beyond civic

Data Space Blueprint

Technical Requirements

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

Table of Contents

Executive Summary

This document outlines the technical requirements to build a Trustworthy Data Space in Switzerland. It is derived directly from the functional requirements identified in (Beyond Civic AG 2024).
The proposed system supports the design and implementation 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 more.
This document clarifies the definitions such as technical requirements and non-functional requirements. It also expands the understanding of the different taxonomies used to classify data. It provides a clear list of business rules embedding the purpose, description and exceptions that come with it.
Additionally, it provides a list of external requirements divided in 3 groups: User interfaces, software interfaces and communication interfaces, that architects should consider when defining the solution scope.
Consequently, each functional requirement is broken down into specific, actionable technical requirements, focusing on the system's behaviour to support stakeholders with their functions. Additionally, each functional requirement could include one or more business rule, and one or more external requirements.
This document concludes with a list of Non-functional requirements that increase the quality of experience for all stakeholders of the data space solution.

1 Introduction

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

1.1 Goal of this document

The goal of this document is twofold:

1. To create a shared understanding of the solution scope.
2. 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 technical requirements, derived from each of the functional requirements identified in (Beyond Civic AG 2024).

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 functional 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
FIPS 140-3	Federal Information Processing Standard 140. Version 3
TLS	Transport Layer Security
UTC	Coordinated Universal Time.
SMTP	Simple Mail Transfer Protocol
RBAC	Role-based access control
ABAC	Attribute-based access control
PBAC	Policy-based access control
SSO	Single Sign On
SAML	Security Assertion Markup Language
OIDC	OpenID Connect
CSV	Comma-Separated Value File
PDF	Portable Document Format

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, Technical Requirements for Data Spaces in Switzerland (this document).

2 Definition of technical and non-functional requirements

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

2.1 Definition of Technical Requirement

This document defines Technical Requirements as a description of “how the system will be built and operate from a technical perspective” (Intellisoft 2024).

2.2 Definition of Non-Functional Requirement

This document defines Non-Functional Requirements as a description of how a system behaves while setting boundaries for its operational aspects, they are often understood as the system’s quality attributes (Intellisoft 2024).

2.3 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.)

3 Data Requirements and Taxonomy

This section describes the different perspectives of data the solution must support.

3.1 Data classification according to processing level

The requirements presented in this document assume that data shared may belong to any of the following categories:

Data-driven insights	Actionable knowledge and conclusions derived from analysing and interpreting data, often used to inform decisions or strategies.
Processed data	Data that has been cleaned, transformed, and formatted, making it ready for analysis or integration into workflows and systems.
Pre-processed data	Data that has undergone preliminary steps, such as filtering, normalization, or aggregation (incl anonymisation and pseudonymisation) to prepare it for further processing or analysis.
Raw data	Untouched, unstructured, or unprocessed data directly collected from its source, often requiring significant preparation before use.

3.2 Data classification according to source

The requirements presented in this document assume that data shared may belong to any of the following categories:

User-entered data	Data purposefully entered by users into a system.
Event/Sensor data	Recorded from events occurring in the real world or digitally.
Transactional data	Generated from interactions or exchanges captured by a system.
Ref/Facts data	Information that is used solely for the purpose of categorising data. E.g. country codes, area codes, currencies.
Synthetic data	Artificially generated data that mimics real-world data characteristics but does not correspond to actual entities or events.

3.3 Data classification according to structure

The requirements presented in this document assume that data shared may belong to any of the following categories:

Structured	Semi-structured	Unstructured
Data organized into predefined formats, such as tables with rows and columns, making it easily searchable and analysable	Data that does not follow a strict format but has some organizational properties, such as tags or markers, making it partially searchable.	Data without a predefined structure or format, often requiring advanced tools to analyse.

ID	Name	Age	Degree
1	Jean	21	BSc
2	David	31	MSc
3	Mark	41	PhD

Figure 1. Example of Data classification by structure

4 Business rules

This section introduces business rules that work in tandem to ensure the correct behaviour of the overall solution.

ID	BR-1
Name	**Organizational identifiers for users**
Purpose	To ensure that only authorized personnel with valid organizational email addresses can create user accounts within the system.
Details	**Email domain verification:** The system shall only allow the creation of user accounts with email addresses that belong to the organization's approved domain(s).
	Configurable domain list: The Governance Authority shall have the ability to update the list of approved organizational email domains.
	Rejection of Personal Emails: Email addresses from public domains shall be automatically rejected during the account creation process.
Exceptions	Any exceptions to this rule must be approved by the Governance Authority and logged for audit purposes.

ID	BR-2
Name	**Acceptance of Organizations Based on Governance Authority List**
Purpose	To ensure that only authorized organizations can be added to the data space, maintaining compliance with governance policies and standards.
Details	The system shall validate every organization against an approved list maintained by the Governance Authority before allowing it to be registered or added to the system.
	If an organization is not found on the approved list, the system shall reject the registration request and provide an error message indicating that the organization is not authorized.
	Data Space Infrastructure Operators shall have read-only access to view the current approved organization list for auditing or inquiry purposes.
	Any changes to the governance-approved organization list must be logged and auditable.
Exceptions	Organizations added under exceptional circumstances must be flagged for review until formal approval from the Governance Authority is received.

ID	BR-3
Name	**Logging and Auditability of Data Queries/Transfers/Streams**
Purpose	To ensure transparency and accountability in data handling by maintaining a complete log of all data queries, transfers and streams which are accessible for audit purposes by the data provider.
Details	The system shall log all data queries, transfers and streams including the following details: 1. Type (e.g. query, download, stream) 2. Timestamp of the query or transfer.

	3. User or system initiating the query/transfer/stream. 4. Destination (Data Recipient organization)
	Logs shall be stored securely to prevent unauthorized access or tampering and must comply with relevant data protection and retention policies.
	Authorized representatives of the data provider shall have on-demand access to view and audit the logs through a secure interface.
	The system shall provide filtering and reporting capabilities to assist in log review, including the ability to generate summaries of queries/transfers over specified time periods.
	Logs must be retained for a minimum of the governance-mandated duration (e.g., 12 months) unless otherwise specified by the data provider or legal requirements.
Exceptions	Queries or transfers initiated by internal system maintenance or automated processes may be excluded from the default audit log view but must remain accessible in the system's backend for compliance verification.
	Any failure to log a query or transfer due to a system error must trigger an alert to system administrators and must be documented in an incident report reviewed by the data provider.

