

Data Space Blueprint

Functional Requirements

Author: *Beyond Civic AG*
Version: *v0.9 / 25.03.2025*

Table of Content

Executive Summary	3
1 Introduction.....	4
1.1 Goal of this document.....	4
1.2 Structure of the document	4
1.3 Audience.....	4
1.4 Scope and Limitations of this document	4
1.5 Disclaimer.....	5
1.6 Acronyms used in this document.....	5
1.7 Mandate.....	5
1.8 Relationship with other reports.....	5
2 Definition of functional requirements.....	6
2.1 Definition of a functional requirement	6
2.2 Requirements Notation and Conventions.....	6
2.3 Categorization Regarding Data Interoperability	7
2.4 Categorization regarding DSSC Building blocks.....	7
2.5 Categorization Regarding Trustworthy Data Space Principles.....	7
3 Functional Requirements.....	9
3.1 Functional Requirements from Data Provider.....	9
3.2 Functional Requirements from Data Recipient.....	13
3.3 Functional Requirements from Data Space Governance Authority	16
3.4 Functional Requirements from Data Producer.....	19
3.5 Functional Requirements from Data Subject	21
3.6 Functional Requirements from Data Steward	23
3.7 Functional Requirements from Data Scientist/Engineer	25
3.8 Functional requirements from Legal counsel.....	27
3.9 Functional Requirements from Data Space Auditor / Regulator.....	28
4 Analysis.....	29
4.1 Requirements per trustworthy data space principle.....	29
4.2 Requirements per DSSC Building Block	30
4.3 Requirements grouped by interoperability focus.....	31
4.4 Requirements per Stakeholder.....	32
4.5 Categories or themes of functional requirements	33
5 References	34

Executive Summary

This document outlines the functional requirements to design a Trustworthy Data Space in Switzerland. It draws attention to the basic principles of trustworthy data spaces identified by the Swiss Government, those are: Transparency, Control, Fairness and Effectiveness.

It also overlayed the requirements with 5 of 6 Data Space Building Blocks introduced by the European Data Spaces Support Centre including: Governance, Data interoperability, Data sovereignty and Trust, and Data value Creation Enablers.

The proposed system supports the design of data spaces that facilitate collaboration among diverse stakeholders of the Swiss Data Ecosystem including Data Providers, Data Receivers, Governance Authority, Data Engineers, Legal Counsels and others.

Each high-level stakeholder requirement is then broken down into specific, actionable functional requirements, focusing on the system's behaviour and responsibilities emphasized from the stakeholder's perspective when interacting with the system.

The document concludes with an analysis of the functional requirements, amongst the key findings, the functional requirements identified fit into the following trustworthy principles: Control (35%) and Responsibility (20%); Concurrently they align mostly with the following DSSC Building Blocks: Governance (40%) and Data Value Creation Enablers (25%). Finally, most of the requirements fit on Data Governance (58%) identified by the Data Interoperability Focus report.

1 Introduction

This document aims to enumerate functional requirements for data spaces. Each functional requirement is expressed using terminology based on RFC2119.

1.1 Goal of this document

The goal of this document is threefold:

1. To create stakeholder alignment on the business needs of data space solutions.
2. To create a shared understanding of the solution scope.
3. To provide a basis for decision-making regarding data space solutions.

1.2 Structure of the document

This document introduces the reader to what are functional requirements, theoretical frameworks to classify such requirements, it groups them into high-level requirements for each stakeholder identified in the baseline document (Beyond Civic AG 2025) and finally, it decomposes the high-level requirements into fine-grained functional requirements.

1.3 Audience

This document is intended for a diverse group of stakeholders involved in developing, implementing, and utilising data ecosystems. The audience includes:

- Sponsors of public-private data ecosystems, such as governmental agencies that provide funding and governance oversight.
- Subject matter experts who offer domain-specific insights in data spaces.
- Software architects responsible for integrating systems with data spaces.
- Data space solution vendors supplying products and services for enterprise data sharing.
- Data space participants who contribute and consume data in the Swiss Data Ecosystem.

1.4 Scope and Limitations of this document

The document is written in the Swiss/European context, it is sector-agnostic, and it provides a list of concrete functional requirements for data space initiatives in the Swiss Data Ecosystem.

The document provides a general framework and may require tailoring to specific contexts and regulatory landscapes. While this report addresses common legal considerations, it's not a substitute for professional legal advice, and readers should consult with legal experts to ensure full compliance with applicable regulations, especially regarding data protection and privacy.

This report does not cover the technical requirements, which will be included in a separate report.

1.5 Disclaimer

The information provided in this report is intended for informational purposes only. Any actions taken based on this content are at the reader's risk. While we have made every effort to ensure accuracy, we make no warranties or representations regarding the information's completeness, reliability, or suitability.

It is based on the provided sources and represents a synthesis of the information available at the time of writing. However, the rapidly evolving nature of the data space landscape may lead to new developments and considerations beyond the scope of this document.

Furthermore, the success of data spaces hinges on factors beyond the scope of this document, including stakeholder commitment, clarity of the use cases, and the availability of adequate resources.

1.6 Acronyms used in this document

Term	Definition
DSSC	Data Spaces Support Centre
EU	European Union
CH	Switzerland

1.7 Mandate

Beyond Civic AG, a company based in Luzern was asked to work together with the Federal Chancellery and the Federal Department of Foreign Affairs to produce a report for the General Public by the end of 2024 on the functional requirements for trustworthy dataspaces in Switzerland. The report should cover national and international perspectives while taking into consideration previous art related to the topic.

