or industry-specific laws, ensuring that data sharing is in line with privacy requirements and ethical considerations. This is especially important in sectors such as healthcare, where the confidentiality of patient data must be maintained, or in industrial settings, where proprietary information must be protected.

In practice, federated policies enable various use cases. In healthcare, hospitals and research institutions can securely share patient data to advance medical research without compromising privacy. In smart cities, data from various sources – such as transportation systems, utilities and public services – can be integrated to improve city management while maintaining the ownership rights of each individual participant. Similarly, manufacturers and suppliers can collaborate in industrial data spaces to optimize supply chains without revealing sensitive business information.

3.2 Cross-border adaptation

Federated policies are absolutely critical for cross-border data exchange. They provide a structured framework that balances collaboration with sovereignty, ensuring that data can move seamlessly across jurisdictions while respecting the legal, cultural, and regulatory differences of each region. In a world increasingly interconnected by digital ecosystems, the ability to exchange data across borders is essential for innovation, economic growth, and addressing global challenges. Federated policies are uniquely suited to address the complexities involved in this exchange.

The primary reason is the diversity of data protection laws and regulations worldwide. For example, regions like the European Union enforce stringent privacy standards under frameworks such as GDPR, while other countries have differing levels of regulation or varying interpretations of data rights. Federated policies are the key to ensuring that data exchange adheres to these local laws. These policies enable participants to set and enforce rules for data access, usage, and storage. This compliance-by-design approach minimizes the risk of legal violations, builds trust, and ensures ethical handling of data.

[6] (Gaia-X, 2021)

Data sovereignty is a critical issue. Organizations and governments are concerned about maintaining control over their data, especially when it crosses borders. Federated policies can be a suitable solution to reduce this difficulty. They provide mechanisms for participants to retain ownership and decision-making authority over their data while allowing controlled sharing. This is especially crucial in sectors like healthcare, finance, and defense, where sensitive data must be protected even as it flows internationally.
Federated models are key to interoperability, which is a cornerstone of cross-border collaboration. Federated policies standardize protocols, formats, and access mechanisms, enabling systems in different countries to communicate and work together efficiently. This is crucial in scenarios such as international research, where data from multiple nations must be aggregated and analyzed in a cohesive manner.
Federated policies are key to establishing trust frameworks that underpin cross-border cooperation. These frameworks define shared principles for security, privacy, and accountability, ensuring that all parties involved in the data exchange are held to the same high standards. This fosters confidence among stakeholders and encourages broader participation in global data ecosystems.
In practice, this approach drives transformative outcomes. Cross-border data exchange in healthcare leads to breakthroughs in medical research and pandemic response. In trade and commerce, federated policies seamlessly integrate supply chains across regions, enhancing efficiency and resilience. In environmental science, they enable the global sharing of data necessary to address climate change.
Federated policies are pivotal in enabling secure, compliant, and interoperable data exchange across borders, unlocking the potential of a truly global digital economy. Federated policies ensure that the benefits of data-driven innovation are realized without compromising sovereignty, security, or trust. They are a cornerstone of modern data governance.

3.3 Governance Levels[7]

The new European Interoperability Framework[8], developed by the European Commission and depicted in Figure 2, provides a systematic approach to addressing and governing interoperability challenges. (acc. IDSA Position Paper Governance[9])
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.

[7] (International Data Spaces Association, 2024)

[8] (European Commission, 2017)

[9] (International Data Spaces Association, 2021)

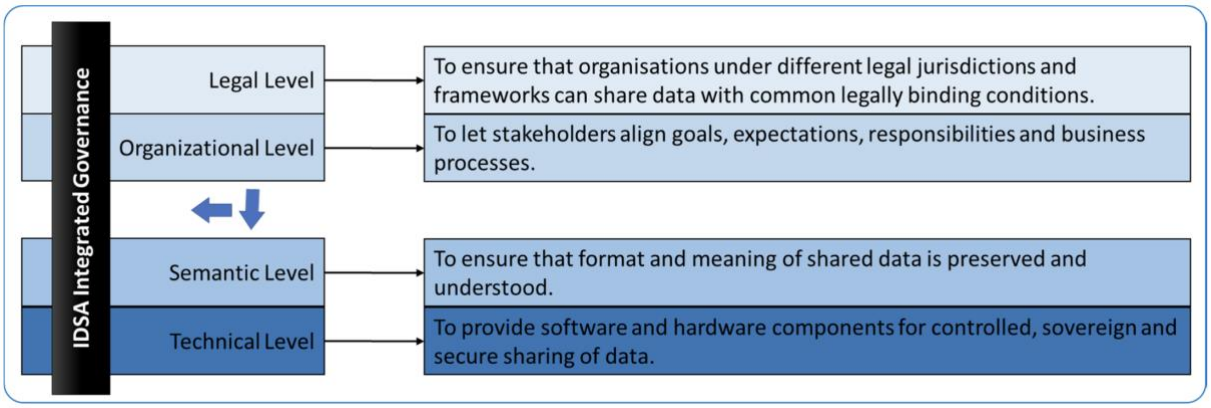

Figure 2: Layered functional model as aligned with the New European Interoperability Framework (Source: IDSA)

3.3.1 Organizational Level

This level focuses on aligning goals, responsibilities, and processes among stakeholders to ensure smooth operations within and across data spaces. Key areas include:
Onboarding and Certification: Processes to verify and authorize new participants in a data space, ensuring adherence to agreed-upon rules and standards.
Service Level Agreements (SLAs): These legal agreements mandate the maintenance of quality and performance standards for services provided within the data space.
Operational Processes: Coordinate workflows and customer service processes to enhance the user experience and efficiency.
It is crucial to establish clear organizational protocols and shared expectations. This fosters collaboration and trust among participants, ensuring that data spaces operate effectively and consistently.

3.3.2 Legal Level

Governance at the legal level guarantees data sharing compliance with varying legal frameworks and jurisdictions. It encompasses:
Joint Legal Agreements: These are frameworks that define the rules and conditions for data transactions across participants and spaces.
Verification of Legal Status: Mechanisms to confirm the legal compliance of entities before data sharing, reducing risks and ensuring adherence to governance schemes.
This level provides a strong foundation for legal interoperability. It ensures that data sharing aligns with regulatory requirements while safeguarding the rights and interests of all participants.