ID	**BR-4**
Name	**Enforcement of Data Sharing Agreements Duration for Data Products**
Purpose	To ensure that data access is granted only for the specified duration defined by its data sharing agreement, thereby protecting data security and compliance with governance rules.
Details	The system shall enforce access control policies by automatically granting and revoking access to data product based on the duration specified in the agreement.
	Data sharing agreements shall include: 1. Start date and time (preferably in UTC) 2. End date and time (preferably in UTC) 3. Authorized organization (organizational user)
	The system shall generate an automated notification for users when access is about to expire (e.g., 7 days and 24 hours before expiration).
	Upon expiration of access, the system shall: 1. Immediately revoke user or role permissions to the data product. 2. Log the revocation action in the audit trail. 3. Notify the affected stakeholders (Data Provider, Data Recipient, Governance Authority) of the revocation.

Exceptions	Any failure to log a query or transfer due to a system error must trigger an alert to system administrators and must be documented in an incident report reviewed by the data provider.

5 External requirements

This section introduces software components or systems that work in tandem to ensure the correct functionality of the overall solution.

5.1 User interfaces

Screens, user input, outputs, navigation

ID	Screen Name	Description
UI-1	User sign in screen	A screen where existing users can enter their credentials (username and password) to access their account and its associated features.
UI-2	User signup screen	A screen where new users can register by providing necessary details like username, email, and password to create a new account.
UI-3	Invite member screen	A screen where current users or admins can send invitations to new members to join the platform or specific teams, typically by entering the email address of the invitee.
UI-4	List data products (catalogue) screen	A screen displaying a catalogue of available data products, allowing users to browse, search, and filter through various datasets offered on the data space.
UI-5	Create data product screen	A screen where users can submit and configure new data products, providing relevant details such as title, description, and metadata for the dataset being created.
UI-6	Request access to data product screen	A screen where users can request permission to access specific data products by submitting a request form that will be reviewed by the data owner or admin.
UI-7	Create data sharing agreement screen	A screen where users can create agreements for sharing data, specifying terms, conditions, and permissions related to the use and sharing of data products.
UI-8	User management screen	A screen where the governance authority can manage and maintain the overall access of users into the data space platform.
UI-9	Data product management screen	A screen where Data Providers can maintain all different descriptions and accessors of each Data Product offered in the catalogue.
UI-10	User Audit & Monitoring screen	A screen where users can observe all different actions, related to the user.

UI-11	Data Audit & Monitoring screen	A screen where users can observe all different actions, related to the data products that the user interacts.
UI-12	Agreements/Compliance/Policy Audit & Monitoring screen	A screen where users can observe all different actions, related to the agreements that the user interacts.
UI-13	Data Product details, preview and access screen	A screen where Data Recipients are shown details of the Data Products and have clear instructions to access data efficiently.
UI-14	Reputation and feedback screen	A screen where users can evaluate the reputation of participants and datasets, and to provide their own feedback.
UI-15	Governance console screen	A screen where Governance Authority can create, update, delete, propose, accept, reject policies for the overall governance of the data space.
UI-16	Dispute resolution screen	A screen where users can request, mediate and resolve disputes.
UI-17	Consent screen	A screen where users can propose, request, accept, reject consent.
UI-18	Market insights and compensation screen	A screen where users can request, review, learn valuations of data assets.

5.2 Software interfaces

Operating systems, databases, web services, commercial integrated systems

ID	Software Name	Description
SI-1	Operating system	The fundamental software that manages hardware resources and provides services for running applications.
SI-2	Reverse proxy	A server that sits between client devices and a web server, forwarding requests from clients to the appropriate server. It helps with load balancing, security, and caching.
SI-3	Load balancer	A system that distributes incoming network traffic across multiple servers to ensure no single server is overwhelmed, improving performance, reliability, and scalability.
SI-4	Database	A structured system for storing, organizing, and managing data. It allows for efficient data retrieval, updating, and manipulation, supporting operations like queries and transactions.
SI-5	SMTP service	A service that handles the sending and routing of emails using the SMTP, ensuring emails are delivered from senders to recipients.
SI-6	Process orchestrator system	A system that automates, coordinates, and manages the execution of complex workflows and processes, ensuring tasks are carried out in a specified sequence and according to business rules.
SI-7	Identity and access management system	A system that ensures the right individuals have the appropriate access to technology resources. It includes user authentication, authorization, and the management of roles and permissions.
SI-8	Query engine	A system or software component responsible for processing and executing queries on a database or data source. It interprets the data recipient's query (often written in SQL or another query language) and retrieves or manipulates data accordingly, optimizing for efficiency and accuracy.
SI-9	SDK	Software Development Kit is a collection of tools, libraries, documentation, and code samples provided to developers to facilitate the creation and integration of software applications for specific platforms, frameworks, or devices.
SI-10	Monitoring & Logs	It is a component of a software or IT infrastructure designed to track, collect, and analyse system performance, operational metrics, and event logs.

5.3 Communication interfaces

ID	Interface Name	Description
CI-1	HTTP	A stateless, request-response protocol used for transferring hypertext documents between clients and servers over the web.
CI-2	Email	A communication system for sending, receiving, and storing messages between users via email servers over the internet.
CI-3	WebRTC	A protocol that enables real-time, peer-to-peer communication for audio, video, and data sharing directly between browsers without the need for plugins or additional software.
CI-4	Websocket	A full-duplex, bidirectional communication protocol that allows for real-time, persistent connections between a client and server.
CI-5	HTTP Polling	A method where a client repeatedly sends HTTP requests to the server at regular intervals to check for updates.
CI-6	HTTP Long Polling	A variation of polling where the client sends an HTTP request and waits for the server to respond when new data is available, then re-sends the request immediately afterward.
CI-7	Server Side Events	A one-way communication protocol where the server continuously sends updates to the client over a single HTTP connection.
CI-8	gRPC	A high-performance RPC framework that uses HTTP/2 to support bidirectional streaming and low-latency communication for distributed systems.
CI-9	MQTT	A lightweight messaging protocol designed for low-bandwidth, high-latency, or unreliable networks, commonly used in IoT applications.
CI-10	AMPQ	A robust, open standard for message-oriented middleware that supports message queuing, routing, and guaranteed delivery.
CI-11	GraphQL	A query language and runtime for APIs that allows clients to request specific data and subscribe to real-time updates via subscriptions.
CI-12	OData	A protocol designed for building and consuming RESTful APIs, supporting features like filtering, sorting, and paging.
CI-13	REST APIs	The most widely protocol used, it leverages standard HTTP methods for web services.
CI-14	JSON-RPC	JSON-RPC is a lightweight, stateless remote procedure call (RPC) protocol that uses JSON (JavaScript Object Notation) for encoding messages between a client and a server.

