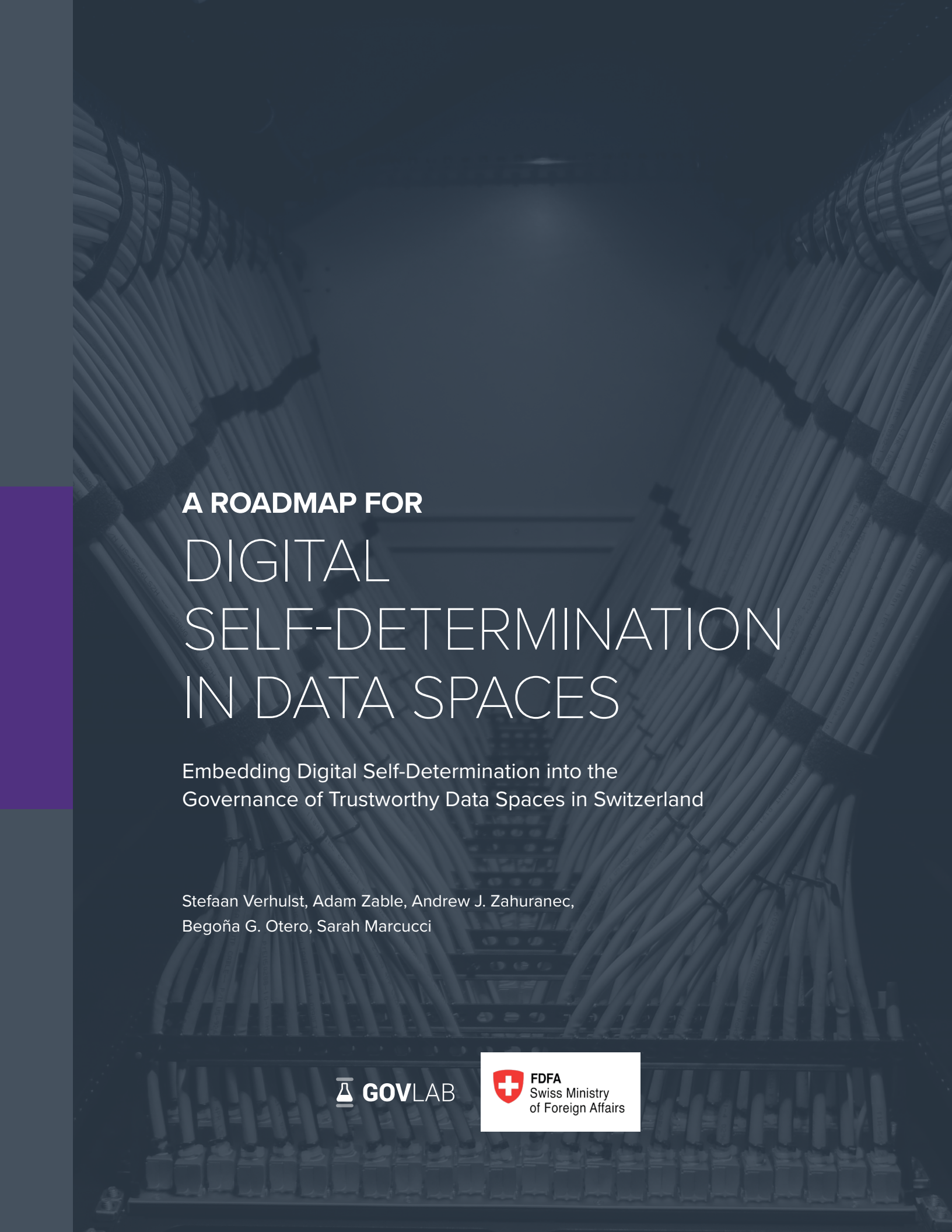


A ROADMAP FOR

DIGITAL SELF-DETERMINATION IN DATA SPACES

Embedding Digital Self-Determination into the Governance of Trustworthy Data Spaces in Switzerland

Stefaan Verhulst, Adam Zable, Andrew J. Zahuranec,
Begoña G. Otero, Sarah Marcucci

GOVLAB

FDFA
Swiss Ministry
of Foreign Affairs

A ROADMAP FOR

DIGITAL SELF-DETERMINATION IN DATA SPACES

Embedding Digital Self-Determination into the Governance of Trustworthy Data Spaces in Switzerland

Stefaan Verhulst, Adam Zable, Andrew J. Zahuranec,
Begoña G. Otero, Sarah Marcucci

GOVLAB

FDFA
Swiss Ministry
of Foreign Affairs

Acknowledgments

This report's authors wish to express their appreciation to the many individuals who contributed to this document's development. We are indebted to Federica Zavattaro (University of Zurich) for her work reviewing and contributing to drafts and helping to build the conceptual framework. We also deeply appreciate the regular guidance and feedback from our partners in the Federal Administration of Switzerland, especially the Focal Point on Trustworthy Data Spaces, including Pablo Wey, Celiane Pochon, Tiffany Maurer, Cyrille Gattiker, and Felix Gille.

Cite as: Verhulst, Stefaan, Adam Zable, Andrew J. Zahuranec, Begoña G. Otero, and Sarah Marcucci. (2026). A Roadmap for Digital Self-Determination in Data Spaces. The GovLab.

CONTENTS

Executive Summary

Switzerland has set ambitious goals for digitally enabled public services, data-driven innovation, and responsible artificial intelligence, particularly in health, research, and public administration. Data spaces are becoming an important mechanism for implementing national data policy and enabling the multiple use of data across sectors. However, strong implementation requires not just technical capacity but also governance arrangements that can support sustained data reuse while maintaining public trust and institutional legitimacy. Existing governance approaches, largely built around individual consent, bilateral data sharing agreements, and sector-specific rules, are increasingly strained in contexts where data is reused across institutions, purposes, and borders, and where automated systems mediate access, analysis, and decision-making (see Section 1.1).