1.8 Relationship with other reports

The present report is part of a series of documents mandated by the Swiss Federal Chancellery and the Swiss Federal Office of Foreign Affairs which include Baseline, Scope and Stakeholders of Trustworthy Data Spaces in Switzerland (in progress) Data Collaboratives Playbook (in progress), Rulebook for Data Collaboratives in Switzerland (in progress), Functional Requirements for Data Spaces in Switzerland (this document), Technical Requirements for Data Spaces in Switzerland (in progress).

2 Definition of functional requirements

The following section presents the relevant concepts and theoretical frameworks used to define the functional requirements of this document.

2.1 Definition of a functional requirement

This document defines Functional requirements as “the outline of what the system must do, its features and user-facing behaviours” (Intellisoft 2024).

2.2 Requirements Notation and Conventions

In requirements engineering, the terms “MUST”, “MUST NOT”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “NOT RECOMMENDED”, “MAY”, “MAY NOT”, “OPTIONAL” are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] (Bradner s.d.). The following is an excerpt adapted from RFC2119:

1. **MUST** This word, or the terms “REQUIRED” or “SHALL”, mean that the definition is an absolute requirement of the specification.
2. **MUST NOT** This phrase, or the phrase “SHALL NOT”, means that the definition is an absolute prohibition of the specification.
3. **SHOULD** This word, or the adjective “RECOMMENDED”, means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
4. **SHOULD NOT** This phrase, or the phrase “NOT RECOMMENDED” means that there may exist valid reasons in particular circumstances when the behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.
5. **MAY** This word, or the adjective “OPTIONAL”, means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option **MUST** be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein, an implementation which does include a particular option **MUST** be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

2.3 Categorization Regarding Data Interoperability

When possible, the functional requirements are classified into one of the following four focus areas of data interoperability (High-Level Forum on European Standardisation 2024):

Data Governance

Lays the groundwork for trusted data sharing by outlining procedures and frameworks for managing data access, retention, and quality.

Data Discovery

It enables users to find relevant datasets through catalogues and peer-to-peer networks.

Data Sharing

Underpinned by contractual agreements and secure exchange mechanisms, focuses on fair value allocation and leverages data intermediaries and altruistic organizations.

Data Usage

Addresses the integration and interpretation of shared data, often relying on semantic technologies and domain ontologies for accurate meaning representation.



Figure 1. Data Interoperability Focus Areas. Adapted from (High-Level Forum on European Standardisation 2024)

2.4 Categorization regarding DSSC Building blocks

Each stakeholder requirement has been classified in at least one of the building blocks identified by DSSC (Data Spaces Support Centre 2024). This is done to ensure alignment with the major European initiatives regarding data spaces.

Business and Organisational Building Blocks Version 1.5

- Business
- Governance
- Legal

Technical Building Blocks Version 1.5

- Data interoperability
- Data sovereignty and trust
- Data value creation enablers

2.5 Categorization Regarding Trustworthy Data Space Principles

Each stakeholder requirement has been classified in at least one of the principles identified by the Swiss Confederation concerning Trustworthy data spaces, which are: Transparency, Control, Fairness, Responsibility and Efficiency (Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK; Eidgenössisches Departement für auswärtige Angelegenheiten EDA 2022).

Transparency: Transparency allows users to acquire the necessary knowledge and insight into how a data space operates (understanding) and gives them the possibility to conceptualise the expected processes.

Control: It means that individuals can effectively exercise their rights when they wish to do so. It gives users the option of becoming active if necessary, going beyond the state of merely being.

Fairness: The principle of fairness guarantees fair treatment to all participants. It does not, however, mean equal treatment within a data space, since differences in roles and forms of governance can mean differences.

Effectiveness: Data spaces are only effective if they allow the relevant data to be exchanged and used without problems.

3 Functional Requirements

This section outlines the specific functionalities and capabilities that the data space implementation must provide to meet the main tasks of stakeholders. These functional requirements serve as a blueprint for designing and developing a system that effectively supports data sharing, interoperability, and collaboration within a trustworthy data space.

3.1 Functional Requirements from Data Provider

SR-DP-1: Data Provider must have the possibility to register their collaborators using standard identifiers (email, credentials).	
Trustworthy Data Space Principle:	Control
DSSC Building block:	Governance
Interoperability Focus Area:	Data Governance

FR-DP-1	Collaborator Registration Interface: The system shall provide a user interface that allows Data Providers to register collaborators by entering their organisational email addresses and/or relevant credentials.
FR-DP-2	Standard Identifier Authentication: The system shall authenticate collaborators using their registered organisational email addresses and/or credentials, ensuring secure access to relevant data and functionalities.

SR-DP-2: Data Provider must be given secure and controlled mechanisms to share data stored in their preferred technology stack (cloud, on-premise or hybrid).	
Trustworthy Data Space Principle:	Control
DSSC Building block:	Data sovereignty and trust
Interoperability Focus Area:	Data Sharing

FR-DP-3	Secure Data Sharing Interface: The system shall provide a secure mechanism that allows Data Providers to share data stored in their preferred technology stack with authorized recipients, ensuring encryption during transmission and access only by authenticated users.
FR-DP-4	Access Control Management: The system shall enable Data Providers to define and manage access permissions for shared data, allowing them to specify who can view, modify, or distribute the data, and to revoke access as needed.

SR-DP-3: Data Provider must be able to publish data products including their metadata and versioning.	
Trustworthy Data Space Principle:	Transparency
DSSC Building block:	Data value creation enablers
Interoperability Focus Area:	Data Discovery

FR-DP-5	Data Product Publishing Functionality: The system shall allow Data Providers to publish data products by defining connection details along with their associated catalogue metadata, making them accessible to authorized users or platforms.	
FR-DP-6	Metadata, Tagging, and Versioning Support: The system shall support the addition and management of catalogue metadata, tagging, and versioning for each published data product, enabling Data Providers to describe, categorize, and track changes to their data over time.	