6 Non-functional requirements

This section outlines the specific non-functional requirements and capabilities that the data space solution should support.

NFR-1	**Security and Confidentiality:** Implementing robust security measures to protect data within the data space from unauthorized access, modification, or disclosure. This includes encryption, access controls, intrusion detection systems, and adherence to industry-standard security practices.

NFR-2	**Sustainability:** Designing the data space infrastructure and operations for long-term sustainability, considering energy efficiency, resource optimization, and environmental impact.

NFR-3	**Transparency:** Providing clear and auditable mechanisms for tracking data flows and usage within the data space, enabling participants to understand how their data is being processed and used. This includes data provenance tracking, transparent logging, and mechanisms for data access requests and justifications.

NFR-4	**Trustworthiness:** Establishing a robust and trustworthy data space environment through transparency, accountability, security, and compliance with ethical principles and regulations.

NFR-5	**Data Sovereignty:** Ensuring that data remains under the control of its rightful owners, respecting legal and regulatory frameworks regarding data storage, processing, and transfer. This includes the use of technologies that enable data sovereignty, such as decentralized architectures and privacy-enhancing techniques.

NFR-6	**Findability and Reusability:** Facilitating the discovery and reuse of data within the data space, using metadata standards, semantic annotations, and data catalogues. This involves implementing FAIR (Findable, Accessible, Interoperable, Reusable) data principles and tools to support data discovery and reuse.

NFR-7	**Interoperability:** Ensuring the data space infrastructure seamlessly integrates with diverse systems, platforms, and protocols to enable efficient data exchange and collaboration. This requires adherence to open standards, the implementation of APIs, compatibility with various data formats, and support for common communication protocols to facilitate smooth interaction between heterogeneous systems.

NFR-8	**Portability:** Enabling the transfer of data between different data spaces and systems without loss of fidelity or integrity, using standardized data formats and transfer protocols. This requires the adoption of portable data formats and mechanisms for data migration and transfer.

NFR-9	**Performance:** Ensuring efficient and timely processing of data transactions within the data space, meeting the performance requirements of different use cases. This involves optimizing infrastructure, data processing algorithms, and network connectivity to handle data volumes and transaction speeds.

NFR-10	**Scalability:** Designing the data space infrastructure to handle increasing data volumes and user traffic, scaling resources as needed to maintain performance and availability. This requires the use of scalable technologies, cloud infrastructure, and dynamic resource allocation mechanisms.

NFR-11	**Auditability:** Enabling comprehensive logging and auditing of data transactions and authentications within the data space, ensuring accountability and traceability of usage. This involves logging data access requests, processing steps, and data lineage information to facilitate audits and investigations.

NFR-12	**Privacy:** Protecting the privacy of individuals whose data is processed within the data space, complying with data protection regulations (e.g., GDPR). This involves implementing privacy-enhancing technologies like anonymization, pseudonymization, and differential privacy.

NFR-13	**Localization:** Ensuring the data space infrastructure supports multiple languages, regional formats, and cultural preferences to provide a seamless user experience across different regions.

NFR-14	**Supportability:** Designing the data space infrastructure to facilitate efficient maintenance, updates, and issue resolution, ensuring long-term operational reliability. This involves implementing clear documentation, modular system architecture, automated monitoring tools, and mechanisms for tracking and addressing user feedback or system issues with minimal downtime.

NFR-15	**Deployability:** Ensuring the data space infrastructure can be easily deployed across diverse environments, including on-premises, cloud, and hybrid setups, with minimal effort and risk. This requires the use of detailed deployment documentation, and configuration management tools to streamline and standardize the deployment process.

NFR-16	**Maintainability:** Designing the data space infrastructure to enable efficient updates, bug fixes, and enhancements with minimal disruption to operations. This requires adopting modular architectures, standardized coding practices, comprehensive documentation, and automated testing frameworks to ensure that the system remains adaptable and easy to modify over its lifecycle.

7 Technical Requirements

This section outlines the specific technical features and capabilities that the data space solution must provide to stakeholders. These technical requirements serve as a blueprint for designing and developing a system that effectively supports data sharing, interoperability, and collaboration within a trustworthy data space.

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.
Business rule:	BR-1, BR-2
External requirements:	UI-1, UI-2, UI-3

TR-DP-1 The interface must validate organisational email addresses in real time and ensure secure transmission of data via TLS 1.3.

TR-DP-2 The system must store collaborator registration data in a database with encryption algorithms approved in FIPS 140-3 and implement input sanitization to prevent injection attacks.

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.
Business rule:	BR-1, BR-2
External requirements:	UI-1, UI-2, UI-3

TR-DP-3 The system shall implement an authentication mechanism using OAuth 2.0 or OpenID Connect, verifying organisational email addresses and credentials securely.

TR-DP-4 All authentication attempts must be logged, and sensitive credentials must be hashed using a secure algorithm before storage.

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.
Business rule:	
External requirements:	UI-4, UI-5, SI-8

TR-DP-5 The system shall implement secure data sharing using HTTPS with TLS 1.3 to ensure encryption during transmission and integrate with the Data Providers' technology stack via standardized APIs (e.g., REST, GraphQL).

TR-DP-6 Access control must be enforced using role-based access control (RBAC) or attribute-based access control (ABAC), ensuring that only authenticated and authorized users can access the shared data.

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.
Business rule:	
External requirements:	UI-8

TR-DP-7 The system shall implement a policy-based access control (PBAC) framework that allows Data Providers to assign granular permissions (e.g., view, distribute) to organisational users, stored securely in a database.

TR-DP-8 The system must provide an audit trail mechanism to log changes in access permissions and user activities, ensuring that access can be revoked in real time and all modifications are traceable.

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 organisational users.
Business rule:	
External requirements:	UI-5

TR-DP-9 The system shall provide a metadata management module that stores catalogue metadata and connection details in a structured format (e.g., JSON, JSON-LD) within a secure database, ensuring metadata compliance with industry standards such as DCAT, DCAT-AP and/or ODPS.

TR-DP-10 The system must include a secure API for authorized users or platforms to access published data products, enforcing authentication and authorization through token-based mechanisms like OAuth 2.0.

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.
Business rule:	
External requirements:	UI-5

TR-DP-11 The system shall implement a version control mechanism that tracks changes to each data product's metadata, storing version history, metadata updates, and tags in a relational database with unique version identifiers.

TR-DP-12 The system must provide a user-friendly interface and API for adding, updating, and querying metadata and tags, ensuring compliance with metadata standards such as DCAT, DCAT-AP and/or ODPS.