Digital Self-Determination (DSD) has emerged as one important response to these pressures. DSD reframes data governance around ongoing agency rather than one-time consent, emphasizing transparency, meaningful choice, institutional accountability, and mechanisms for oversight across the full data lifecycle (see Section 2.1). In the Swiss context, DSD offers a normative and practical foundation for reconciling data reuse with public expectations of autonomy and protection, particularly in sensitive domains such as health.

At the same time, trustworthy data spaces are becoming an important implementation vehicle for Switzerland's data policy ambitions. Data spaces are designed to enable structured, rule-based data sharing across organizational boundaries while embedding safeguards for security, access control, and purpose limitation. Yet without robust governance architectures, data spaces risk scaling existing problems rather than resolving them—formalizing technical interoperability without addressing deeper questions of responsibility, agency, and legitimacy.

DSD is a concept that supports data spaces as a vehicle for data (re-)use and policymaking. Data spaces provide the operational infrastructure that enables data reuse in practice. DSD provides the governance logic that makes such reuse socially acceptable, institutionally accountable, and sustainable over time. Without DSD, data spaces risk becoming technically functional but politically fragile. Without data spaces, DSD remains difficult to operationalize at scale.

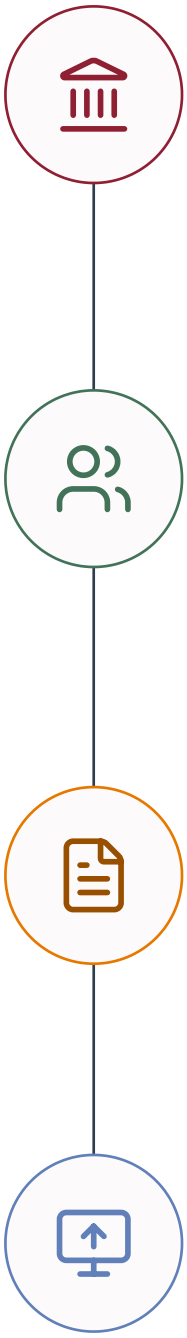
To date, DSD in Switzerland has remained largely conceptual. While high-level principles and codes of conduct exist, stakeholders lack an operational roadmap for embedding DSD consistently across data space governance including institutional roles and decision processes. This gap makes it difficult for data space operators, public authorities, and participating organizations to translate normative commitments into concrete, enforceable practice (see Section 2.3).

This roadmap seeks to address that gap. It seeks to provide an implementable architecture for operationalizing Digital Self-Determination within Switzerland's data ecosystem, with a particular focus on trustworthy data spaces as the primary site of action. It is intended for data space architects, governance authorities, and organizations or individuals responsible for designing and operating data sharing infrastructures. It builds directly on existing Swiss policy instruments, including the Federal Council report Creating trustworthy data spaces based on digital self-determination and the Code of Conduct for operating trustworthy data spaces based on digital self-determination, and focuses on how their principles can be implemented in practice (See Section 4). To support implementation, it introduces concrete tools intended to guide data space operators as they try to integrate DSD into data space governance, tailored to the institutional realities of the Swiss data ecosystem, which are provided in the appendices.

The roadmap is structured around four sequential but iterative phases. This starts with the most basic aspects of building a data space (establishing governance), with each successive phase building on that with additional mechanisms to incorporate digital self-determination into data space activities. For each phase, the roadmap includes a tool which offers guidance on how to best implement digital self-determination (see next page).

Taken together, these phases allow digital self-determination to be central at any phase of data space deployment. They seek to offer Switzerland a credible path to strengthening trust, enabling responsible data reuse, and supporting a resilient, participatory data ecosystem aligned with its democratic and federal traditions.

Figure 1: Roadmap for Digital Self-Determination in Data Spaces



ESTABLISH GOVERNANCE FOUNDATIONS

Defines purpose, principles, roles and responsibilities, decision rights, and accountability arrangements that form the basis for legitimate participation.

TOOLS

Assessment for Data Space Governance;

Guidance on Costs for Digital Self-Determination Implementation in a Data Space

ENABLE THE EXPRESSION OF EXPECTATIONS, INTERESTS, AND PREFERENCES

Introduces participatory and deliberative mechanisms through which individuals, groups, and communities can articulate expectations and boundaries regarding data use.

TOOL

Guidance on Public Engagement Mechanism Selection

TRANSLATE EXPECTATIONS INTO OPERATIONAL GOVERNANCE PRACTICES

Focuses on embedding expressed expectations into binding rules, contracts, technical controls, and oversight mechanisms across the data lifecycle.

TOOLS

List of Governance Instruments in Data Spaces

Model Swiss Data Sharing Agreement with Digital Self-Determination Clauses

CONTINUOUSLY STRESS TEST AND VALIDATE LEGITIMACY, ADAPTABILITY, AND BENEFIT

Uses monitoring, stress testing, and review processes to assess legitimacy, respond to emerging risks, and adapt governance over time.

TOOL

Options for Stress Testing DSD

CONTINUOUS LEARNING AND ADAPTATION

Source: Created by CCM Design

I. Introduction

1. Context and Purpose of This Roadmap

Switzerland's administrative, health, research, and innovation systems rely on the availability and (re-)use of high-quality, trustworthy data. Federal initiatives such as DigiSanté and the Swiss Data Ecosystem aim to modernize these systems, improve data flows, and enable new forms of value creation across the public and private sectors. At the same time, advances in machine learning and AI introduce new risks linked to opacity, asymmetrical capabilities, and collective or downstream harms.

While there is no shortage of privacy and data protection frameworks, these systems were designed for digital ecosystems where data collection and (re-)use were relatively limited and predictable. This is no longer the case. Today's data ecosystems are decentralized and interconnected. Sensitive inferences can be drawn from non-sensitive data. Assets are used well beyond its original purpose. All these developments pose serious governance challenges—unrealistic burdens posed on individuals, the question of whether static, one-off authorization is sufficient for reuse, and the limits of binary choice in a fluid ecosystem.