SR-DP-4: Data Provider must be able to draft data-sharing agreements that best fit their business.

Trustworthy Data Space Principle:	Fairness
DSSC Building block:	Legal
Interoperability Focus Area:	Data Sharing

FR-DP-7	Customizable Data Sharing Agreement Creation: The system shall enable Data Providers to draft and customize data-sharing agreements within the platform, allowing them to specify terms, conditions, and clauses that align with their specific business needs.
FR-DP-8	Agreement Template Library with Editing Capabilities: The system shall offer a library of standard data-sharing agreement templates that Data Providers can select and modify, providing flexibility to adjust legal language, permissions, and restrictions to best fit their business objectives.

SR-DP-5: Data Provider must be given the instruments to monitor and audit the access and usage of the data products offered.

Trustworthy Data Space Principle:	Responsibility
DSSC Building block:	Governance
Interoperability Focus Area:	Data Governance

FR-DP-9	Access Monitoring Dashboard: The system shall provide Data Providers with a dashboard that displays real-time and historical data on access and usage of their offered data products, including details such as who accessed the data, when it was accessed, and what actions were performed.
FR-DP-10	Comprehensive Audit Logging and Reporting: The system shall maintain detailed audit logs of all interactions with the Data Provider's data products and shall enable Data Providers to generate customizable reports for auditing purposes, supporting compliance and internal review processes.

SR-DP-6: Data Provider must be given the instruments to monitor the quality of the data products according to corresponding agreements.

Trustworthy Data Space Principle:	Responsibility
DSSC Building block:	Data value creation enablers
Interoperability Focus Area:	Data Governance

FR-DP-11 **Data Quality Monitoring Tools:** The system shall provide instruments that enable Data Providers to monitor the quality of their data products, including features such as data validation, integrity checks, and quality metrics dashboards.

FR-DP-12 **Agreement Compliance Assessment:** The system shall allow Data Providers to evaluate the quality of their data products against the standards specified in corresponding agreements, providing reports and alerts when quality criteria are not met.

SR-DP-7: Data Provider must be able to define and manage data usage policies in a machine-readable format.

Trustworthy Data Space Principle:	Control
DSSC Building block:	Data sovereignty and trust
Interoperability Focus Area:	Data Sharing

FR-DP-13 **Policy management dashboard:** The system shall provide a user-friendly interface for Data Providers to define and manage data usage policies, including but not limited to permissions, restrictions, and expiration rules.

FR-DP-14 **Policy validation tools:** The system shall include functionality to validate the defined data usage policies against pre-established schema rules to ensure accuracy and compliance. Errors or inconsistencies in policy configuration shall trigger automated alerts, guiding the Data Provider to make corrections before policies are finalised.

SR-DP-8: Data Provider must be able to revoke access to data products when agreements are breached or expire.

Trustworthy Data Space Principle:	Control
DSSC Building block:	Data sovereignty and trust
Interoperability Focus Area:	Data Sharing

FR-DP-15 **Access Revocation Interface:** The system shall provide a user interface that allows Data Providers to revoke access to specific data products for collaborators, specifying the reason for revocation (e.g., agreement breach)

FR-DP-16 **Automated Access Termination:** The system shall automatically terminate access to data products when agreements reach their expiration date or are flagged as breached, ensuring compliance with access control policies.

SR-DP-9: Data Provider must be able to receive and respond to requests for data access, including the ability to negotiate data usage agreements.	
Trustworthy Data Space Principle:	Responsibility
DSSC Building block:	Legal
Interoperability Focus Area:	Data Sharing

FR-DP-17	Data Access Request Management: The system shall provide a user interface for Data Providers to view, approve, or deny incoming data access requests, with the ability to attach comments or conditions.
FR-DP-18	Agreement Negotiation and Tracking: The system shall enable Data Providers to negotiate data usage agreements with requesters by facilitating communication, document sharing, and agreement version tracking.

3.2 Functional Requirements from Data Recipient

SR-DR-1: Data Recipient must have the possibility to register its collaborators using standard identifiers (email, credentials).	
Trustworthy Data Space Principle:	Control
DSSC Building block:	Governance
Interoperability Focus Area:	Data Governance

FR-DR-1	Collaborator Registration Interface: The system shall provide a user interface that allows Data Recipients to register collaborators by entering their email addresses and assigning initial credentials.
FR-DR-2	Standard Identifier Authentication: The system shall authenticate collaborators using their registered email addresses and credentials, ensuring secure access to relevant data and functionalities.

SR-DR-2: Data Recipient must have tools to enable the management of data-sharing agreements clearly and transparently.	
Trustworthy Data Space Principle:	Transparency
DSSC Building block:	Legal
Interoperability Focus Area:	Data Sharing

FR-DR-3	Data Sharing Agreement Management Interface: The system shall provide Data Recipients with tools to manage data-sharing agreements, allowing them to view, accept, decline, and monitor the status of each agreement clearly and transparently.
FR-DR-4	Agreement Tracking and Notification System: The system shall enable Data Recipients to track the terms and conditions of their data-sharing agreements, providing notifications of any updates, renewals, or expirations to ensure ongoing compliance and awareness.

SR-DR-3: Data Recipients must have mechanisms for modern Data Access and Integration.	
Trustworthy Data Space Principle:	Efficiency
DSSC Building block:	Data interoperability
Interoperability Focus Area:	Data Sharing

FR-DR-5	Modern Data Access Mechanisms: The system shall provide Data Recipients with modern data access methods, including APIs (Application Programming Interfaces), data streaming services, and real-time data feeds, to facilitate efficient retrieval and consumption of data products.
FR-DR-6	Data Integration Support Tools: The system shall offer tools and features that enable Data Recipients to seamlessly integrate received data into their existing systems and workflows, supporting various data formats, protocols, and interoperability standards.