3.3.3 Semantic Level

This level ensures the preservation and clarity of data meaning and structure during exchanges. The challenge of achieving uniformity is due to the diversity of semantic models used by data providers and consumers. Governance at this level includes:
Common Semantic Data Models: Efforts to establish shared models to reduce complexity.
Semantic Management Data Apps: Tools that enable semantic conversions or mappings, ensuring compatibility between different data systems.
Importance: Governance at the semantic level is key to minimizing the complexities associated with interconnecting diverse systems, facilitating meaningful and efficient data usage across domains.

3.3.4 Technical Level

The technical level covers the essential hardware and software components for secure, sovereign, and controlled data sharing. It addresses the mechanics of connectivity and the implementation of interoperable systems. The technical level includes the following aspects:
Handshake Protocols: Secure peer-to-peer connections identify, authorize, and attest to the participating entities. Multiple protocols, including lightweight and hybrid approaches, cater to diverse security needs.
Identity and Authentication: Legal identities are verified at two levels. Individuals, organizations, or software components are authenticated as legal entities. These entities are registered members of a data space.
Authorization: Access and usage control policies govern data sharing. These policies align with both business needs and external regulatory frameworks.
App Enabling: The application execution environment (AEE) within the IDS Connector supports the deployment of data apps, orchestrating data flows while respecting usage policies.
Importance: At this level, governance is essential for ensuring the infrastructure is robust, interoperable, and scalable. This enables trusted data exchanges that safeguard sovereignty and meet specific security needs.

3.4 Ecosystem orchestration with Ostrom Principles

3.4.1 Introduction

Elinor Ostrom's eight principles for governing the commons[10], developed from her research on common-pool resources (CPRs), can offer valuable insights for data space governance. Data spaces refer to collaborative environments where data is shared between entities, often for the benefit of multiple stakeholders, without relinquishing control of the data. Ostrom's principles focus on local governance and collective action, which are increasingly relevant for digital environments like data spaces, where users seek to balance open access with security, privacy, and equitable usage.

Principles of Commons (acc. Elinor Ostrom):[11]

- Boundaries of users and resource are clear
- Congruence between benefits and costs
- Users had procedures for making own rules
- Regular monitoring of users and resource conditions
- Graduated sanctions
- Conflict resolution mechanisms
- Minimal recognition of rights by government
- Nested enterprises / larger networks

The following sub-chapters examine the 8 principles in relation to Data Spaces.

3.4.2 Clearly defined boundaries

The boundaries of the common resource and the community of users must be clearly defined.

[10] (Ostrom, 2015)

[11] (Williams, 2018)

In a data space, the participants (i.e., data providers, data users, and intermediaries) need clear definitions of who can access the data, under what terms, and which data assets are included. Well-defined access control policies and contractual boundaries for data usage are essential. This ensures that the data remains available for collective benefit while protecting proprietary or sensitive information.

3.4.3 Rules adapted to local conditions

Rules governing the use of the commons must be adapted to the local context.
Data-sharing agreements and rules in data spaces must reflect the specific requirements of each domain (e.g., healthcare, finance, mobility). Different sectors have varying privacy, security, and ethical concerns, and governance frameworks must be flexible and tailored to address those needs. Sensitive data like healthcare records, for example, requires stricter access rules compared to less sensitive data.

3.4.4 Collective-choice arrangements

Users of the commons must be able to participate in decision-making processes regarding the rules that govern resource use.
Data space governance must involve all relevant stakeholders (e.g., data providers, users, and intermediaries) in the development of the rules and protocols. This approach ensures that decisions about data use, privacy policies, and technical standards are inclusive and address the needs of all parties. Collaborative governance mechanisms, like data stewardship councils, are key to balancing interests and ensuring fair use.

3.4.5 Effective monitoring

Users must monitor their own resource use or assign someone accountable for doing so.
Data spaces require monitoring to ensure compliance with usage policies and to track data flows. This necessitates the implementation of automated systems for tracking data usage, access logs, and ensuring that users adhere to data sharing agreements. Transparent monitoring mechanisms are essential for accountability and preventing data misuse or breaches.

3.4.6 Graduated sanctions

Sanctions for rule violations must be graduated, depending on the seriousness and context of the offense.
Violations of data usage agreements, such as unauthorized access or breach of data privacy, will result in appropriate, proportional sanctions. These sanctions should range from warnings for minor infractions to restrictions or full denial of access for severe breaches. Graduated sanctions are key to maintaining trust while enforcing the rules fairly.

3.4.7 Conflict-resolution mechanisms

Users must have access to low-cost and effective mechanisms to resolve conflicts.
Disputes over data usage, interpretation of policies, or privacy concerns will arise in data spaces. It is essential to have clear, fair, and low-cost conflict resolution mechanisms, such as mediation or arbitration, to address these issues without derailing the entire collaborative effort. These mechanisms are essential for fostering trust and ensuring continuous collaboration among stakeholders.

3.4.8 Minimal recognition of rights to organize

External authorities must recognize and respect the self-organization of resource users.

Data space stakeholders must have the autonomy to establish their governance rules without excessive interference from external entities, such as governments or third-party regulators. However, legal frameworks must recognize the rights of these entities to self-organize, provided they comply with overarching data protection regulations (such as GDPR in Europe). This ensures flexibility in how data spaces manage their internal rules while staying compliant with legal norms.

3.4.9 Nested enterprises

Common resources are often part of larger systems, and governance should be organized in multiple layers.
Data spaces interact with other data ecosystems and networks. For example, a healthcare data space intersects with broader national health data governance frameworks. A multi-layered governance system is essential. This system must accommodate both the local data space rules and the overarching legal or regulatory frameworks (e.g., sectoral data governance regulations). Nested governance ensures coherence across different levels of data sharing.