Digital Self-Determination (DSD) is the principle of respecting, embedding, and enforcing people's and peoples' agency, rights, interests, preferences, and expectations throughout the digital data life cycle in a mutually beneficial manner for all parties involved.[1] It offers a new approach to data governance and data protection that aligns data systems with communities and their changing preferences. It shifts governance from one-time permissions to ongoing agency, from isolated transactions to system-level oversight, and from individual consent alone to a combination of individual and collective rights, participatory mechanisms, and institutional accountability.

It is also a principle that is complementary to Switzerland's growing reliance on data spaces—decentralized infrastructure that enables data transactions between different ecosystem parties.[2] Data spaces emphasize subsidiarity, decentralization, and interoperability with coherence maintained through a governance framework.[3] A strong governance framework is one that all parties can agree on, one that supports their various commitments and translates abstract interests into concrete rules. Many data spaces in Switzerland already contain many of the commitments one would expect from systems designed for DSD.

The purpose of this roadmap is to outline how Digital Self-Determination can be further embedded within Switzerland's data ecosystem. It offers a structured narrative, governance architecture, and implementation sequence for applying DSD across the technical, organizational, and legal components of these systems.

2. How This Roadmap Is Organized

This document is written primarily for those responsible for the design, governance, and operation of data spaces within the Swiss data ecosystem. It is organized as follows:

Chapter I. Introduction offers context for this research and an overview of how data spaces are currently governed in the Swiss data ecosystem. It details the current institutional set-up, reference architecture, and key national initiatives that form the operational context for this work, including the Swiss Health Data Space developed under DigiSanté.

Chapter II. Foundations of Digital Self-Determination clarifies digital self-determination's conceptual basis, core dimensions, requirements for operationalization, international context, and relationship to adjacent concepts such as digital sovereignty.

Chapter III. A Roadmap for Implementing Digital Self-Determination Within Data Spaces explains how an organization might implement DSD structured around four iterative phases:

- Establishing governance foundations;
- Enabling the expression of expectations;
- Translating expectations into binding governance practices; and
- Continuously validating and adapting governance over time.

Each phase is supported by practical governance tools, including participatory mechanisms, governance instruments, consent and control mechanisms, and stress-testing and review approaches.

Chapter IV. Conclusion reflects on implications for implementation and sequencing.

Appendices:

Appendix I: Assessment for Data Space Governance An assessment tool for evaluating governance readiness across the four governance components (Purpose, Principles, Processes, and Practices).

Appendix II: Guidance on Costs for DSD Implementation in a Data Space A framework for identifying, estimating, and planning the organizational, technical, legal, and financial resources required to implement and sustain DSD over time.

Appendix III: Guidance on Public Engagement Mechanism Selection A taxonomy of participatory mechanisms with guidance on selecting and applying the most appropriate approaches to engage stakeholders and incorporate their expectations into governance decisions.

Appendix IV: List of Governance Instruments in Data Spaces A reference guide to the legal, organizational, technical, and procedural instruments available to translate governance decisions and participatory outcomes into operational data space practices.

Appendix V: Model Swiss Data Sharing Agreement with DSD Clauses A model agreement showing how DSD principles, stakeholder expectations, and governance requirements can be translated into binding provisions for data access, use, oversight, accountability, and adaptation.

Appendix VI: Options for Stress Testing Digital Self-Determination A set of approaches for testing whether governance arrangements remain legitimate, effective, adaptable, and aligned with stakeholder expectations as uses, risks, and circumstances evolve.

II. Foundations of Digital Self-Determination

1. How Digital Systems Complicate Self-Determination

Digital Self-Determination has emerged in response to changes in how data is generated, exchanged, and (re-)used in an interconnected world. The growing number of institutional, sectoral, and technical systems means that choices that affect communities are often made at a distance. Choices are embedded in systems that data providers cannot easily see, understand or influence.

This trend complicates the political and legal traditions that directly connect the legitimacy of systems to the consent of the people who sustain it. It is difficult to exercise personal autonomy and freedom from arbitrary interference if the system does not seek their input, if they have no ability to shape the rules that govern their lives. The *International Covenant on Civil and Political Rights* recognizes that all people possess the right to "freely determine their political status and freely pursue their economic, social and cultural development".[4]

However, many institutions have been slow to extend this right into digital spaces, where algorithmic and automated processes have dominated.[5] Where there is transparency, data governance has relied heavily on individual choice. Guided by existing data privacy law, individuals are expected to understand every duty, learn about the limits and scope of data use, and provide consent based on standards others impose. Among other issues, this dynamic assumes transparency and knowledge of how data is reused across systems, harnessed by many actors, and applied through complicated systems.[6] Future uses are difficult to anticipate in this context and one-off decisions to "opt in" or "opt out" fail to adequately address downstream impacts. It also fails to address individual expectations, larger societal interests, or how these both can shift over time in response to new information.[7]

This challenge is structural—a result of "**agency asymmetry**". Data-driven systems often concentrate decision-making power in institutions that control data infrastructure. Meanwhile, individuals and communities face high informational, technical, and organizational barriers to influence those decisions.[8] Even in systems that recognize the human right of people to meaningfully dictate how others use their information, people often lack the practical ability to shape how data about them is interpreted or acted upon.[9]

2. How Digital Self-Determination Alters This Dynamic

DSD responds to these challenges by reframing governance to focus on the conditions that can make agency possible. Instead of centering individual actions—an "opt-in" prompt for example—DSD looks at whether individuals and affected groups can understand how data is used and influence the rules that govern it. It pushes institutions to act responsively to people and their expectations around purpose, beneficiaries, risk, and other topics. This shifts the focus from individuals to the ways that systems are designed, the roles they require, and the processes that shape how data is used across its full lifecycle.