SR-DR-4: Data Recipient must have access to a catalogue and evaluate relevant and high-quality Data Products.	
Trustworthy Data Space Principle:	Transparency
DSSC Building block:	Data value creation enablers
Interoperability Focus Area:	Data Discovery

FR-DR-7	Data Product Catalogue and Search Functionality: The system shall provide Data Recipients with access to a searchable catalogue of data products, allowing them to list and discover relevant high-quality data by applying filters, keywords, and sorting options based on various criteria such as category, quality ratings, and recency.
FR-DR-8	Data Product Evaluation Tools: The system shall enable Data Recipients to evaluate data products by offering features such as data previews, quality metrics, user reviews, and ratings, assisting them in assessing the relevance and quality before accessing or integrating the data.

SR-DR-5: Data Recipients must have access to User-Friendly tools and interfaces for Data Exploration and Analysis.	
Trustworthy Data Space Principle:	Efficiency
DSSC Building block:	Data value creation enablers
Interoperability Focus Area:	Data Usage

FR-DR-9	Intuitive Data Visualization Tools: The system shall provide Data Recipients with user-friendly data visualization tools that enable them to create, customize, and interact with various chart types and graphical representations to facilitate data exploration and insights.
FR-DR-10	Simplified Data Query Interface: The system shall offer an easy-to-use interface that allows Data Recipients to perform data queries and filters with the support of query languages, supporting functions like guided search and examples.

SR-DR-6: The Data Recipient must be able to search and filter the data catalogue based on various criteria, including data type, keywords, provider, and usage policies.	
Trustworthy Data Space Principle:	Efficiency
DSSC Building block:	Data value creation enablers
Interoperability Focus Area:	Data Discovery

FR-DR-11	Advanced Search Functionality: The system shall provide a search interface for Data Recipients to query the data catalogue using keywords and filters such as data type, provider, and usage policies.
FR-DR-12	Dynamic Filtering System: The system shall allow Data Recipients to refine search results dynamically by applying multiple filters simultaneously, ensuring relevant data is easily discoverable.

SR-DR-7: The Data Recipient must be able to assess the trustworthiness of data products and providers, potentially leveraging a trust framework and reputation system.	
Trustworthy Data Space Principle:	Transparency
DSSC Building block:	Data sovereignty and trust
Interoperability Focus Area:	Data Governance

FR-DR-13	Trustworthiness Assessment Framework: The system shall provide a trust framework that evaluates and displays trust scores for data products and providers based on predefined criteria such as data quality, compliance, and historical usage feedback.
FR-DR-14	Reputation and Feedback System: The system shall enable Data Recipients to view provider reputation scores and user-generated reviews and to submit their feedback on data products and providers to contribute to the reputation system.

SR-DR-8: The Data Recipient must be able to download and integrate data products into their systems, potentially using standardized APIs and data formats.	
Trustworthy Data Space Principle:	Efficiency
DSSC Building block:	Data interoperability
Interoperability Focus Area:	Data Usage

FR-DR-15	Data Download Capability: The system shall provide Data Recipients with the ability to download data products in various standardized formats, ensuring compatibility with commonly used tools and systems.
FR-DR-16	API Integration Support: The system shall offer standardized APIs to enable Data Recipients to programmatically access and integrate data products directly into their systems, ensuring seamless interoperability.

3.3 Functional Requirements from Data Space Governance Authority

SR-GA-1: Data Space Governance Authority must have the possibility to register its collaborators using standard identifiers (email, credentials).	
Trustworthy Data Space Principle:	Control
DSSC Building block:	Governance
Interoperability Focus Area:	Data Governance

FR-GA-1	Collaborator Registration Interface: The system shall provide a user interface that allows the Data Space Governance Authority to register collaborators by entering their email addresses and assigning initial credentials.
FR-GA-2	Standard Identifier Authentication: The system shall authenticate collaborators using their registered email addresses and credentials, ensuring secure access to relevant data and functionalities.

SR-GA-2: Data Space Governance Authority should have instruments and mechanisms to ensure the establishment and enforcement of a Governance Framework, including defining rules, policies and procedures for data space participation, data access, compliance and dispute resolution.	
Trustworthy Data Space Principle:	Responsibility
DSSC Building block:	Governance
Interoperability Focus Area:	Data Governance

FR-GA-3	Governance Framework Management Tools: The system shall provide the Data Space Governance Authority with instruments to define, establish, and modify the governance framework, including creating rules, policies, and procedures for data space participation, data access, compliance, and dispute resolution.
FR-GA-4	Enforcement and Compliance Mechanisms: The system shall enable the Data Space Governance Authority to enforce the governance framework by implementing mechanisms for monitoring participant compliance, detecting violations, and facilitating dispute resolution processes according to the established policies.

SR-GA-3: Data Space Governance Authority should have instruments and mechanisms to facilitate collaboration and interoperability among participants, including the selection and adoption of standards, protocols and vocabularies.	
Trustworthy Data Space Principle:	Efficiency
DSSC Building block:	Data interoperability
Interoperability Focus Area:	Data Governance

FR-GA-5	Standards and Protocols Management Tools: The system shall provide the Data Space Governance Authority with instruments to select, adopt, and manage standards, protocols, and vocabularies, ensuring interoperability among participants.
FR-GA-6	Collaboration Facilitation Mechanisms: The system shall offer mechanisms that facilitate collaboration among participants, such as shared communication platforms, data exchange interfaces, and interoperability testing tools that align with the selected standards and protocols.

SR-GA-4: Governance authority must establish and maintain a transparent and accessible mechanism for reporting and addressing data-related complaints and disputes.