3.4.10 Conclusion

Data spaces, like Ostrom's commons, require thoughtful governance to ensure sustainable and equitable use. The following principles highlight how Ostrom's framework for managing shared resources can be applied to data spaces:
Ostrom's commons and data spaces stress the importance of collective decision-making. This necessitates the active involvement of all relevant stakeholders to ensure diverse perspectives are considered and fair outcomes are achieved. By fostering inclusivity, data spaces can build trust and align the interests of participants.
Ostrom's principle of tailoring rules to local conditions is key to the governance of data spaces. Flexible and context-specific governance rules are essential for data spaces to adapt to the unique requirements of different types of data and sectors. This adaptability is crucial for ensuring governance frameworks remain relevant and effective.
Effective monitoring is a cornerstone of Ostrom's commons and data space governance. Regular oversight of resource use is essential for maintaining trust among participants and ensuring compliance with established rules. This oversight must include physical commons and data. Transparent monitoring mechanisms are essential for accountability and deterring misuse.
Conflict resolution mechanisms are essential for data spaces, just as they are for common-pool resources. These mechanisms address disagreements over data access, privacy concerns, and the terms of use. Well-defined conflict resolution processes are key to minimizing disruptions and upholding the integrity of the data space.
Ensure sustainable and fair data sharing.
Data space governance is the key to achieving sustainable, fair, and effective data sharing. Robust governance prevents misuse, promotes trust, and maximizes benefits for all participants, creating a shared digital ecosystem that mirrors the best practices of managing common-pool resources.
Further information regarding the implementation of the Ostrom principles can also be found on the website of the Mozilla Foundation.[12]

[12] (Anouk Ruhaak, 2021)

4 Organizational form

4.1 Preliminary remark

The choice of legal form is crucial for determining the possibilities and freedoms in the design of governance. The decision on the appropriate legal form is critical and depends on the purpose and objectives of a data space or data ecosystem. This summary is based on the circumstances in Switzerland and can only be applied to other countries and legal systems to a limited extent. The principles are comparable, making the decision criteria internationally relevant.

4.2 Data Space Governance Authority as a legal entity

The data space authority can absolutely be organized as a legal entity. In this case, the sponsoring body would be constituted as an association, and its members would be those persons or organizations (or authorities) that have a leading role (responsibility and organization in relation to the data space). Participants in the data space (providers and users) are not members of the legal entity or company; they are in a contractual relationship with each other and with the data space operator. This form guarantees the multi-level structure within the data space based on the contract between the data space operator and the participants. The details of the multi-level structure are contractually regulated in accordance with the requirements. You can also create different participant categories by designing different contract variants with different content.

4.3 Data Space as a legal entity

Another option is to organize the entire data space as a legal entity. This means that all participants (particularly data providers and data users) are involved in the company. The distinction between the data space owner and other participants, such as data providers and data users, is clear: the owner acts as a corporate body. Examples include: In the case of an association, this would be the association board and general meeting; in the case of a cooperative, it would be the board of directors and general meeting; and in the case of a limited liability company, it would be the management and shareholders' meeting. Further distinctions between shareholders (such as different categories of members) can, as far as we know, be made in particular within the framework of the articles of association. Active and passive members are one example. However, creating different categories of cooperative members would likely be challenging, as cooperative members are subject to the same rights and obligations under Art. 854 CO They have the same rights and obligations towards each other, unless an exception arises from the law. For corporations such as the AG or the GmbH, the principle of equal treatment could possibly represent an obstacle when defining different categories of members (for the GmbH, see Art. 813 CO: "The managing directors and third parties involved in the management must treat the shareholders equally under the same conditions."). It is important to note that we are making assumptions about the different requirements of the various company forms. We would like to point out that information from the relevant authorities or qualified experts is necessary in this regard.

4.4 Possible Legal Bodies

4.4.1 Organizational forms of international law

The multilateral treaty is the legal basis, but the organization lacks independent legal personality. International organizations have independent legal personality.

It is clear that organizational forms of international law do not permit the participation of private parties. In principle, only states (and international organizations) can sign an international treaty, as only these have international legal personality. However, there is a possibility of finding a way for private parties to participate in the treaty.

4.4.2 Organizational forms of national public law

"In contrast to private law, public law does not have a numerus clausus of organizational forms, i.e. the possible company forms are generally not limited. The most common forms of organization under public law are the dependent and the independent public-law institution (as dedicated assets) as well as the public-law corporation with the sub-forms of the special-purpose association, the special-law joint-stock company and the public-law cooperative."[13]
Particularly suitable in situations where the activities are to be performed under public law and the state is to obtain or retain an exclusive or majority influence on the activity.[14] .

4.4.3 Organizational forms of national private law

Legal entities under the Swiss Civil Code and the Swiss Code of Obligations (of which the state can be a member): These include associations, foundations, AGs, GmbHs, and cooperatives. Forms of organization under private law are preferable where there is an increased need for partnership-based cooperation between the state and the private sector.
Private individuals should participate on an equal footing with public authorities, so national private law is preferable to public law.

4.5 Possible organizational forms of national private law

The organizational forms of private law can be divided into person-related and capital-related companies[15] [16].

4.5.1 Capital-related companies

If the shareholder is only of interest to the company because he contributes the necessary capital, these are referred to as capital-related companies. Examples include: AG, GmbH (mixed form).

4.5.2 Person-related companies

If the person's abilities, interests, capital strength, or other factors are crucial for their participation in the company, then it is a person-related company. The ideal type is a simple partnership. Other examples include a cooperative or an association.
The primary purpose of a Data Space Governance Authority is not to inject capital. Instead, members should exchange data (which can be understood as "ability") with each other. Their person is therefore decisive — person-related companies make more sense.

---

[13] (Andreas Abegg, 2020)

[14] (Acemoglu, n.d.)

[15] (Brenda Schönenberger, 2022)

[16] (Vogt, n.d.)

4.5.3 Which personal form of organization

- This is a simple partnership: It is not long-lasting enough to be suitable. It lacks legal personality.
- General partnership: It is not suitable because only natural persons can be members.
- Cooperative: It is not suitable because at least seven members are required for formation. Membership may only be refused on the basis of reasons set out in the articles of association.
- GmbH (as mixed form between capital and person-related): It permits profit-seeking. TriRegio is not profit-oriented, so it is probably not suitable. Share capital is mandatory.
- Association: This is strictly for non-material purposes. It is highly flexible. Founders' capital not required.