The mindset offered by DSD also helps organizations to address data system complexity in a world where data's impact extends beyond what is legally defined personal data. It acknowledges that data that is aggregated, anonymized, or combined with other non-personal assets can still impact the well-being of individuals. Even when it no longer meets the strict legal criteria for personally identifiable information, it is still data for and about them. Risk scores, classifications, and behavioral predictions affect access to services and opportunities and how people are treated—collectively and individually.[10] These impacts may not be visible or contestable under traditional data protection frameworks.[11] This fact is particularly relevant amid the rise of federated and AI-enabled environments where new uses emerge continuously, risks evolve as datasets are combined, algorithmic inference chains are opaque, and accountability is distributed.

DSD therefore functions as a normative governance principle. It provides a lens for assessing whether data-driven systems reduce agency asymmetries over time. It creates credible pathways for influence, allowing people to contest data use and make systems adapt. If realized through institutionally grounded decision-making authority, participatory mechanisms, governance mechanisms that translate expectations into rules, and regular renewal cycles, it ensures that as data is reused across contexts and expectations shift, institutions shift as well.

3. How Digital Self-Determination is Operationalized

To be more than an aspirational value, DSD must be practically embedded into how organizations and data spaces operate. While there is no single implementation model suitable for all contexts (and governance may be distributed across systems, processes, and cultures), data space operators may find it useful to organize implementation efforts around a simple heuristic that breaks governance into manageable components:

PURPOSE

Purpose is the final destination for all data activities. It defines the why of a data space, that being the end goal that all people involved in the effort are working toward. A well-defined purpose often indicates who it is seeking to inform or serve or the pathway to achieve that goal.

PRINCIPLES

Principles are the compass for activities. They set the direction that the data space will travel as it seeks to accomplish the purpose. They are the values, norms, and commitments that the data space organizer seeks to uphold through their work.

PROCESSES

Processes are the means by which a data space travels. It is the means of making decisions, the operational backbone of a data space. It defines workflows for data collection, validation, sharing, and retirement as well as individual roles and responsibilities. Strong processes operationalize work, engage stakeholders, and clarify accountability.

PRACTICES AND POLICIES

Practices and policies are the individual steps taken toward the destination. These are the concrete, enforceable rules, standards, and tools that put governance into action. They are how people manage day-to-day activities of the data space and involve themselves in planning, acquisition, processing, sharing, reusing, and monitoring.

The 4Ps are mutually reinforcing. Purpose and Principles establish direction, while Processes and Practices operationalize and enforce that direction. We use the 4Ps as a framework to guide the roadmap.

4. Digital Self-Determination and Data Space Governance in the International Context

While this report offers guidance tailored to Switzerland, similar efforts to institutionalize DSD are emerging globally. These efforts—detailed below—reveal two key facts: First, only a few jurisdictions are relying on data spaces for their governance strategies. These models instead use many kinds of data-sharing systems but prioritize sovereignty, interoperability, and data federation. This supports technical and legal infrastructure but underemphasizes participatory governance and ongoing legitimacy. Trust in these models is usually operationalized through technical safeguards rather than a focus on public trust and societal engagement. Second, there is a growing recognition that traditional, compliance-based governance is insufficient to maintain legitimacy, trust, and agency as data reuse and AI applications expand. This recognition underscores the importance of public legitimacy and ongoing societal engagement in governance processes.

The following examples illustrate some of the major approaches to data space governance and participatory data governance internationally. While several countries are making strides with governance models for data spaces and participatory data governance, Switzerland stands out as the only country explicitly attempting to integrate Digital Self-Determination into data space governance.

Jurisdiction	Illustrative Initiative(s)	Relevance to DSD
European Union	EHDS, Gaia-X, DSSC	Regulatory frameworks and interoperable data spaces that strengthen individual rights and institutional governance
Japan	DATA-EX, Open Data Spaces	Federated, interoperable technical infrastructure for cross-sector data sharing
Australia	Data & Digital Government Strategy	Social license and co-design in public-sector data governance
New Zealand	Ngā Tikanga Paihere	Indigenous participation and stewardship
Canada	HDRN Public Engagement	Translation of public expectations into concrete governance requirements through citizen deliberation.
Taiwan	vTaiwan	Mechanisms for continuous public participation and government responsiveness.

DATA SPACE GOVERNANCE

EUROPEAN UNION

The European Health Data Space (EHDS) Regulation, adopted in 2025, is one of the first sector-specific implementations of a data space concept within the European Union (EU). It provides a framework for electronic health data that supports both primary use (e.g. healthcare delivery and patient access/control) and secondary use (e.g. research, innovation, policy-making, and regulatory purposes), creating interoperable infrastructure and governance structures to enable these use across EU member states. The regulation grants individuals the right to access, share, and manage their health data. It supports data portability, access logs, opt-out options, and correction rights. These provisions strengthen individual agency and data sovereignty.[12]

While the EHDS ensures compliance with European data protection laws, it lacks robust participatory governance mechanisms that would allow citizens and affected communities to influence ongoing decisions regarding health data use.[13] The regulation also emphasizes individual rights and data protection but does not fully incorporate mechanisms for ongoing legitimacy or bottom-up feedback that are central to DSD.