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.
Business rule:	
User interfaces:	UI-7

TR-DP-13 The system shall provide a template-based document editor with customizable fields for terms, conditions, and clauses, storing agreements securely in a version-controlled database.

TR-DP-14 The system should support digital signatures using standards like eIDAS, ZertES or DocuSign integration to ensure legally binding agreements and maintain audit trails.

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.
Business rule:	
External requirements:	UI-7

TR-DP-15 The system shall store standard agreement templates in a centralized repository, allowing users to retrieve and edit them via a dynamic document editor that supports text formatting and clause customization.

TR-DP-16 The system must implement access control for the library, ensuring only authorized users can view, edit, or save modified templates, with changes tracked in a version-controlled system.

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.
Business rule:	
External requirements:	UI-9

TR-DP-17 The system shall implement a real-time data tracking mechanism that logs user access events, including timestamps, user identity, and actions performed, storing this information in a secure, queryable database.

TR-DP-18 The dashboard must use a visualization library to display interactive charts, tables, and filters, enabling Data Providers to view and analyse access and usage trends over time.

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.
Business rule:	
External requirements:	UI-10

TR-DP-19 The system shall implement an audit logging framework that records all interactions with data products, including user identity, action type, timestamp, and affected resources, storing logs securely in a tamper-proof database.

TR-DP-20 The system must provide a report generation module that allows Data Providers to create customizable reports with filters (e.g., by user, action type, or date range) and export them in standard formats like PDF or CSV.

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.
Business rule:	
External requirements:	UI-11

TR-DP-21 The system shall implement automated data validation and integrity check routines, running on predefined schedules or triggers, and logging detected anomalies in a secure monitoring database.

TR-DP-22 A quality metrics dashboard must be provided, using a visualization library to display key indicators such as completeness, accuracy, consistency, and freshness of data, with drill-down capabilities for detailed analysis.

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.
Business rule:	
External requirements:	UI-12

TR-DP-23 The system shall implement a compliance rules engine that maps agreement-specified quality standards to measurable criteria, periodically evaluating data products against these criteria and storing results in a compliance database.

TR-DP-24 The system must provide an alerting mechanism to notify Data Providers of non-compliance via configurable channels (e.g., email, dashboard notifications), along with a reporting module to generate detailed compliance assessment reports in PDF or CSV formats.

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.
Business rule:	
External requirements:	UI-12

TR-DP-25 The system shall include a policy management module that enables Data Providers to define, update, and store data usage policies in a structured, version-controlled database, with support for attributes such as permissions, restrictions, and expiration rules.

TR-DP-26 The dashboard must provide an intuitive interface for policy creation and management and integrate with the access control mechanism to enforce these policies in real time.

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.
Business rule:	
External requirements:	UI-12

TR-DP-27 The system shall implement a policy validation engine that checks defined data usage policies against pre-established schema rules, using a rules-based or schema-driven approach (e.g., JSON Schema validation).

TR-DP-28 The system must provide real-time feedback on validation errors via the interface, highlighting issues and suggesting corrections, and trigger automated alerts (e.g., email or dashboard notifications) if inconsistencies are detected during policy creation or updates.

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).
Business rule:	
External requirements:	UI-12

TR-DP-29 The system shall include an access revocation module that updates permissions in the access control database in real-time, ensuring immediate enforcement of access restrictions upon revocation.

TR-DP-30 The user interface must provide a reason entry field (with predefined options and free text) and log the revocation details, including the reason, timestamp, and user ID, in a secure audit trail for compliance purposes.

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.
Business rule:	
External requirements:	SI-6

TR-DP-31 The system shall implement a scheduled task or event-driven mechanism to monitor agreement expiration dates and breach flags, automatically updating access permissions in the access control database to revoke access upon triggering conditions.

TR-DP-32 An automated notification system must alert relevant stakeholders (e.g., Data Providers and affected users) of access termination events, specifying the reason (expiration or breach) and including details of the impacted data products.

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.
Business rule:	
External requirements:	UI-6

TR-DP-33 The system shall include a request management module that logs incoming data access requests in a secure database and provides an interface for Data Providers to review, approve, or deny requests, with real-time updates to the access control system.

TR-DP-34 The interface must include a comment field for Data Providers to attach additional information or conditions, storing these along with the decision in an audit trail for traceability.

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.
Business rule:	
External requirements:	UI-12

TR-DP-35 The system shall include a communication module integrated with the agreement management interface, allowing secure message exchanges and document sharing between Data Providers and requesters, with all interactions logged in an audit trail.

TR-DP-36 An agreement version control system must be implemented to track and store all iterations of agreements, tagging each version with metadata such as timestamps, user IDs, and change summaries for traceability.

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.
Business rule:	BR-1, BR-2
External requirements:	UI-1, UI-2, UI-3

TR-DR-1 The interface must validate organisational email addresses in real time and ensure secure transmission of data via TLS 1.3.

TR-DR-2 The system must store collaborator registration data in a database with encryption algorithms approved in FIPS 140-3 and implement input sanitization to prevent injection attacks.

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.
Business rule:	BR-1, BR-2
External requirements:	UI-1, UI-2, UI-3

TR-DR-3 The system shall implement an authentication mechanism using OAuth 2.0 or OpenID Connect, verifying organisational email addresses and credentials securely.

TR-DR-4 All authentication attempts must be logged, and sensitive credentials must be hashed using a secure algorithm before storage.

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.
Business rule:	
External requirements:	UI-12

TR-DR-5 The system shall include a management module with a dashboard interface that displays the status of all data-sharing agreements (e.g.,

pending, accepted, declined), enabling Data Recipients to perform actions such as viewing, accepting, or declining agreements.

TR-DR-6 The module must maintain an audit trail that logs all actions taken on agreements, including timestamps, user IDs, and the status, stored securely in a tamper-proof database.

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.
Business rule:	
External requirements:	UI-12

TR-DR-7 The system shall implement a tracking module that monitors agreement terms, renewal dates, and expiration timelines, storing details in a structured database and automatically flagging upcoming deadlines or changes.

TR-DR-8 A notification system must be integrated to alert Data Recipients of updates, renewals, or expirations via configurable channels (e.g., email, in-app notifications), ensuring timely action and compliance.

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.
Business rule:	BR-3
External requirements:	UI-13

TR-DR-9 The system shall implement JDBC, RESTful and/or GraphQL APIs with secure authentication mechanisms (e.g., API keys or Json Web Tokens), enabling Data Recipients to query and retrieve data products efficiently.

TR-DR-10 The system could support data streaming protocols such as WebSocket, WebRTC, Apache Flink or Apache Kafka to deliver real-time data feeds, ensuring low-latency and reliable data access for subscribed recipients.