There's no question: association seems to be the best choice for most data spaces.

4.6 Association requirements

Every association needs statutes, but its structure is characterized by a high degree of flexibility compared to other forms of association[17] [18].
If it engages in commercial activities, it is required to be entered in the commercial register. From a certain business volume, the association is obliged to have its accounts audited by an authorized auditor. This is the case if at least two of the following three criteria are met: a balance sheet total of CHF 10 million, a turnover of CHF 20 million, a workforce of at least 50 full-time equivalents.
In some cases, the boards of directors decide to create paid positions when voluntary work is no longer sufficient to organize the association's operations. Then, just like other companies, the association must comply with the labor code.

4.7 Reasons against a cooperative as a Data Space Governance Authority

Since in some cases it seems obvious to choose a cooperative as a form of organization, we want to shed light on the challenges involved. There are two main challenges in choosing the organizational form of a cooperative for a data space. One is the control of membership and the other is the sanctioning mechanism.
The cooperative is governed by the so-called open-door principle. This means that the cooperative must in principle be open to an unlimited number of members (see Art. 828 para. 1 and 839 CO). Entry into the cooperative must be permitted at any time and must not be made excessively difficult (Art. 839 para. 2 CO). At the same time, requirements for potential new members are permissible, provided that the purpose of the cooperative requires objectively justified personal requirements.
In this sense, it is possible to define objective criteria in advance in the articles of association that effectively limit the number of cooperative members or restrict the group of cooperative members to certain persons. The Articles of Association are adopted by the

[17] (Christa Camponovo, 2019)

[18] (SECO, 2023)

General Meeting. It should therefore not be possible for the Board of Directors (management) to refuse membership to interested persons at its own discretion.
With regard to sanctions, these must be described in the articles of association and can therefore only be assessed on a case-by-case basis to a limited extent. The articles of association may determine the grounds on which a member of the cooperative may be excluded (Art. 846 para. 1 CO).

4.8 Characteristics of an optimal Data Space Governance Authority

Cities can establish ownership by means of a constitutive agreement. The sponsoring body / Data Space Governance Authority allows public corporations as members. These members can either be founding members or join ex-post by means of an "Accession Agreement." Ex-post accession to the association is possible. All members have the same rights. If desired, different membership categories can be provided for in the statutes.
The 'Constitutive Agreement' allows members to establish the following rules and regulations: These include 'General Terms and Conditions', 'Description of Data Network', and 'Governance Model'. These rules must be recorded in the articles of association.
The Data Space Governance Authority has the lowest possible threshold for the participation of a public body. It is also durable. Public corporations can be part of an association under private law.
Data Space Governance Authority is open to the private sector. While the public sector is currently the driving force behind this initiative, companies and other organizations will be able to participate in the medium term. Private individuals can easily become part of the association. Different membership categories are available.

5 Governance Authority and Operations

The establishment and management of a data space typically necessitates two fundamental areas of responsibility that are crucial for its effective operation: Governance and operation.
The area of governance comprises the development of framework conditions, standards, and rules that ensure secure and fair data exchange. This includes defining guidelines for data protection, data sovereignty and interoperability as well as monitoring and certifying compliance with these requirements. The aim is to create a trustworthy environment that protects the interests of all participants and facilitates collaboration.
Operations would concentrate on providing and managing the technical infrastructure and implementing the defined rules in practice. This includes setting up platforms, ensuring smooth data transfer, complying with security requirements, and providing services such as access management or interoperability tools.
There are various approaches to dealing with these two areas of responsibility. One option, for example, is to have the Data Space Governance Authority (DSGA) oversee both areas of responsibility. Another option is to have the DSGA focus on governance and have one or more operating organizations handle operations.
It is important to note that the interplay between these two areas — strategic governance and operations — is crucial for the functionality and trustworthiness of a data space.

5.1 Integration of operations as a task of the Governance Authority

5.1.1 Advantages:

Consistency and centralized control: An integrated structure could combine strategy, governance and operations, which could enable coherent implementation of policies and guidelines.
Efficiency gains: The combination of governance and operational tasks could open up synergies that could lead to cost savings and shorter decision-making paths.
Faster decision-making processes: The Governance Authority has a direct influence on operations and can implement changes or new requirements immediately.
It is possible to avoid coordination problems: A single organization could eliminate the need for complex coordination mechanisms between governance and operations.

5.1.2 Disadvantages:

Conflicts of interest: It is possible that the governance authority's operational role could result in a perception of bias, which may lead to a loss of trust among stakeholders.
There is a risk of monopoly formation if the governance authority controls operations, as this could restrict competition and inhibit innovation.
It is possible that the governance authority could be overburdened by the combination of regulatory and operational tasks, which could potentially impair its efficiency.
Lack of flexibility: An integrated structure could be less adaptable to technological developments or market changes.

5.2 Separation of governance authority and operating company

5.2.1 Advantages:

Independence and neutrality of the Governance Authority: The Governance Authority is in a position to act independently and focus exclusively on defining and enforcing guidelines, standards, and rules without being influenced by operational interests. This approach is believed to contribute to enhancing the trust of stakeholders.
It would be beneficial to clarify the division of roles: The governance authority could take on the regulatory and strategic tasks, while the operating company could concentrate on technical and operational activities (e.g., platform operation, infrastructure management). This approach is intended to prevent potential conflicts between governance and operations.
It has been suggested that promoting competition: A neutral governance authority could potentially open up the market to different operating companies, which may encourage innovation and competition. This could potentially prevent monopolization of operations.
It also offers the potential for enhanced scalability and flexibility. It is possible for a separate operating company to implement scalable solutions without this being directly linked to the governance structure.

5.2.2 Disadvantages:

The coordination process is quite complex. The separation may require clear processes and mechanisms for cooperation between the governance authority and the operating company. It is possible that coordination issues may arise.
Increased costs: It is possible that two separate organizations may require more resources and lead to higher operating costs.