The Data Spaces Support Centre (DSSC) is a European Commission-funded coordination and support action within the EU's Digital Europe Programme that aims to accelerate the creation of sovereign, interoperable, and trustworthy data spaces across sectors.[14] Through the *Data Spaces Blueprint*, the DSSC provides guidelines and building blocks for governance, business, legal, and technical dimensions of data spaces. While it includes modules on participation management and governance authority, it focuses more on technical interoperability and institutional governance, without fully embedding the participatory structures that DSD seeks to establish.[15]

Gaia-X, another significant EU initiative, focuses on creating a federated, interoperable data infrastructure to support data sovereignty across industries and public sectors. While Gaia-X helps develop domain-specific data spaces adhering to common standards and transparency principles, it does not explicitly integrate collective participation mechanisms. Its emphasis on federation, transparency, and trust aligns with a governance orientation stronger than traditional infrastructure models but does not directly address ongoing societal engagement or public accountability, which are core to the DSD framework.[16]

JAPAN

Japan is pursuing a federated, cross-sector approach to data spaces, with a focus on data sovereignty, interoperability, and the development of shared infrastructure. The Data Society Alliance (DSA)—a collaboration between industry, government, and academia—leads efforts to create interoperable data ecosystems and facilitate cross-sector data circulation through shared standards and technologies. The DSA seeks to establish a cohesive framework for data sharing across multiple sectors, aligning stakeholders around a common vision of secure, sovereign data exchange.[17]

At the heart of these efforts is DATA-EX, a federated data exchange platform designed to enable seamless cross-domain data sharing while ensuring that data sovereignty remains with the data providers. DATA-EX provides critical capabilities, such as data cataloging, discovery, authentication, authorization, provenance tracking, and quality evaluation. It is set to enter full production shortly, offering organizations the flexibility to build custom data sharing infrastructures tailored to specific sectoral and local needs, while maintaining interoperability with global frameworks like Gaia-X.[18]

Japan's data space strategy emphasizes:

- **Data sovereignty**, allowing data providers to retain control over how their data is shared;
- **Fairness**, ensuring equitable access through a common digital platform; and
- **Interoperability**, enabling cross-domain data exchange while respecting local regulations.[19]

To consolidate and advance this vision, Japan's Open Data Spaces initiative seeks to create a unified technical specification for data spaces across sectors, rebranding the country's data space efforts under the Open Data Spaces moniker. The Information-Technology Promotion Agency (IPA) will play a key role in facilitating this effort, including the creation of a secretariat to oversee development and hosting events like the Open Data Spaces Summit, aimed at engaging international stakeholders and promoting collaboration.[20]

Further accelerating this development is the formation of the Japan Data Space Alliance (JDSA), a collaborative body comprising the DSA, Digital Policy Forum Japan, Japan Digital Trust Forum, and the Robot Revolution & Industrial IoT Initiative. The JDSA aims to promote data space adoption, foster policy development, create cross-sector use cases, and ensure global interoperability, working to establish a trustworthy and cohesive data ecosystem in Japan.[21]

Japan's focus is on technical infrastructure, sovereignty, legal control, and interoperability, while not emphasizing participatory governance mechanisms or collective agency.

PARTICIPATORY DATA GOVERNANCE

AUSTRALIA

Australia's *Data and Digital Government Strategy* commits the federal government to collaborative, human-centered design grounded in co-design.[22] This emphasis on agency is especially visible in health and public data initiatives, where the concept of a social license is frequently used to describe public acceptance beyond formal compliance. The *Evidence Brief on Social license for Health Data* (2023) highlights participatory engagement, transparency, and continuous feedback as central to legitimacy.[23] At the same time, analysis suggests that existing data sharing legislation remains fragmented and that governance gaps persist in the absence of consistent terminology, access infrastructure, and enforceable participation mechanisms.[24]

NEW ZEALAND

Stats NZ measures its "social license to operate" through four pillars: value of data, safe data, trust and transparency, and working together.[25] These principles are operationalized through governance requirements tied to access to the Integrated Data Infrastructure. The *Ngā Tikanga Paihere* framework embeds Māori participation, cultural values, and oversight into data governance, with adherence treated as a condition for continued access.[26]

CANADA

Health Data Research Network Canada conducted a large-scale public and patient engagement process in 2024 to define which uses and users of health data fall within social license. The process produced 85 governance requirements related to benefits, fairness, oversight, privacy, and transparency. Findings showed conditional public support for health data use, alongside persistent concerns regarding commercial use and the use of data about marginalized populations.[27]

TAIWAN

Taiwan's *vTaiwan* platform combines online and in-person deliberation to allow citizens to raise issues, debate solutions, and submit proposals to the government. When proposals receive sufficient public support, ministries are required to respond formally.[28]

5. Distinguishing Digital Self-Determination and Digital Sovereignty

Recently, national and regional digital policy debates have framed digital sovereignty as a strategic policy goal. The Swiss Federal Council, for example, has adopted a report on Switzerland's Digital Sovereignty that defines digital sovereignty as the state's capacity to act in and monitor the digital space in order to fulfill its public functions, and notes geopolitical and technological pressures that shape this agenda.[29] Similar framings appear across Europe and elsewhere, where policy attention centers on resilience, control of infrastructure, and the management of technological dependencies in a rapidly evolving global digital economy.[30]

However, digital sovereignty is not digital self-determination and involves different kinds of agency. Digital sovereignty concerns a state's or institution's authority over digital infrastructure, data governance frameworks, and technological capabilities within its jurisdiction. It emphasizes collective control and institutional resilience in response to geopolitical competition, cross-border data flows, and strategic dependencies.[31] In this frame, state institutions are the vehicle to realize agency. Yet, authority over infrastructure, however necessary, does not settle the deeper question: what ultimately matters is who has the power to shape, govern and challenge the systems built upon it.[32]

DSD, in contrast, is the ability of individuals and communities to influence how data about them is governed, shared, and used. It operates at the level of individual and collective agency, rather than at the level of states or institutions. It centers autonomy and accountability, rather than territorial authority or strategic control. DSD aligns governance requirements that address questions of individual and collective agency—questions that sovereignty-oriented approaches do not resolve.

Digital sovereignty provides a stable institutional and infrastructural foundation. DSD, meanwhile, guides the participatory and accountability mechanisms needed to sustain legitimacy and trust over time.

A ROADMAP FOR IMPLEMENTING DIGITAL SELF-DETERMINATION WITHIN DATA SPACES

From Foundations to Implementation

The preceding sections establish Digital Self-Determination as a governance principle and clarify why it requires systematic operationalization in data spaces in Switzerland. The remainder of this document translates that foundation into an implementable roadmap for data space architects, governance authorities, and organizations responsible for designing and operating data spaces within the Swiss data ecosystem.