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.
Business rule:	BR-3
External requirements:	UI-13

TR-DR-11 The system shall provide data transformation and export tools that support multiple formats (e.g., JSON, CSV, XML) and protocols (e.g., FTP, HTTPS, API-based), ensuring compatibility with diverse systems.

TR-DR-12 The system must comply with interoperability standards such as OpenAPI or OData and include integration guides or SDKs to simplify embedding received data into existing workflows.

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 keywords, tags, publisher, and recency.
Business rule:	
External requirements:	UI-4

TR-DR-13 The system shall implement a searchable database of data products, supporting advanced query capabilities such as keyword search, filters (e.g., tags, publisher, recency), and sorting options (e.g., recency, popularity).

TR-DR-14 The user interface must include an intuitive search bar and filtering panel, with results displayed dynamically, and integrate with metadata standards like DCAT, DCAT-AP, ODPS for consistent data product descriptions.

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 requesting access and/or integrating the data.
Business rule:	
External requirements:	UI-4, UI-13

TR-DR-15 The system shall provide a data preview feature, allowing users to view a sample of the data product securely, with appropriate restrictions to prevent unauthorized downloading or misuse.

TR-DR-16 The system must implement a quality evaluation dashboard displaying metrics (e.g., completeness, accuracy, freshness) alongside user-generated reviews and ratings stored in a secure database for collaborative assessment.

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.
Business rule:	BR-3
External requirements:	UI-13

TR-DR-17 The system shall include a visualization module that supports generating and customizing various chart types (e.g., bar, line, pie, scatter plots) using a library with interactive features like tooltips, zooming, and/or filtering.

TR-DR-18 The visualization tools must integrate seamlessly with the data preview and analytics modules, allowing users to dynamically select datasets and configure graphical parameters through an intuitive interface.

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.
Business rule:	BR-3
External requirements:	UI-13

TR-DR-19 The system shall implement a query interface enabling users to construct queries, filters, and conditions, using standard query languages (e.g., SQL or SPARQL).

TR-DR-20 The interface could include guided search features, such as auto-suggestions, dropdowns for field selection, and tooltips, to assist users in refining queries and ensuring accurate results without requiring technical expertise.

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.
Business rule:	
External requirements:	UI-4

TR-DR-21 The system shall implement a full-text search engine to enable keyword-based queries, combined with filter options for metadata.

TR-DR-22 The user interface could feature a multi-faceted search panel with interactive dropdowns, checkboxes, and sliders for filtering, dynamically updating search results in real time based on user input.

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.
Business rule:	
External requirements:	UI-4

TR-DR-23 The system shall implement a dynamic filtering engine that supports combining multiple filters (e.g., by data type, provider, date range) using logical operators (e.g., AND, OR), with real-time updates to the displayed search results.

TR-DR-24 The user interface must provide an interactive filtering panel with options like dropdowns, checkboxes, and range sliders, ensuring filters can be adjusted or removed dynamically without reloading the page.

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.
Business rule:	
External requirements:	UI-14

TR-DR-25 The system shall implement a trustworthiness scoring engine that calculates trust scores for data products and providers based on weighted criteria (e.g., data quality metrics, compliance records, user feedback) stored in a secure database.

TR-DR-26 The user interface must display trust scores alongside data products in the catalogue, with an explanation of contributing factors and a breakdown of criteria to ensure transparency and assist Data Recipients in decision-making.

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.
Business rule:	
External requirements:	UI-14

TR-DR-27 The system shall implement a reputation management module that aggregates and displays provider reputation scores, calculated based on user-generated reviews, ratings, and predefined performance metrics, stored securely in a relational database.

TR-DR-28 The user interface must provide a feedback submission form for Data Recipients to leave ratings and detailed reviews, with moderation tools to filter inappropriate content and ensure data integrity.

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.
Business rule:	
External requirements:	UI-13

TR-DR-29 The system shall implement a secure data export module that supports downloading data products in multiple standardized formats such as CSV, JSON, and XML, ensuring compatibility with widely used tools and systems.

TR-DR-30 The download functionality must enforce access control policies and log all download events, including user identity, timestamp, and data product details, in a secure audit trail.

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.
Business rule:	BR-3
External requirements:	UI-13

TR-DR-31 The system shall provide standardized JDBC, RESTful and/or GraphQL APIs, adhering to specifications such as OpenAPI, to enable programmatic access to data products with support for querying, filtering, and retrieving data.

TR-DR-32 The APIs must include secure authentication mechanisms, such as API Keys or JSON Web Tokens, and detailed documentation with SDKs or code examples to facilitate seamless integration into recipient systems.

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.
Business rule:	BR-1, BR-2
External requirements:	UI-1, UI-2, UI-3

TR-GA-1 The interface must validate organisational email addresses in real time and ensure secure transmission of data via TLS 1.3.

TR-GA-2 The system must store collaborator registration data in a database with encryption algorithms approved in FIPS 140-3 and implement input sanitization to prevent injection attacks.

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.
Business rule:	BR-1, BR-2
External requirements:	UI-1, UI-2, UI-3

TR-GA-3 The system shall implement an authentication mechanism using OAuth 2.0 or OpenID Connect, verifying organisational email addresses and credentials securely.

TR-GA-4 All authentication attempts must be logged, and sensitive credentials must be hashed using a secure algorithm before storage.

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.
Business rule:	
External requirements:	UI-15

TR-GA-5 The system shall implement a governance management module with a user-friendly interface that allows the Data Space Governance Authority to create, update, and delete rules, policies, and procedures. These definitions must be stored in a structured, version-controlled database.

TR-GA-6 The module must include validation tools to ensure rules and policies comply with predefined schema or regulatory standards, with audit logging to track changes and maintain an immutable record of governance framework updates.

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.
Business rule:	
External requirements:	UI-15

TR-GA-7 The system shall implement a compliance monitoring engine that continuously audits participant activities against the defined governance framework, logging potential violations in a secure database and triggering automated alerts for review by the Governance Authority.

TR-GA-8 A dispute resolution module must be integrated, providing tools for submitting, tracking, and resolving compliance-related cases, with support for documenting evidence, assigning case statuses, and maintaining an audit trail of the resolution process.

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.
Business rule:	
External requirements:	UI-15

TR-GA-9 The system shall include a standards management module that allows the Governance Authority to select, store, and update standards, protocols, and vocabularies in a structured, centralized repository, supporting metadata tagging for efficient retrieval.

TR-GA-10 The module must provide integration tools for validating participant implementations against the selected standards and protocols, with reporting features to highlight compliance status and interoperability gaps.