6 Rulebook Overview

6.1 References

6.1.1 Current developments

There are now numerous rulebooks from various institutions and research institutes. These books are subject to constant change and often refer to each other, even if different philosophies and concepts are pursued in some cases. As a general rule, these rulebooks are designed with a view to aligning with the circumstances and needs of the respective stakeholders. From our perspective, there is room for improvement in terms of addressing aspects such as public-private data exchange and cross-border data exchange. This Rulebook endeavors to address these aspects by drawing on the existing work of various European initiatives.
If I'm not mistaken, the most important underlying documents are the SITRA rulebook, the IDSA rulebook, and the DSSC Blueprint V1.5.

6.1.2 SITRA Rulebook[19]

The Rulebook Template is a resource that can be used to establish data networks and define data-sharing agreements. It is designed to assist organizations in creating rulebooks, complying with laws, and promoting a fair data economy by fostering trust and shared values.
It has been said that it highlights the benefits of data sharing, such as enabling research, improving services, and fostering innovation, while lowering costs and enhancing collaboration. It is essential that networks operate in a manner that is fair, lawful, and transparent, ensuring compliance with data protection and competition laws.
The template, which was released under a Creative Commons Attribution 4.0 license, is designed to allow for sharing and adaptation, with the understanding that credit should be given to its authors and modifications should be disclosed.

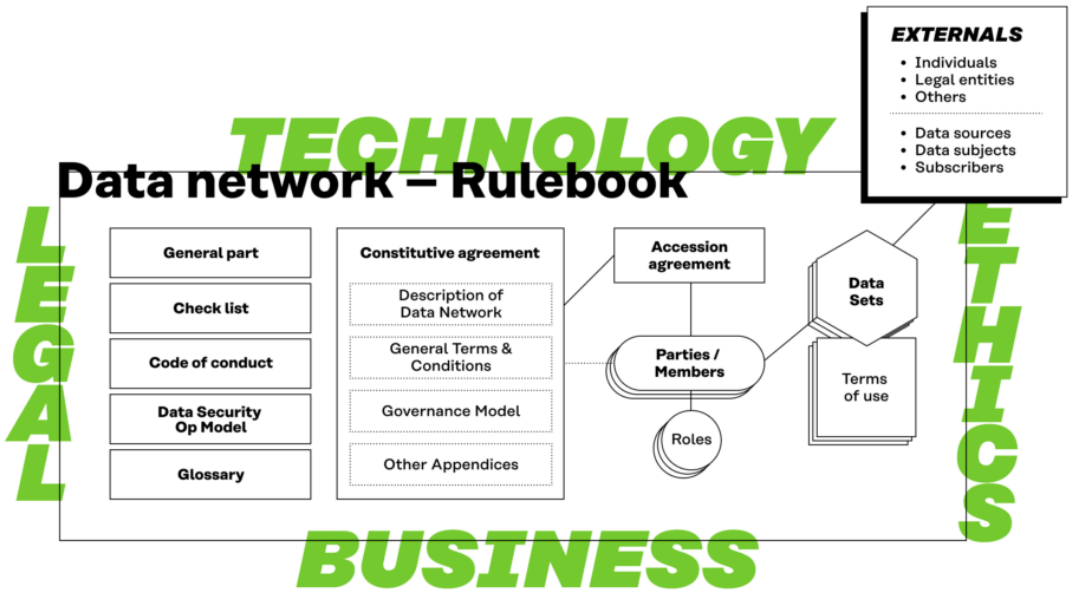

Figure 3: SITRA Rulebook, The relations between different parts of a rulebook (Source: SITRA)

[19] (Olli Pitkänen, 2025)

6.1.3 IDSA Rulebook[20]

The Rulebook is intended for businesses, organizations, and individuals involved in or considering data-driven ecosystems or business models, especially those focused on data sharing. It is a resource that may be of interest to anyone interested in participating in secure, trusted data access and sharing, including through data marketplaces, peer-to-peer systems, and platforms.

The Rulebook is intended to serve as a reference document, offering guidance on the governance framework for developing and operating data spaces. The goal of this framework is to ensure data sovereignty and secure sharing of sensitive data. It provides guidelines on functional, technical, operational, and legal aspects of data sharing, focusing on how to implement the International Data Spaces Association's (IDSA) data sharing scheme (IDS). This scheme includes a reference architecture, open-source tools, and a certification process, with the aim of establishing IDS as a global standard for secure data sharing.

The Rulebook also endeavors to define roles and responsibilities for participants, service providers, and the IDSA support organization. It is intended to serve as a guide to help ensure trust, compliance, and collaboration within data spaces, with the aim of helping organizations create business value from data.

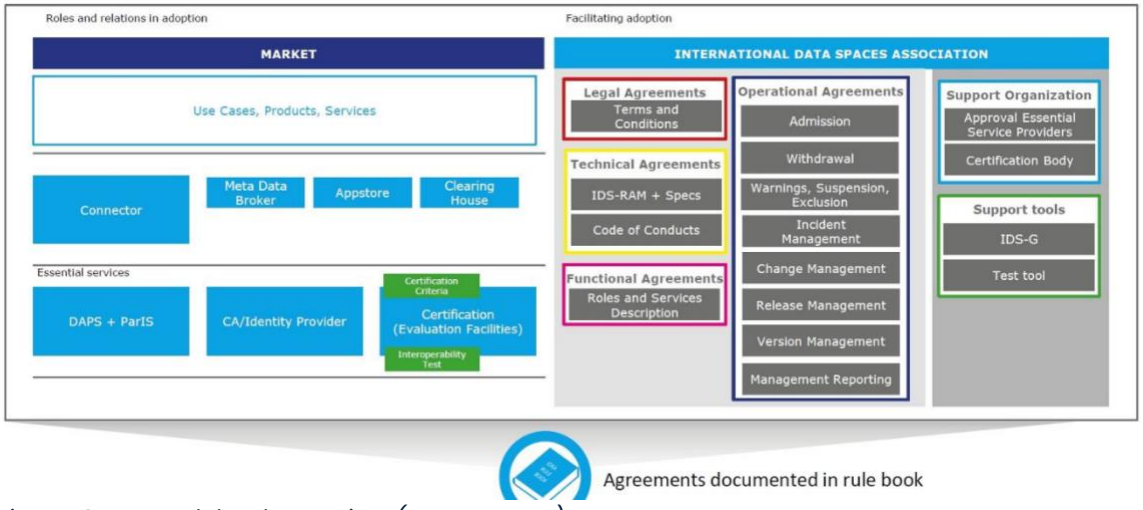

Figure 4: IDSA Rulebook overview (Source: IDSA)

6.1.4 DSSC Blueprint[21]

The DSSC Blueprint is intended for individuals who are beginning to explore the field of data spaces, offering a general introduction to key concepts. It presents a starter kit that offers an introduction to the fundamental principles behind data spaces, provides an explanation of the common vocabulary and relationships through a conceptual model and glossary, and compiles a collection of the most widely used standards across various domains. The intention is to offer a concise and easily comprehensible introduction to data spaces, assisting newcomers in grasping the fundamental concepts and terminology in this emerging field.