The roadmap is organized around **four core governance functions** that must be designed, implemented, and sustained for DSD to operate in practice. These functions describe the recurring work required to embed agency, legitimacy, and accountability into data space governance and have it remain effective over time. Specifically, operationalizing DSD requires data spaces to:

- **Establish governance foundations**, including purpose, principles, roles, decision rights, and accountability structures;
- **Enable the expression of expectations, interests, and preferences** through participatory and deliberative mechanisms;
- **Translate expressed expectations into binding governance practices**, including rules, contracts, technical controls, and oversight arrangements; and
- **Continuously validate and adapt governance,** using monitoring, stress testing, and review processes to maintain legitimacy, responsiveness, and public benefit.

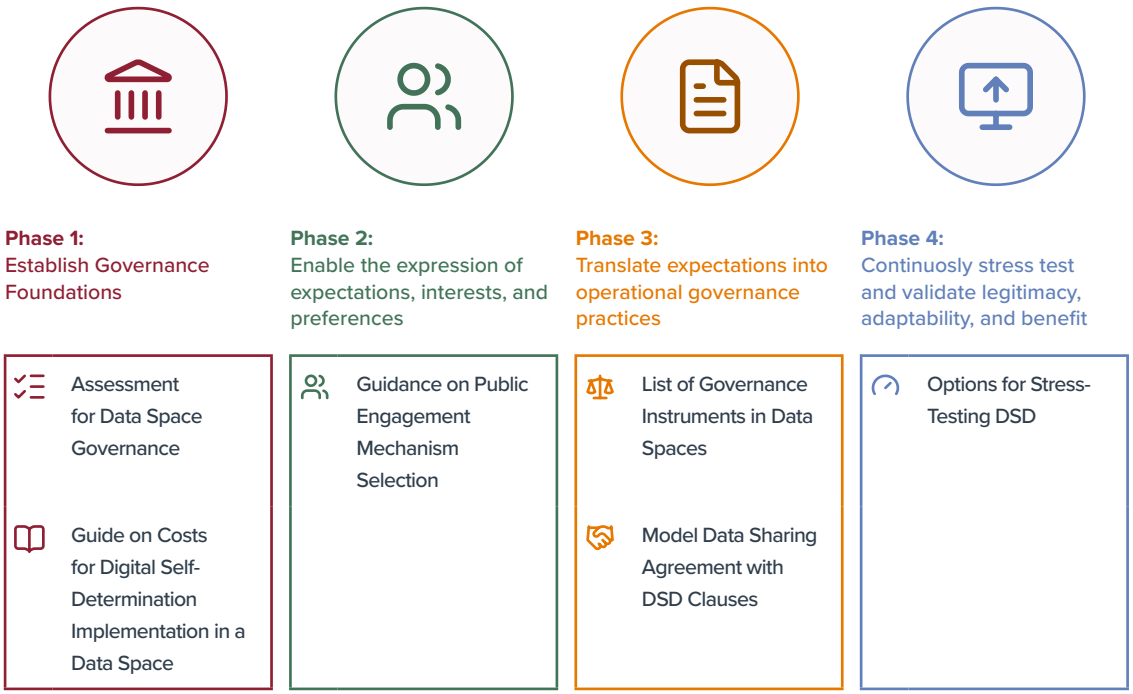
These four functions structure the roadmap that follows. Each phase focuses on one function while recognizing that they are interdependent and recur throughout the lifecycle of a data space. Following this orienting section:

- **Phase 1** addresses governance foundations;
- **Phase 2** focuses on participation and preference formation;
- **Phase 3** examines how expectations can be translated into enforceable governance instruments; and
- **Phase 4** introduces mechanisms for stress testing DSD.

The main chapters are complemented by appendices that provide detailed guidance on the tools referenced throughout the roadmap (see Figure 1):

- **Appendix I:** Assessment for Data Space Governance;
- **Appendix II:** Guidance on Costs for Digital Self-Determination Implementation in a Data Space
- **Appendix III:** Guidance on Public Engagement Mechanism Selection
- **Appendix IV:** List of Governance Instruments in Data Spaces
- **Appendix V:** Model Swiss Data Sharing Agreement with Digital Self-Determination Clauses; and
- **Appendix VI:** Options for Stress Testing DSD.

Figure 1: Roadmap for Digital Self-Determination in Data Spaces



PHASE 1

ESTABLISHING A GOVERNANCE STRUCTURE FOR THE DATA SPACE

Phase 1 lays the foundation on which every subsequent phase of this roadmap depends. Implementing DSD requires a governance structure that defines purpose, principles, authority, roles, responsibilities, decision rights, accountability mechanisms, and oversight functions. This chapter organizes that work around four governance components — Purpose, Principles, Processes, and Practices & Policies (the "4Ps") — and outlines how to:

- Clarify purposes
- Clarify principles
- Clarify the governance mandate
- Ensure representation of key actors
- Define community oversight functions
- Establish rules for transparency, escalation, and dispute resolution
- Maintain governance legitimacy over time
- Conceptualize resource and funding needs

This phase should be worked through when a data space is being designed or launched, or when DSD is being introduced into an existing one, and revisited whenever the assurance work of Phase 4 reveals weaknesses in the governance architecture. Two implementation tools support it:

Appendix I: Assessment for Data Space Governance turns this chapter's guidance into a scored assessment that practitioners (ideally together with their stakeholders) can use to evaluate governance readiness across the four components.

Appendix II: Guidance on Costs for DSD Implementation in a Data Space helps translate the resource requirements outlined in Section 1.3 into a concrete, sustainable budget.