Trustworthy Data Space Principle:	Transparency
DSSC Building block:	Governance
Interoperability Focus Area:	Data Governance

FR-GA-7	Complaint Submission Portal: The system shall provide a user interface for stakeholders to submit data-related complaints, including fields for describing the issue, attaching evidence, and specifying the data product or provider involved.
FR-GA-8	Complaint Tracking and Resolution System: The system shall enable the Governance Authority to track, manage, and resolve complaints through a transparent workflow that includes status updates, communication with stakeholders, and documentation of resolution outcomes.

SR-GA-5: Governance authority must have the capability to monitor and audit data space activities to ensure compliance with the defined governance framework.

Trustworthy Data Space Principle:	Responsibility
DSSC Building block:	Governance
Interoperability Focus Area:	Data Governance

FR-GA-9	Activity Monitoring Dashboard: The system shall provide a dashboard that allows the Governance Authority to monitor real-time activities within the data space, including data access, modifications, and sharing events, to ensure compliance with the governance framework.
FR-GA-10	Audit Trail and Reporting: The system shall maintain a comprehensive audit trail of all data space activities, enabling the Governance Authority to generate detailed compliance reports and identify potential violations of the governance framework.

SR-GA-6: Governance authority must have the ability to evolve and adapt the governance framework over time to accommodate new technologies, changing regulations, and evolving needs of the data space ecosystem.	
Trustworthy Data Space Principle:	Responsibility
DSSC Building block:	Governance
Interoperability Focus Area:	Data Governance

FR-GA-11	Governance Framework Management Interface: The system shall provide the Governance Authority with a user-friendly interface to update, modify, and publish changes to the governance framework, including rules, policies, and guidelines.
FR-GA-12	Version Control and Stakeholder Notification: The system shall support version control for the governance framework, maintaining a history of changes and automatically notifying stakeholders of updates to ensure compliance with the latest framework.

3.4 Functional Requirements from Data Producer

SR-PD-1: Data Producer must exert control over data usage through consent.	
Trustworthy Data Space Principle:	Control
DSSC Building block:	Data sovereignty and trust
Interoperability Focus Area:	Data Sharing

FR-PD-1	Consent Management Tools: The system shall provide Data Producers with instruments to create, manage, and modify consent agreements, enabling them to specify how their data can be used, by whom, and under what conditions.
FR-PD-2	Consent-Based Data Usage Enforcement: The system shall enforce data usage policies based on the consents provided by Data Producers, ensuring that Data Consumers can access and use the data only within the agreed-upon terms, and preventing unauthorized usage.

SR-PD-2: Data Producer must have access to tools and mechanisms that facilitate the valuation of their data assets based on factors such as data type, quality, volume, uniqueness, market demand, and potential value creation opportunities.	
Trustworthy Data Space Principle:	Fairness
DSSC Building block:	Data value creation enablers
Interoperability Focus Area:	Data Governance

FR-PD-3	Data Asset Valuation Dashboard: The system shall provide Data Producers with a valuation dashboard that analyses their data assets based on criteria such as data type, quality, volume, uniqueness, and market demand, offering an estimated monetary or strategic value.
FR-PD-4	Market Demand and Opportunity Insights: The system shall include tools to analyse market trends and value creation opportunities, providing Data Producers with insights into potential demand for their data assets and recommendations for maximizing their value.

SR-PD-3: Data Producer must be able to participate in a transparent and auditable compensation mechanism that allows them to receive fair and appropriate remuneration for sharing their data assets, based on agreed-upon terms and conditions.	
Trustworthy Data Space Principle:	Fairness
DSSC Building block:	Data value creation enablers
Interoperability Focus Area:	Data Governance

FR-PD-5	Compensation Management System: The system shall provide a mechanism for Data Producers to define and manage compensation terms for their data assets, ensuring transparency in pricing, usage conditions, and remuneration agreements.
FR-PD-6	Payment Tracking and Auditing: The system shall include a transparent and auditable payment tracking feature, enabling Data Producers to view and verify payments received for data-sharing activities, with detailed records of transactions and adherence to agreed-upon terms.

3.5 Functional Requirements from Data Subject

SR-SU-1: Data Subject must exert control over data usage through consent.	
Trustworthy Data Space Principle:	Control
DSSC Building block:	Data sovereignty and trust
Interoperability Focus Area:	Data Governance

FR-SU-1	Consent Management Tools: The system shall provide Data Producers with instruments to create, manage, and modify consent agreements, enabling them to specify how their data can be used, by whom, and under what conditions.
FR-SU-2	Consent-Based Data Usage Enforcement: The system shall enforce data usage policies based on the consents provided by Data Producers, ensuring that Data Consumers can access and use the data only within the agreed-upon terms, and preventing unauthorised usage.

SR-SU-2: Data Subject must have access to tools and mechanisms that facilitate the valuation of their data assets based on factors such as data type, quality, volume, uniqueness, market demand, and potential value creation opportunities.	
Trustworthy Data Space Principle:	Fairness
DSSC Building block:	Data value creation enablers
Interoperability Focus Area:	Data Governance

FR-SU-3	Data Asset Valuation Dashboard: The system shall provide Data Producers with a valuation dashboard that analyses their data assets based on criteria such as data type, quality, volume, uniqueness, and market demand, offering an estimated monetary or strategic value.
FR-SU-4	Market Demand and Opportunity Insights: The system shall include tools to analyse market trends and value creation opportunities, providing Data Producers with insights into potential demand for their data assets and recommendations for maximizing their value.