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.
Business rule:	
External requirements:	UI-15

TR-GA-11 The system could include an integrated collaboration platform that supports secure messaging, document sharing, and real-time communication among participants, with access controls to manage permissions.

TR-GA-12 The system must provide data exchange interfaces and interoperability testing tools that verify compatibility with the selected standards and protocols, generating reports on compliance and offering suggestions for resolving issues.

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.
Business rule:	

External requirements:	UI-14

TR-GA-13 The system shall implement a complaint submission module with a user interface that includes structured fields for issue description, evidence upload (e.g., documents, images), and selection of the relevant data product or provider, storing all submissions securely in a complaint management database.

TR-GA-14 The system must support automated acknowledgment of submitted complaints via email or dashboard notifications, including a unique tracking ID for each complaint to facilitate follow-up and resolution tracking.

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.
Business rule:	
External requirements:	UI-16

TR-GA-15 The system shall implement a complaint management workflow module that tracks complaints through statuses such as "Submitted," "Under Review," "Resolved," and "Closed," with real-time updates and secure storage of related communication and resolution documentation.

TR-GA-16 The system must include a communication interface for the Governance Authority to interact with stakeholders, enabling message exchanges, evidence requests, and updates, with all interactions logged in a secure audit trail for transparency.

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.
Business rule:	
External requirements:	UI-15

TR-GA-17 The system shall include an activity tracking module that captures real-time events such as data access, modifications, and sharing, storing logs in a secure and queryable database for compliance monitoring.

TR-GA-18 The dashboard must provide interactive visualizations (e.g., charts, graphs, and tables) summarizing activity trends and anomalies, with drill-down capabilities to view detailed logs for specific events, users, or data products.

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.
Business rule:	BR-3
External requirements:	UI-15

TR-GA-19 The system shall implement an immutable audit logging mechanism that records all data space activities, including user actions, timestamps, and affected resources, storing logs securely in a tamper-proof database.

TR-GA-20 A reporting module must be provided, enabling the Governance Authority to generate detailed compliance reports with filtering and grouping options (e.g., by user, activity type, or time period) and export them in formats such as PDF or CSV.

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.
Business rule:	
External requirements:	UI-15

TR-GA-21 The system shall include a governance framework editor with a user-friendly interface that supports creating, updating, and publishing rules, policies, and guidelines, storing changes in a version-controlled database.

TR-GA-22 The interface must feature a review and approval workflow, allowing multiple stakeholders to propose, review, and approve changes before publication, with all actions logged in an audit trail for traceability.

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.
Business rule:	
External requirements:	UI-15

TR-GA-23 The system shall implement a version control system that tracks all changes to the governance framework, including timestamps, user IDs, and change descriptions, storing the history in a secure, queryable database.

TR-GA-24 The system must include an automated notification mechanism that alerts stakeholders via email or dashboard notifications of updates to the

framework, providing a summary of changes and access to the latest version.

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.
Business rule:	
External requirements:	UI-17

TR-PD-1 The system shall include a consent management module that allows Data Producers to create and update consent agreements using a template-driven interface, specifying usage permissions, authorized users, and conditions, with storage in a version-controlled database.

TR-PD-2 The system must provide tools for tracking consent status, enabling Data Producers to modify or revoke consent dynamically, with all changes logged in a secure audit trail to ensure transparency and compliance.

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.
Business rule:	
External requirements:	UI-17

TR-PD-3 The system shall implement an access control mechanism that dynamically enforces data usage policies based on the consent agreements, checking the terms before granting access to data and preventing unauthorized usage by Data Consumers.

TR-PD-4 The system must integrate with the data access layer to validate consent conditions in real-time during data access requests, logging all access attempts and enforcing restrictions according to the terms specified in the consent agreement.

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.
Business rule:	
External requirements:	UI-18

TR-PD-5 The system shall implement a data valuation engine that analyses data assets based on predefined criteria (e.g., type, quality, volume, uniqueness, market demand) and calculates an estimated value using an algorithm or set of business rules.

TR-PD-6 The dashboard must display valuation results with interactive visualizations, including charts and graphs, that allow Data Producers to explore different valuation criteria, with the ability to filter and adjust assumptions to reflect different market conditions.

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.
Business rule:	
External requirements:	UI-18

TR-PD-7 The system shall integrate with market analysis tools or third-party data sources to track and analyse market trends, using algorithms to generate insights about potential demand for specific data assets.

TR-PD-8 The system must provide a recommendation engine that suggests value-maximizing strategies for Data Producers, such as pricing models or target markets, based on current demand patterns and data asset characteristics. These insights must be visualized through an interactive dashboard for easy interpretation.

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.
Business rule:	
External requirements:	UI-18

TR-PD-9 The system shall implement a compensation management module that allows Data Producers to define, update, and store compensation terms, including pricing models, usage conditions, and remuneration structures, in a secure database with version control.

TR-PD-10 The system must provide an interface for generating and managing compensation agreements, offering Data Producers transparent pricing options and automated calculations based on usage or licensing terms, with export functionality for formal agreements (e.g., PDF or CSV).

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.
Business rule:	
External requirements:	UI-18

TR-PD-11 The system shall implement a payment tracking module that records all transactions related to data-sharing activities, including payment amounts, dates, and terms, storing this information in a secure, auditable database.

TR-PD-12 The system must provide a user interface where Data Producers can view detailed payment histories, with filtering options by transaction date, amount, or data asset, and generate audit reports in formats such as PDF or CSV for compliance verification.

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.
Business rule:	
External requirements:	UI-17

TR-SU-1 The system shall include a consent management module that allows Data Producers to create, update, and modify consent agreements, with customizable fields for specifying data usage terms, authorized users, and conditions.

TR-SU-2 The system must store all consent agreements in a secure, version-controlled database, and provide a mechanism for Data Producers to track the status of each consent agreement, including timestamps and user signatures for compliance and audit purposes.

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.
Business rule:	
External requirements:	UI-17

TR-SU-3 The system shall integrate an access control layer that dynamically enforces data usage policies by verifying consent agreements before granting access, ensuring data can only be accessed according to the specified terms and conditions.

TR-SU-4 The system must log all data access attempts and monitor compliance with consent terms, providing real-time alerts for unauthorized usage or policy violations and allowing Data Producers to revoke access as necessary.

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.
Business rule:	
External requirements:	UI-18

TR-SU-5 The system shall implement an analytics engine that processes data assets based on key criteria such as type, quality, volume, uniqueness, and market demand, generating an estimated value using a predefined algorithm or machine learning model.