1.1 BUILDING DIGITAL SELF-DETERMINATION INTO DATA SPACE GOVERNANCE

Governance frameworks for data spaces provide the foundation for how data is shared, accessed, and used in ways that are both effective and trustworthy. They clarify the objectives of the initiative, articulate the values that guide it, and establish the structures and practices that make those values operational. Strong governance is not only about managing risks or ensuring compliance; it is about enabling collaboration, building legitimacy, and creating systems that can adapt as circumstances and technologies evolve. This requires planning and having the resources to implement it.

Digital Self-Determination plays a central role in this work. It holds that individuals and communities should meaningfully influence how data that affects them is governed. Embedding DSD into governance ensures that data spaces function not only as technical infrastructures but also as participatory environments where rights, interests, and diverse perspectives shape decision-making. This focus on agency and accountability strengthens trust while aligning governance with broader societal goals.

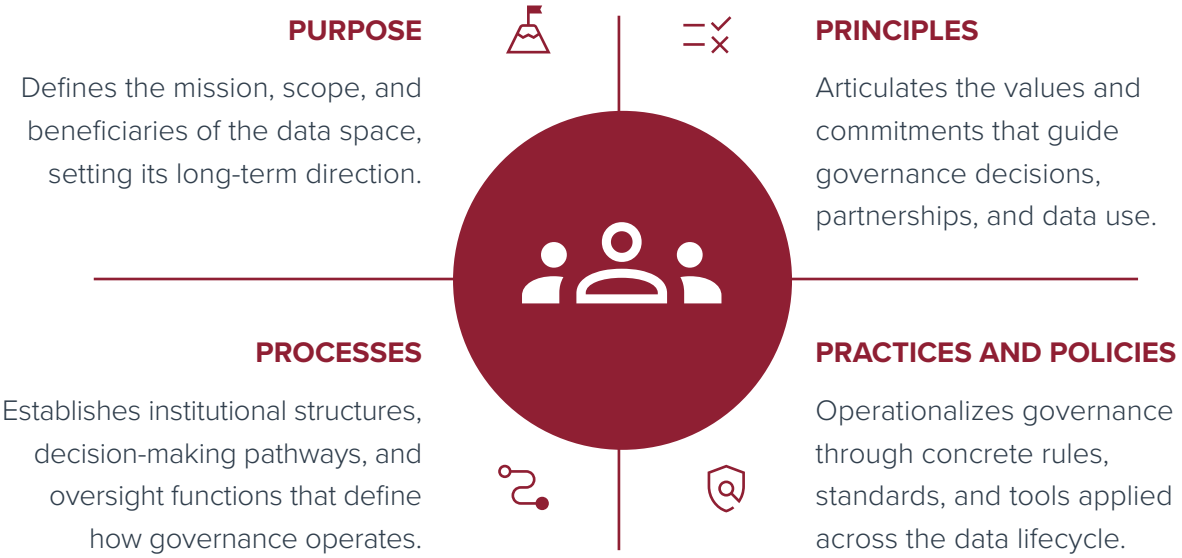
To implement DSD, data space operators must design and align four governance components:

- **Purpose** defines the mission, scope, and beneficiaries of the data space, setting its long-term direction. It explains *why* the data space exists and what collective objectives it aims to advance. A clear purpose that all stakeholders agree on fosters legitimacy, institutional alignment, and common expectations for participation and use.
- **Principles** articulate the values and commitments that should guide governance decisions, partnerships, and data use, such as transparency, accountability, fairness, and participation. Principles provide the normative foundation and can serve as a benchmark for testing and adapting governance practices over time.
- **Processes** establish the institutional structures, decision-making pathways, and oversight functions that define *how* governance operates. They determine how decisions are made, implemented, and reviewed. Strong processes translate principles into action, support stakeholder engagement, and clarify accountability.
- **Practices & Policies** operationalize governance through concrete rules, standards, and tools applied across the data lifecycle. They represent the "what" of governance, turning principles and processes into daily operations such as access rules, audit requirements, participation mechanisms, and documentation standards.

Below, we offer guidance on what each of these components are, what they entail, and how data space operators can use them to realize or incorporate DSD. A checklist at the bottom of this section summarizes the work. In ***Appendix I: Questionnaire for Data Space Governance***,

we further expand on this guidance by offering an assessment tool that data space operators can use to evaluate whether they have meaningfully realized each of the 4Ps and meaningfully embedded DSD into their operations.

Figure 2: The 4 Ps



1.2 GUIDANCE ON DSD INCORPORATION INTO DATA SPACES BASED ON THE 4PS MODEL

1. PURPOSE

Component	What it is	DSD lens
Mission and public value	The guiding goal of the data space: your “north star” and the public interest it serves.	Work with stakeholders to shape or validate the mission so people can see their interests reflected.
Scope and boundaries	What’s in and what’s out: geographies, communities, domains, data types, and activities.	Collaborate with stakeholders on what data collection and use they consider justified; document concerns and mitigations (e.g., federated access, data disposal).
Beneficiaries & Stakeholders	Who has a stake: direct participants and those affected by outcomes.	Map who supplies data, who uses it, and who is affected; check whether benefits outweigh costs and are shared fairly.

Alignment with broader goals	How the data space connects with other organizations' priorities in the same region, sector, or function.	Engage partners early; align operations to build support or surface conflicts before they harden.
Measuring success	How you'll know you're succeeding: quantitative and qualitative, short/ medium/long term.	Co-define success with the community; agree how results are shared and how to handle trade-offs.