SR-SU-3: Data Subject must be able to participate in a transparent and auditable compensation mechanism that allows them to receive fair and appropriate remuneration for sharing their data assets, based on agreed-upon terms and conditions.	
Trustworthy Data Space Principle:	Fairness
DSSC Building block:	Data value creation enablers
Interoperability Focus Area:	Data Governance

FR-SU-5	Compensation Management System: The system shall provide a mechanism for Data Producers to define and manage compensation terms for their data assets, ensuring transparency in pricing, usage conditions, and remuneration agreements.
FR-SU-6	Payment Tracking and Auditing: The system shall include a transparent and auditable payment tracking feature, enabling Data Producers to view and verify payments received for data-sharing activities, with detailed records of transactions and adherence to agreed-upon terms.

3.6 Functional Requirements from Data Steward

SR-ST-1: Data Steward must be able to authenticate credentials that identify him/her as a member of a specific organisation.	
Trustworthy Data Space Principle:	Control
DSSC Building block:	Governance
Interoperability Focus Area:	Data Governance

FR-ST-1	Organisation-Based Authentication System: The system shall provide Data Steward with authentication mechanisms that allow them to log in using credentials that identify them as members of a specific organisation, such as through enterprise Single Sign-On (SSO) or federated identity management systems.
FR-ST-2	Verification of Organisational Membership: The system shall verify and confirm the organisational affiliation of authenticated Data Steward, ensuring that their credentials are valid and that they are recognized as legitimate members of their specified organisation for purposes of access control and collaboration.

SR-ST-2: Data Steward must be able to perform all activities of data providers when representing an organisation that provides data in the data space.	
Trustworthy Data Space Principle:	Responsibility
DSSC Building block:	Governance
Interoperability Focus Area:	Data Governance

FR-ST-3	Full Functionality Access for Data Stewards: The system shall allow Data Stewards to perform all activities of Data Providers on behalf of their organisation within the data space, including data publishing, metadata management, data sharing agreement drafting, and monitoring.
FR-ST-4	Representative Permissions and Controls: The system shall grant Data Stewards the necessary permissions and controls to act as representatives of their organisation, enabling them to manage and oversee the organisation's data provisioning activities within the data space.

SR-ST-3: Data steward must be able to perform all activities of data recipients when representing an organisation that receives data in the data space.	
Trustworthy Data Space Principle:	Responsibility
DSSC Building block:	Governance
Interoperability Focus Area:	Data Governance

FR-ST-5	Full Functionality Access for Data Stewards: The system shall allow Data Stewards to perform all activities of Data Recipients on behalf of their organisation within the data space, including data requesting, metadata viewing, data sharing agreement signing, and monitoring.
FR-ST-6	Representative Permissions and Controls: The system shall grant Data Stewards the necessary permissions and controls to act as representatives of their organisation, enabling them to manage and oversee the organisation's data-receiving activities within the data space.

3.7 Functional Requirements from Data Scientist/Engineer

SR-DE-1: Data Scientist/Engineer must be able to authenticate credentials that identify him/her as a member of a specific organisation.	
Trustworthy Data Space Principle:	Control
DSSC Building block:	Governance
Interoperability Focus Area:	Data Governance

FR-DE-1	Organisation-Based Authentication System: The system shall provide Data Scientists/Engineers with authentication mechanisms that allow them to log in using credentials that identify them as members of a specific organisation, such as through enterprise Single Sign-On (SSO) or federated identity management systems.
FR-DE-2	Verification of Organisational Membership: The system shall verify and confirm the organisational affiliation of authenticated Data Scientists/Engineers, ensuring that their credentials are valid and that they are recognized as legitimate members of their specified organisation for purposes of access control and collaboration.

SR-DE-2: The Data Scientist/Engineer must be able to access and query data sets and data services relevant to their assigned projects and tasks, within the boundaries defined by the Data Usage Policies associated with those data assets.	
Trustworthy Data Space Principle:	Efficiency
DSSC Building block:	Data sovereignty and trust
Interoperability Focus Area:	Data Usage

FR-DE-3	Authorized Data Query Access: The system shall enable Data Scientists/Engineers to query and retrieve data that their organisation has access to, providing appropriate query tools and interfaces that facilitate data analysis within the scope of their organisational permissions.
FR-DE-4	Access Control Enforcement Based on Organisational Rights: The system shall enforce access control mechanisms that ensure Data Scientists/Engineers can only query data sets to which their organisation has been granted access, preventing unauthorised data retrieval and maintaining compliance with data governance policies.

SR-DE-3: Data Scientist/Engineer must be able to utilise a range of data analysis and processing tools and environments, including both open-source and commercial solutions, within the secure confines of the data space infrastructure.	
Trustworthy Data Space Principle:	Efficiency
DSSC Building block:	Data value creation enablers
Interoperability Focus Area:	Data Usage

FR-DE-5	Integrated Data Analysis Toolkit: The system shall provide Data Engineers with access to a suite of pre-configured data analysis and processing tools, including both open-source (e.g., Python, R, Apache Spark) and commercial solutions, directly within the secure data space infrastructure.
FR-DE-6	Secure Sandbox Environment: The system shall offer a secure, isolated sandbox environment for Data Engineers to perform data analysis and processing tasks, ensuring compliance with data security and governance policies while allowing flexibility in tool usage.

SR-DE-4: The Data Scientist/Engineer must be subject to continuous monitoring and auditing of their data access and usage activities, with all actions logged and auditable to ensure compliance with data space policies and relevant regulations.	
Trustworthy Data Space Principle:	Responsibility
DSSC Building block:	Governance
Interoperability Focus Area:	Data Sharing

FR-DE-7	Continuous Activity Monitoring: The system shall implement continuous monitoring of Data Engineer activities, logging all data access, modifications, and processing actions in real time to ensure adherence to data space policies and relevant regulations.
FR-DE-8	Auditable Logging and Reporting: The system shall maintain an immutable audit log of all actions performed by Data Engineers, providing detailed records that can be queried and exported for compliance reviews and regulatory reporting.