TR-SU-6 The system must provide a dynamic, interactive dashboard with visualizations (e.g., graphs, charts) that allow Data Producers to view and adjust valuation metrics, and filter the data based on specific criteria for more granular insights.

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.
Business rule:	
External requirements:	UI-18

TR-SU-7 The system shall integrate with external market data sources (e.g., industry reports, market analysis tools) to analyse trends and forecast demand for specific data assets, using machine learning models or analytics algorithms.

TR-SU-8 The system must provide a recommendation engine that generates insights and strategies for Data Producers to optimize the value of their data assets, based on current market trends and demand patterns, with visualizations and actionable insights displayed on an interactive dashboard.

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.
Business rule:	

External requirements:	UI-18

TR-SU-9 The system shall include a compensation management module that allows Data Producers to define pricing models, usage conditions, and remuneration structures for their data assets, storing this information in a secure, version-controlled database.

TR-SU-10 The system must provide an interface for generating compensation agreements and automatically calculating payments based on usage or licensing terms, with export functionality for formal agreements (e.g., PDF or CSV) and transparency in payment history.

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.
Business rule:	
External requirements:	UI-18

TR-SU-11 The system shall implement a payment tracking module that securely records transaction details, including payment amounts, dates, and terms, storing this information in an auditable and tamper-proof database.

TR-SU-12 The system must provide a user interface that allows Data Producers to view transaction histories, filter by date or amount, and generate detailed audit reports in formats such as PDF or CSV, ensuring compliance and transparency in the payment process.

FR-ST-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.
Business rule:	BR-1, BR-2
External requirements:	UI-1, UI-2, UI-3

TR-ST-1 The system shall integrate with enterprise Single Sign-On (SSO) or federated identity management systems (e.g., SAML, OpenID Connect) to authenticate Data Scientists/Engineers based on their organisation-specific credentials.

TR-ST-2 The authentication system must ensure secure data transmission using TLS 1.3 and support role-based access control (RBAC) to assign appropriate permissions based on the user's organisation and role, logging all authentication events for audit purposes.

FR-ST-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.
Business rule:	BR-1, BR-2
External requirements:	UI-1, UI-2, UI-3

TR-ST-3 The system shall implement an integration with the organisation's identity provider (e.g., Active Directory or LDAP) to verify the authenticity of Data Scientists/Engineers' credentials during the authentication process, ensuring they are valid and linked to the correct organisation.

TR-ST-4 The system must include a validation mechanism that cross-references the authenticated user's identity with a list of approved organisation members, and logs all verification events for security and auditing purposes, ensuring compliance with access control policies.

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.
Business rule:	
External requirements:	UI-4, UI-5, UI-7, UI-9, UI-10, UI-11, UI-12, UI-14, UI-16, UI-18

TR-ST-5 The system shall provide Data Stewards with full administrative access privileges to perform activities such as data publishing, metadata management, data-sharing agreement drafting, and monitoring, through RBAC mechanisms.

TR-ST-6 The system must implement an audit logging feature that tracks all actions taken by Data Stewards, including data publishing, changes to metadata, agreement updates, and monitoring activities, ensuring transparency and accountability for all actions performed on behalf of the organisation.

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.
Business rule:	
External requirements:	UI-4, UI-5, UI-7, UI-9, UI-10, UI-11, UI-12, UI-14, UI-16, UI-18

TR-ST-7 The system shall implement a RBAC system that grants Data Stewards the appropriate permissions to manage data provisioning activities, such as

creating and modifying datasets, managing metadata, and overseeing data-sharing agreements.

TR-ST-8 The system must provide an interface for Data Stewards to oversee and track their organisation's data activities, including real-time access to data usage metrics, audit trails of data access, and the ability to configure and enforce organisational data policies.

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.
Business rule:	
External requirements:	UI-4, UI-6, UI-8, UI-9, UI-10, UI-11, UI-12, UI-13, UI-14, UI-16, UI-18

TR-ST-9 The system shall grant Data Stewards full access to perform Data Recipient activities, such as requesting data, viewing metadata, signing data-sharing agreements, and monitoring data access, using RBAC to define permissions.

TR-ST-10 The system must log all actions performed by Data Stewards in a secure audit trail, tracking activities like data requests, agreement signings, and access monitoring, ensuring transparency and accountability for actions taken on behalf of the organisation.

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.
Business rule:	
External requirements:	UI-4, UI-6, UI-8, UI-9, UI-10, UI-11, UI-12, UI-13, UI-14, UI-16, UI-18

TR-ST-11 The system shall implement a RBAC model that grants Data Stewards the necessary permissions to manage data-receiving activities, such as initiating data requests, reviewing metadata, and signing data-sharing agreements on behalf of their organisation.

TR-ST-12 The system must provide Data Stewards with an oversight interface that includes real-time monitoring of data access, status of agreements, and access logs, ensuring they can efficiently manage and track their organisation's data-receiving activities within the data space.

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 SSO or federated identity management systems.
Business rule:	BR-1, BR-2
External requirements:	UI-1, UI-2, UI-3

TR-DE-1 The system shall integrate with enterprise SSO solutions or federated identity management systems (e.g., SAML, OpenID Connect) to authenticate Data Scientists/Engineers based on their organisation-specific credentials, ensuring secure and seamless login.

TR-DE-2 The authentication process must enforce secure transmission using TLS 1.3 and validate the user's organisational affiliation during login, storing session details securely and providing RBAC to assign relevant permissions based on the user's organisation and role.

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.
Business rule:	BR-1, BR-2
External requirements:	UI-1, UI-2, UI-3

TR-DE-3 The system shall integrate with the organisation's identity provider (e.g., Active Directory, LDAP) to verify the organisational affiliation of Data Scientists/Engineers during the authentication process, ensuring their credentials match records within the organisation's system.

TR-DE-4 The system must implement real-time verification checks against the organisation's directory, using secure API calls or protocols like SAML or OpenID Connect, and log all verification events to ensure compliance with access control policies.

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.
Business rule:	BR-3
External requirements:	SI-8

TR-DE-5 The system shall implement a query interface (e.g., SQL-based, GraphQL, or RESTful API) that allows Data Scientists/Engineers to query data within the scope of their organisation's access permissions, ensuring that only authorized data is retrievable based on predefined access control policies.

TR-DE-6 The system must integrate with RBAC mechanisms to enforce permissions, allowing Data Scientists/Engineers to retrieve only the data their organisation has been granted access to, while logging all queries for audit purposes.

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.
Business rule:	BR-3
External requirements:	SI-7, SI-8

TR-DE-7 The system shall integrate with RBAC and/or ABAC mechanisms to enforce organisation-specific permissions, ensuring that Data Scientists/Engineers can only query and retrieve data sets their organisation is authorized to access.