The DSSC Building Blocks are intended to provide descriptions, specifications, and recommended decisions for implementing the various building blocks required to deploy

[20] (International Data Space Association, 2024)

[21] (Data Space Support Centre, 2025)

a data space. It covers key aspects such as business, legal, governance, interoperability, trust, and value creation. It is intended for building block implementers, data space architects, and research projects, with the aim of offering clear specifications for creating compliant building blocks that adhere to EU regulations and recommended standards.

Figure 5: DSSC, Overview of Business & Organizational Building Blocks (Source: DSSC)

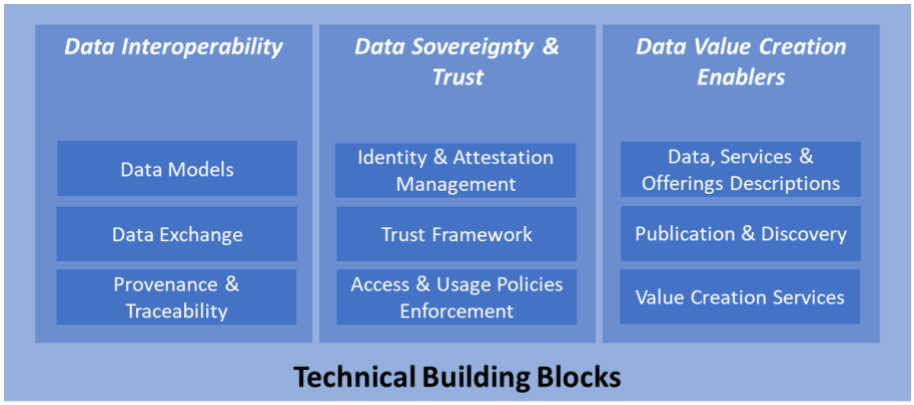

Figure 6: DSSC, Three categories of technical building blocks (Source: DSSC)

6.2 Ambition and Goals

A Data Space Rulebook serves as the fundamental framework for governing and operating data ecosystems. Its goal is to create a trusted, secure and collaborative environment in which organizations can transparently share, exchange and use data while complying with legal and ethical requirements.

At its core, the framework seeks to enable seamless data sharing by promoting mutual trust among participants, supporting technical and semantic interoperability, and enabling innovative collaborations that drive new business models, services, and solutions. Furthermore, it seeks to ensure fairness and inclusivity, allowing all participants – regardless of size or influence – to participate equally in the data space.

The objectives of a Data Space Rulebook focus on defining the roles and responsibilities of participants, establishing governance frameworks, and setting rules for data use, access, and sharing. An important priority is safeguarding data sovereignty to ensure that data owners retain control over how their data is accessed and used. The framework also aims to standardize technical requirements to enable interoperability and secure data flows, while outlining mechanisms for conflict resolution and compliance monitoring.

By embedding ethical principles and sustainable practices, the framework ensures that the data space functions in a way that respects societal values, prevents bias, and maintains confidentiality and intellectual property. It also promotes transparency and accountability, strengthening trust between stakeholders, while providing a flexible

framework that can adapt to evolving technologies, regulatory frameworks and the needs of stakeholders.

7 Data Ecosystem Rulebook

7.1 Preliminary Remarks

As mentioned in Chapter 6, the existing rulebooks already provide a well-developed basis for the development and establishment of a data space or data ecosystem along the concepts of a data space. However, these documents do not or only insufficiently address cross-border and cross-sector aspects, especially when it comes to public-private data collaboration. In particular, the hierarchy of documents and the attempt to keep as much as possible generally valid and thus to prevent a flood of documents has resulted in a certain lack of clarity and detail. For example, the place of jurisdiction for data collaboration for a cross-border data space cannot be defined centrally for all transactions. Instead, the option of individualization must be guaranteed. This means that the data sharing agreement must be much more detailed and specific.
Furthermore, the various blueprints and rulebooks do not cover the functional separation of the ecosystem and the data space. As a result, there is often confusion and a lack of clarity.

7.2 Structure

The following structure of documents was created to address the challenges of cross-border and cross-sector data sharing while taking Swiss law into account. The documents work in combination and refer to each other. In this respect, a detached view is not possible or only possible with caution.