3.8 Functional requirements from Legal counsel

SR-LC-1: Legal counsel must be able to authenticate credentials that identify him/her as a member of a specific organisation.	
Trustworthy Data Space Principle:	Control
DSSC Building block:	Governance
Interoperability Focus Area:	Data Governance

FR-LC-1	Organisation-Based Authentication System: The system shall provide Data Scientists/Engineers with authentication mechanisms that allow them to log in using credentials that identify them as members of a specific organisation, such as through enterprise Single Sign-On (SSO) or federated identity management systems.
FR-LC-2	Verification of Organisational Membership: The system shall verify and confirm the organisational affiliation of authenticated Data Scientists/Engineers, ensuring that their credentials are valid and that they are recognized as legitimate members of their specified organisation for purposes of access control and collaboration.

SR-LC-2: Legal counsel must be able to evaluate, approve, request voiding and audit agreements of his/her organisation.	
Trustworthy Data Space Principle:	Responsibility
DSSC Building block:	Legal
Interoperability Focus Area:	Data Governance

FR-LC-3	Agreement Management Interface for Legal Counsel: The system shall provide Legal Counsel with tools to evaluate, approve, and request the voiding of agreements about their organisation, including features for reviewing agreement terms, providing approvals, and submitting voiding requests.
FR-LC-4	Audit and Compliance Monitoring Tools: The system shall enable Legal Counsel to audit all agreements of their organisation by offering access to agreement histories, change logs, and compliance reports, ensuring transparency and adherence to legal and organisational policies.

3.9 Functional Requirements from Data Space Auditor / Regulator

SR-AU-1: Auditor must be able to authenticate credentials that identify him/her as a member of a specific organisation.	
Trustworthy Data Space Principle:	Control
DSSC Building block:	Governance
Interoperability Focus Area:	Data Governance

FR-AU-1	Organisation-Based Authentication System: The system shall provide Data Scientists/Engineers with authentication mechanisms that allow them to log in using credentials that identify them as members of a specific organisation, such as through enterprise Single Sign-On (SSO) or federated identity management systems.
FR-AU-2	Verification of Organisational Membership: The system shall verify and confirm the organisational affiliation of authenticated Data Scientists/Engineers, ensuring that their credentials are valid and that they are recognized as legitimate members of their specified organisation for purposes of access control and collaboration.

SR-AU-2: Auditor must be able to evaluate and audit agreements and compliance with these agreements where/when required.	
Trustworthy Data Space Principle:	Responsibility
DSSC Building block:	Governance
Interoperability Focus Area:	Data Sharing

FR-AU-3	Agreement Access and Evaluation Tools for Auditors: The system shall provide Auditors with the ability to access and review all agreements pertinent to their auditing responsibilities, including full details of the terms and conditions, to evaluate and assess compliance as required.
FR-AU-4	Compliance Auditing Mechanisms: The system shall enable Auditors to monitor and audit compliance with agreements by providing access to activity logs, compliance reports, and other relevant data, allowing them to verify that all parties are adhering to the agreed-upon terms whenever necessary.

4 Analysis

4.1 Requirements per trustworthy data space principle

The following chart depicts the frequency of Stakeholder requirements grouped by the basic principles of Trustworthy Data Spaces:

Count of Requirements by Principle

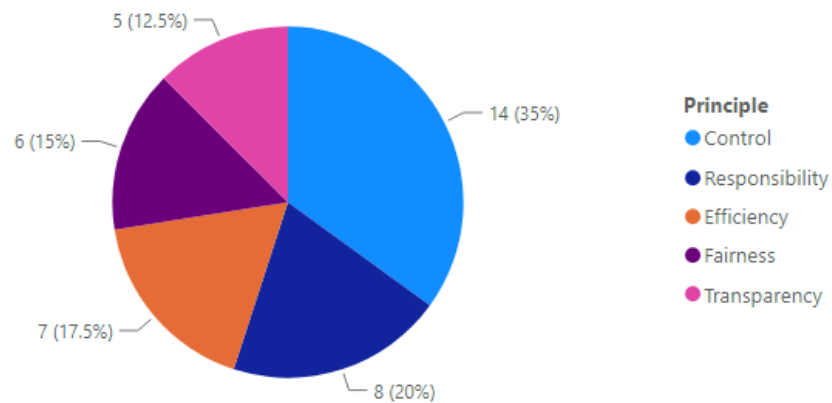


Figure 2. Requirements grouped by Trustworthy Data Space Principle

This distribution reflects a structured approach that primarily values control and responsibility, supported by efficiency, fairness, and transparency.

4.2 Requirements per DSSC Building Block

The following chart depicts the frequency of Stakeholder requirements grouped by the Building Blocks suggested by DSSC:

Count of Requirements by DSSC Building block

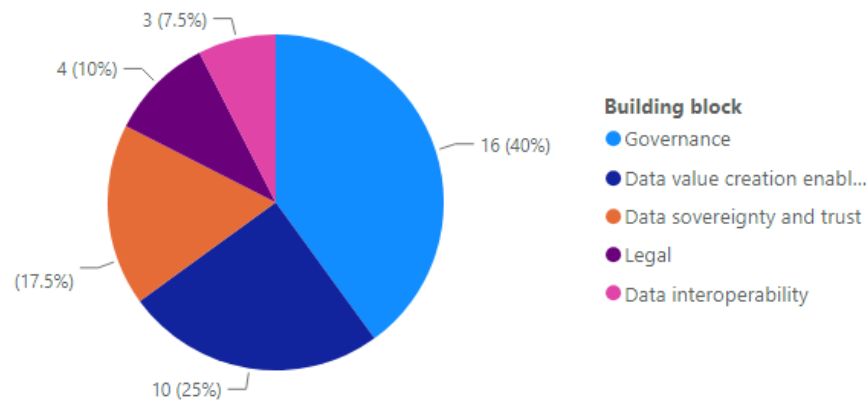


Figure 3. Requirements grouped by DSSC Building Block

This distribution denotes the functional requirements mentioned in this document prioritised governance and value creation above the supporting of legal compliance and interoperability as defined by the DSSC.