TR-DE-8 The system must validate each query request against the organisation's permissions before data retrieval, logging all access attempts (successful and unsuccessful) for auditing and compliance purposes, and preventing unauthorized data access through real-time enforcement.

FR-DE-5	Integrated Data Analysis Toolkit: The system shall provide Data Engineers with access to a suite of data analysis and processing tools, including both open-source (e.g., Python, R, Apache Spark) and commercial solutions.
Business rule:	BR-3
External requirements:	SI-9

TR-DE-9 The system shall integrate pre-configured open-source and commercial data analysis tools (e.g., Python, R, Apache Spark, Tableau) within a secure environment, ensuring that Data Engineers can access and use these tools without the need for external installations.

TR-DE-10 The system must provide RBAC to restrict tool usage based on user roles and permissions, ensuring that only authorized Data Engineers can utilize specific tools or perform data processing activities, while maintaining data security and compliance.

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.
Business rule:	BR-3
External requirements:	SI-9

TR-DE-11 The system shall implement a secure, isolated sandbox environment using containerization technologies to enable Data Engineers to perform data analysis and processing tasks without compromising the security of production data or systems.

TR-DE-12 The sandbox environment must enforce data access policies, logging all activities and restricting access to sensitive data based on user permissions, while providing Data Engineers with flexibility in tool usage and integration with data analysis frameworks such as Python, R, and Apache Spark.

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.
Business rule:	BR-3
External requirements:	SI-5, SI-6, SI-10

TR-DE-13 The system shall implement a real-time activity monitoring module that logs all data access, modifications, and processing actions performed by Data Engineers, storing this information securely in a centralized, queryable audit log.

TR-DE-14 The system must provide automated alerts for any activities that deviate from predefined policies or regulatory requirements, with role-based access to view logs, and offer comprehensive reporting features to track compliance and generate audit reports for review.

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.
Business rule:	BR-3
External requirements:	SI-5, SI-6, SI-10

TR-DE-15 The system shall implement an immutable logging mechanism that records all actions performed by Data Engineers, including data access, modifications, and processing tasks, ensuring that logs are tamper-proof and stored in a secure, write-once, read-many (WORM) databases.

TR-DE-16 The system must include query and export capabilities for the audit logs, allowing authorized users to generate detailed reports in formats such as PDF or CSV, for compliance reviews, regulatory reporting, and internal audits.

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 SSO or federated identity management systems.
Business rule:	BR-1, BR-2
External requirements:	UI-1, UI-2, UI-3

TR-LC-1 The system shall integrate with enterprise SSO or federated identity management systems (e.g., SAML, OIDC) to authenticate Data Scientists/Engineers based on their organisation-specific credentials, ensuring secure and seamless login.

TR-LC-2 The authentication system must support secure communication using TLS 1.3, validate the user's organisational affiliation during login, and RBAC to assign relevant permissions based on the user's organisation and role.

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.
Business rule:	BR-1, BR-2
External requirements:	UI-1, UI-2, UI-3

TR-LC-3 The system shall integrate with the organisation's identity provider (e.g., Active Directory, LDAP) to verify the organisational affiliation of Data Scientists/Engineers during the authentication process, ensuring their credentials match records within the organisation's system.

TR-LC-4 The system must perform real-time verification of the authenticated user's organisational membership, ensuring that only valid, recognized members are granted access to organisation-specific data and collaboration tools. All verification actions shall be logged for audit purposes.

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.
Business rule:	
External requirements:	UI-12

TR-LC-5 The system shall include an agreement management interface that allows Legal Counsel to review, approve, and request the voiding of agreements,

with tools for displaying agreement terms, highlighting key clauses, and enabling inline annotations or comments.

TR-LC-6 The system must implement RBAC to ensure only Legal Counsel can approve or void agreements, and include an audit trail to log all actions, including approval timestamps, voiding requests, and any comments submitted for compliance and review.

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.
Business rule:	BR-3
External requirements:	SI-5, SI-6, SI-10

TR-LC-7 The system shall provide a comprehensive audit and compliance monitoring module that enables Legal Counsel to access agreement histories, including version changes, approvals, amendments, and voiding requests, stored securely in a version-controlled database.

TR-LC-8 The system must generate automated compliance reports, detailing adherence to legal and organisational policies, and allow Legal Counsel to export these reports in formats such as PDF or CSV for further review and documentation.

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 SSO or federated identity management systems.
Business rule:	BR-1, BR-2
External requirements:	UI-1, UI-2, UI-3

TR-AU-1 The system shall integrate with enterprise SSO or federated identity management systems (e.g., SAML, OpenID Connect) to authenticate Data Scientists/Engineers using organisation-specific credentials, ensuring secure and streamlined login.

TR-AU-2 The authentication system must support secure communication via TLS 1.3 and validate the user's organisation membership during login, leveraging RBAC to assign appropriate permissions based on the authenticated user's organisation and role.

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.
Business rule:	BR-1, BR-2
External requirements:	UI-1, UI-2, UI-3

TR-AU-3 The system shall integrate with the organisation's identity provider (e.g., Active Directory, LDAP) to verify the organisational affiliation of Data Scientists/Engineers during the authentication process, ensuring their credentials are valid and align with organisational records.

TR-AU-4 The system must perform real-time verification against the organisation's directory to confirm that the authenticated user is a legitimate member, allowing access to organisation-specific resources while logging all verification actions for auditing and compliance purposes.

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.
Business rule:	BR-3
External requirements:	UI-12

TR-AU-5 The system shall implement an agreement access module that allows Auditors to securely access and view all relevant agreements, with full details of terms, conditions, and associated metadata, stored in a read-only format for review.

TR-AU-6 The system must provide an audit trail feature that logs all actions taken by Auditors, including viewing, accessing, or downloading agreements, ensuring compliance with internal policies and regulatory requirements for transparency and accountability.

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.
Business rule:	BR-3
External requirements:	SI-5, SI-6, SI-10

TR-AU-7 The system shall implement a compliance monitoring module that tracks all activities related to agreements, including data access, modifications, and sharing, and stores this data in an audit log that is accessible to Auditors for review.

TR-AU-8 The system must generate automated compliance reports that include key metrics on adherence to agreement terms and allow Auditors to filter and

export these reports (e.g., in PDF or CSV format) to verify that all parties are compliant with the agreed-upon terms.

8 References

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/pdfrfc/rfc2119.txt.pdf.

Intellisoft. 2024. *Functional vs technical requirements.* 27 09. Accessed 11 13, 2024. https://intellisoft.io/functional-requirements/.