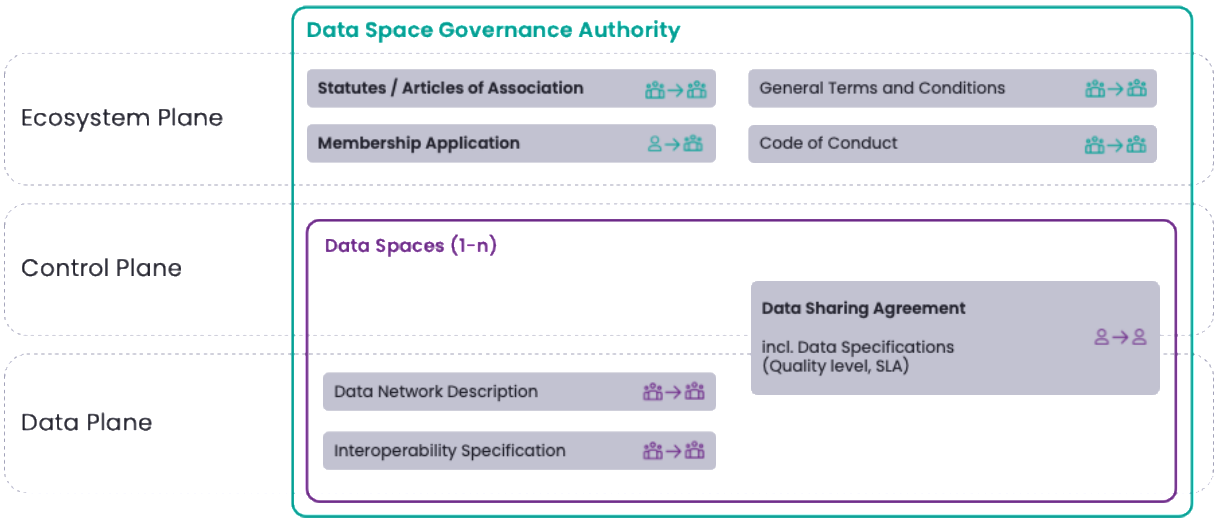

Figure 7: Data Ecosystem Rulebook Overview (Source: Beyond Civic)

7.3 Rulebook: Ecosystem Reference Documents

7.3.1 General Terms & Conditions

The general terms & conditions for a data space establish a structured framework that ensures fair, transparent, and legally compliant data sharing among participants. They build mutual trust, promote fairness, and support sustainable and ethical data practices within the network. They provide guidance to participants on complying with relevant laws

and regulations, such as GDPR, while facilitating governance through clear decision-making processes and member management.

7.3.2 Code of Conduct (CoC)

The code of conduct for data space governance is the foundational framework that guides the ethical, legal, and operational behavior of the Data Space Governance Authority and all participants. Its primary purpose is to promote trust, transparency, and accountability in data sharing and usage. The code provides a framework for responsible and sustainable data governance that benefits all stakeholders and aligns with societal values.

7.3.3 Glossary

The Data Space Glossary is a centralized reference for terms and concepts. Its primary purpose is to standardize definitions, improve communication, and foster a shared understanding among stakeholders. By aligning terminology, the glossary supports data interoperability and simplifies onboarding for new members.

7.3.4 Statutes / Articles of Association

The Statutes / Articles of Association is the foundational document for establishing an association-oriented data space organization. It formalizes an operational framework to provide a shared legal basis that defines the network's goals, roles, and responsibilities of members. It establishes governance structures, including decision-making processes and membership criteria.
The standard template is based on Swiss law. It shall be customized and once finalized, it becomes a binding framework for collaboration.

7.3.5 Membership Application / Accession Agreement

The membership application serves as an accession agreement for the seamless integration of new members into an existing data network in accordance with the statutes. Its main objective is to formalize the onboarding process and ensure that new members agree to abide by the established rules, governance structures, and operating standards of the network. The procedure for admitting new members is regulated in the statutes/articles of association.
The membership application has been created under Swiss law and can be adapted or created in variants depending on the categories of members.

7.4 Rulebook: Data Space Reference Documents

7.4.1 Data Network Description

The Data Network Description of a data space serves as a definition and structured framework that outlines the components, participants and policies for data exchange within an ecosystem. It describes the mechanisms for data exchange, including technical standards and secure communication. The description defines technological infrastructure and trust mechanisms to ensure transparency, accountability and compliance.

7.4.2 Interoperability Specifications

Interoperability Specifications of a data space define the technical, semantic, organizational, and legal standards and frameworks that enable seamless, secure, and efficient data exchange between participants within the space. These specifications

ensure that different systems, platforms, and stakeholders can collaborate effectively while adhering to shared rules and principles.

7.4.3 Data Sharing Agreement (DSA)

A Data Sharing Agreement (DSA) is a formal document that governs how data is shared between participants, while ensuring compliance with the principles, rules and governance framework of the data space. DSAs define rights of use, restrictions and license terms, ensuring that data is used trustworthy and within agreed boundaries. The agreement is aligned with the data space's interoperability standards and covers technical, semantic, organizational and legal aspects to ensure seamless and secure data sharing.
More and more model contracts[22] are being provided to handle the complexity of the wide range of DSAs. These are predefined, standardized legal templates designed to facilitate and optimize the conclusion of data sharing agreements.

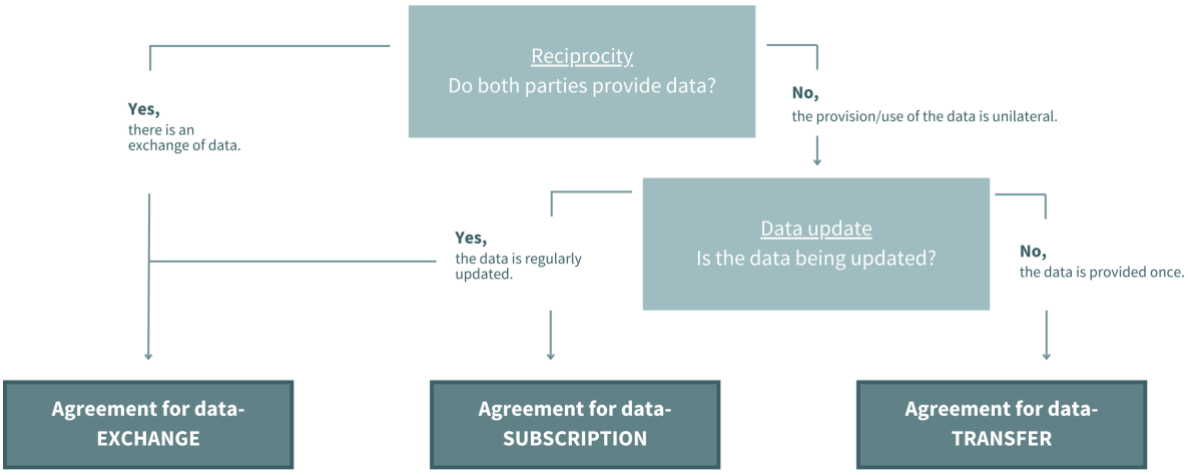

Figure 8: Model Contract Decision Tree from the Swiss Intellectual Property Institute (IPI)

The model contracts from the Swiss Intellectual Property Institute are design in sucha way that they should be compatible with European law. They can therefore be used for cross-border transactions within EU member states and between the EU and Switzerland. The place of jurisdiction for the contract is always that of the data provider / data holder. There is no obligation under European law that the place of jurisdiction for the contract must be in the country of the data consumer / data user. Furthermore, we are not aware of any national or regional regulations that would provide for such a rule. Such regulations would most likely be in violation of European law and therefore void.