4.3 Requirements grouped by interoperability focus

The following chart depicts the frequency of requirements grouped by interoperability focus:

Count of Requirements by Interoperability Focus

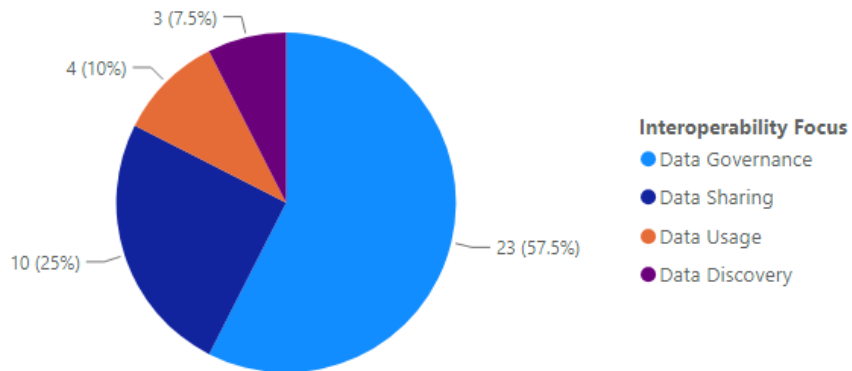


Figure 4. Requirements grouped by Data Interoperability Focus

This distribution underscores that the functional requirements discussed in this document have a strong focus on Data Governance at the expense of Data Discovery and Data Usage which are usually more technical requirements.

4.4 Requirements per Stakeholder

The following chart depicts the frequency of requirements grouped by Stakeholder:

Count of Requirements by Stakeholder

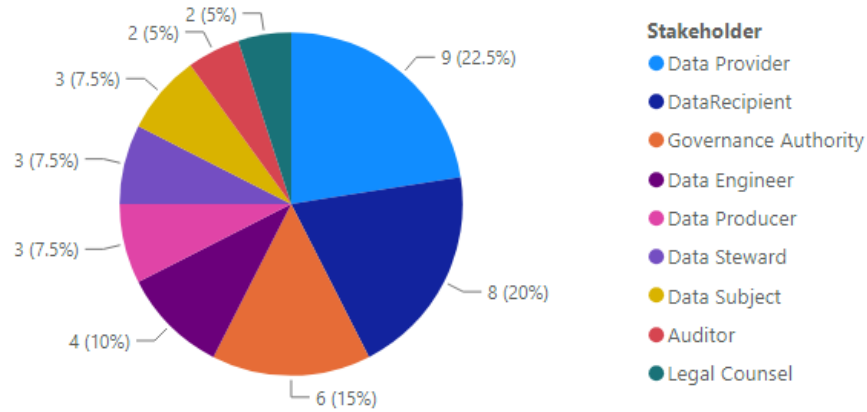


Figure 5. Requirements grouped by stakeholder

This distribution suggests the functional requirements were centred around data provision and receipt we suggest further research to include additional requirements, particularly from Data Producers (both natural and legal persons).

4.5 Categories or themes of functional requirements

The following chart depicts the “thematic” categories of functional requirements identified regardless across all stakeholder requirements.

Count of Functional Requirement Name

BY CATEGORY

Category

- User registration and Authentication
- Data Access and Sharing
- Data Discovery and Publishing
- Activity Monitoring
- Agreement Compliance and Audit
- Agreement Drafting and Negotiation
- Compensation Mechanisms
- Consent Management
- Data Visualization and Analysis
- Governance Management
- Role management
- Value Assessment
- Complaint Management
- Data Usage Policies
- Governance Evolution and Adaptation
- Trust and Reputation
- Quality Monitoring



This distribution shows "User registration and Authentication" and "Data Access and Sharing" emerge as prioritized categories, reflecting their critical role in ensuring secure access and effective data exchange.

5 References

- Beyond Civic AG. 2025. *Baseline, Scope and stakeholders of Trustworthy Data Spaces in Switzerland*. Bern: Beyond Civic AG.
- Bradner, Scott. n.d. *Keywords for use in RFCs to Indicate Requirement Levels*. Prod. Internet Engineering Task Force (IETF). Accessed 11 13, 2024. <https://www.rfc-editor.org/rfc/pdf/rfc2119.txt.pdf>.
- Data Spaces Support Centre. 2024. *Building Block Overview*. Vers. 1.5. 9 10. Accessed 11 13, 2024. <https://dssc.eu/space/bv15e/766064046/Building+Block+Overview>.
- Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK; Eidgenössisches Departement für auswärtige Angelegenheiten EDA. 2022. *Creating Trustworthy Data Spaces Based on Digital Self-determination*. Bern: Schweizerische Eidgenossenschaft. Accessed 11 13, 2024. <https://www.news.admin.ch/news/message/attachments/70835.pdf>.
- High-Level Forum on European Standardisation. 2024. *Final report of work-stream 14 Data Interoperability*. Deputy Director-General – Chief Standardisation Officer, European Union Commission, Bruxelles: Publications Office of the EU. Accessed 11 13, 2024. <https://ec.europa.eu/docsroom/documents/58914?locale=en>.
- Intellisoft. 2024. *Functional vs technical requirements*. 27 09. Accessed 11 13, 2024. <https://intellisoft.io/functional-requirements/>.