[22] (IGE / IPI, 2024)

8 References

Acemoglu, T. (n.d.). *#06 Trägerschaften: So gelingt die gemeinsame Umsetzung von E-Government-Lösungen*. Retrieved from Digitale Verwaltung Schweiz: https://www.digitale-verwaltung-schweiz.ch/blog/6-traegerschaften-so-gelingt-die-gemeinsame-umsetzung-von-e-government-loesungen

Andreas Abegg, M. F. (2020). *Kriterien für die Wahl der Rechtsform öffentlicher Unternehmen.* Von recht - Zeitschrift für juristische Weiterbildung und Praxis, 1/20: https://www.unilu.ch/fileadmin/fakultaeten/rf/institute/wirtschaft_regulierung/05_Newsletter/2020/Abegg-Frei_Wahl-der-Rechtsform-oeffentlicher-Unternehmen_recht-1-2020-37.pdf abgerufen

Anouk Ruhaak, G. B. (2021). *A Practical Framework for Applying Ostrom's Principles to Data Commons Governance.* Von Mozilla Foundation: https://foundation.mozilla.org/en/blog/a-practical-framework-for-applying-ostroms-principles-to-data-commons-governance/ abgerufen

Brenda Schönenberger, M. G. (2022). *Unterschiedliche Rechtsformen.* Von vitamin B: https://www.vitaminb.ch/uploads/media/default/2761/Rechtsformen_2022.pdf abgerufen

Christa Camponovo, M. G. (2019). *MERKMALE DES VEREINS.* Von vitamin B: https://www.vitaminb.ch/uploads/media/default/1550/Merkmale%20des%20Vereins2019.docx.pdf abgerufen

Data Space Support Centre. (2024). *Organisational Form and Governance Authority* . Retrieved from Data Space Support Centre - Blueprint v1.0: https://dssc.eu/space/BVE/357074549/Organisational+Form+and+Governance+Authority

Data Space Support Centre. (2025). *Data Spaces Blueprint v1.5*. Retrieved from Data Space Support Centre: https://dssc.eu/space/bv15e/766061169/Data+Spaces+Blueprint+v1.5+-+Home

European Commission. (2017). *The New European Interoperability Framework* . Von European Commission - ISA2: https://ec.europa.eu/isa2/eif_en/ abgerufen

European Commission. (n.d.). *3.1. Governance Perspective*. Retrieved from European Commission - JRC Data Spaces Knowledge Base: https://wikis.ec.europa.eu/display/jrcdataspaceswiki/3.1.+Governance+Perspective

European Commission. (n.d.). *3.3. Data Governance*. Retrieved from European Commission - JRC Data Spaces Knowledge Base: https://wikis.ec.europa.eu/display/jrcdataspaceswiki/3.3+Data+Governance

European Commission. (n.d.). *3.4. Governance within Common European Data Spaces*. Retrieved from European Commission - JRC Data Space Knowledge Base: https://wikis.ec.europa.eu/display/jrcdataspaceswiki/3.4.+Governance+within+Common+European+Data+Spaces

Gaia-X. (2021). *Gaia-X Federation Services (GXFS).* Retrieved from Gaia-X Ecosystem Kickstarter: https://gaia-x.eu/wp-content/uploads/files/2021-12/GXFS_1.pdf

IGE / IPI. (2024). *Model agreements* . Von IGE - Intellectual property: https://www.ige.ch/en/intellectual-property/ip-and-society/access-to-non-personal-data-in-the-private-sector/model-agreements abgerufen

International Data Space Association. (2024). *IDSA Rulebook*. Retrieved from International Data Space Association: https://internationaldataspaces.org/idsa-rulebook/

International Data Spaces Association. (2021). *Governance for Data Space Instances.* Von International Data Spaces Association: https://internationaldataspaces.org/wp-content/uploads/IDSA-Position-Paper-Governance-for-Data-Space-Instances-Aspects-and-Roles-for-IDS-Stakeholders.pdf abgerufen

International Data Spaces Association. (2024). *Interoperability in Data Spaces*. Retrieved from International Data Spaces - IDS-Knowledgebase: https://docs.internationaldataspaces.org/ids-knowledgebase/idsa-rulebook/idsa-rulebook/3_interoperability

ITU, The World Bank. (2024). *Navigating Data Governance: A Guiding Tool for Regulators*. Retrieved from Digital Regulation Platform: https://digitalregulation.org/navigating-data-governance-a-guiding-tool-for-regulators/

Olli Pitkänen, M. T. (2025). *Rulebook model for a fair data economy (version 3.0)* . Retrieved from SITRA: https://www.sitra.fi/en/publications/rulebook-for-a-fair-data-economy/

Ostrom, E. (2015). *Governing the Commons.* Retrieved from Cambridge University Press: https://www.cambridge.org/core/books/governing-the-commons/A8BB63BC4A1433A50A3FB92EDBBB97D5

SECO. (2023). *Wie gründet man einen Verein und welche Motivation steckt dahinter?* Retrieved from KMU-Portal des SECO: https://www.kmu.admin.ch/kmu/de/home/aktuell/monatsthema/2023/wie-gruendet-man-einen-verein-und-welche-motivation-steckt-dahinter.html

Vogt, P. D.-U. (n.d.). *Gesellschaftsrecht*. Retrieved from Lehrstuhl für Privat- und Wirtschaftsrecht: https://www.rwi.uzh.ch/static/elt/lst-vogt/gesellschaftsrecht/einfgesellschaft/de/html/index.html

Williams, J. (2018). *Elinor Ostrom's 8 rules for managing the commons.* Retrieved from The Earthbound Report: https://earthbound.report/2018/01/15/elinor-ostroms-8-rules-for-managing-the-commons/