2. PRINCIPLES

Component	What it is	DSD lens
Inclusivity & representation	Governance that reflects diverse interests, especially groups often left out.	Agree how communities want to be involved or protected; embed inequity reduction into decision pathways.
Transparency	Decisions and operations are clear and easy to explain: data processing, decision-making, and participation.	Identify what people need visibility into; agree cadence, format, and whether they prefer alerts or delegated monitoring.
Accountability	Who is responsible for what, and what happens if something goes wrong.	Center community agency via meaningful oversight and control; clarify accountability and how stakeholders can verify activities.
Effectiveness and agility	Capacity to decide and act with speed while remaining thorough where needed.	Set realistic expectations on what can be achieved and how quickly; make trade-offs and costs of speed explicit.
Durability	Ability to continue through funding gaps, leadership changes, trust issues, or conflicts of interest.	Treat durability as sustaining support; plan for relationship renewal and contingencies the community can accept.
Balance of trade-offs	How you prioritize when values conflict, resolve disputes, and clarify objectives.	Use participatory methods to map value priorities and acceptable trade-offs; if consensus fails, design a fair deliberation process.

3. PROCESSES

Component	What it is	DSD lens
Governance bodies and roles	Formal structure for strategy, day-to-day oversight, and compliance.	Create bodies that respond to community concerns (advisory, oversight, technical) and verify they match expectations.

Component	What it is	DSD lens
Decision-making framework	Standards and logic for evaluating conflicts, datasets, use cases, and partnerships.	Publish criteria; validate with affected communities and experts; revise to balance purpose, risk, and value.
Stakeholder engagement and participation	Mechanisms for regular, meaningful input and legitimacy-building.	Define “meaningful” engagement per stakeholder (risk, interest, role); agree pathways and dispute handling.
Oversight, monitoring, and evaluation	Processes to track actions, results, and consequences (internal and external).	Enumerate legal/professional/contractual duties; validate sufficiency with stakeholders; define responsible-operation indicators.
Adaptation and learning	Feedback capture, evaluation of what works, and improvement mechanisms.	Define what is tracked, who can trigger reviews (or trigger events), and how findings become changes.
Financial and operational sustainability	Funding, staffing, and institutional support that keep governance running.	Discuss funding structures and the risks they create; explain design choices and safeguards the community accepts.

4. PRACTICES AND POLICIES

Component	What it is	DSD lens
Data acquisition, inventory, and provenance	How data sources are identified, mapped, categorized, and tracked.	Structure inventories to match community expectations; label assets so they can be deleted/handled differently if expectations change.
Access and permissioning	Who can access what and under which conditions (credentials, logging, restrictions by intended use).	Align access with agreed purpose and risk tolerance; log access and support enforcement against inappropriate use.
Privacy, security, and risk management	Protecting people and systems via privacy-preserving methods, security controls, and role-based access.	Map risks by data type and severity based on consultation; define incident response and mitigation steps.
Legal and contractual frameworks	Legal context and contracts governing roles, rights, and responsibilities.	Translate legal/contract terms into clear implications; clarify expectations and how compliance is ensured.

Component	What it is	DSD lens
Interoperability and standards	Technical standards enabling data to work across systems (metadata, ontologies, APIs, federation).	Align technical design to captured community values; ensure traceability from expectations to implementation.
Capacity building and knowledge sharing	Training and documentation for stewards, users, representatives, and staff.	Tie training directly to engagement findings so stakeholders see responsiveness.
Monitoring, evaluation, and continuous improvement	Ongoing auditing and feedback loops to keep policies and practices current.	Use metrics the community understands; define how feedback changes policy and under which conditions.
Exit, archiving, and end-of-life policies	How data is archived, deleted, transitioned, or repurposed when no longer needed.	Decide end-of-life handling based on agreed purpose and risk tolerance; consult before retiring/repurposing data.

5. QUICK CHECK-UP

Purpose Mission validated; scope agreed; beneficiaries mapped; alignment checked; success metrics co-defined	**Principles** Inclusivity designed; transparency mechanisms set; accountability chain defined; agility expectations aligned; durability risks planned; trade-offs rules agreed
Processes Bodies/roles established; decision criteria published; engagement pathways active; oversight indicators running; learning loops working; funding model risk-mitigated	**Practices** Inventory/provenance auditable; access governed and logged; privacy/security controls implemented; legal instruments operationalized; standards aligned; training delivered; continuous improvement cycle active; exit plan agreed

1.3. WHAT RESOURCES ARE NEEDED TO IMPLEMENT DIGITAL SELF-DETERMINATION?

Implementing DSD requires deliberate and sustained investment. It does not add a single, discrete cost item to an otherwise unchanged data space budget. It reshapes how resources are planned, allocated, and governed across the full lifecycle of the data space.

A data space that claims to uphold DSD must be able to support participation, enforce collective

decisions, explain and correct its actions, and adapt governance as conditions change. Each of these functions carries recurring operational costs. Treating DSD as a one-off design feature or compliance exercise creates structural underfunding and undermines legitimacy over time.

To make DSD implementable and budgetable, this roadmap organizes costs around the same four governance capacities that structure the phases of implementation. These capacities are stable across domains and use cases, while allowing concrete cost differences to emerge through design choices, scale, and operating context.

1. PARTICIPATION AND PREFERENCE EXPRESSION

Resources must be allocated to mechanisms that allow individuals and affected communities to articulate expectations, boundaries, and concerns regarding data use. This includes ongoing funding for stakeholder engagement, deliberative processes, and inclusive representation. These functions are continuous operational needs, not one-off consultations.

2. TRANSLATION INTO ENFORCEABLE GOVERNANCE

DSD requires that social expectations be converted into binding rules and technical controls. This entails investment in policy development, legal instruments (such as DSD-aligned data sharing agreements), and the technical infrastructure needed to enforce governance decisions across systems. These costs connect legal, organizational, and technical domains.

3. TRANSPARENCY, CONTESTABILITY, AND REDRESS

To sustain legitimacy, a data space must be able to explain decisions, respond to challenges, and correct failures. This requires dedicated resources for logging and audit systems, human-readable explanation layers, user support and complaint handling, and remediation mechanisms. These expenditures function as accountability infrastructure.

4. ONGOING DSD ASSURANCE

DSD treats governance as adaptive rather than static. Resources are therefore required for stress testing governance arrangements, independent evaluation, performance monitoring, and the revision of rules and participation mechanisms over time. These investments ensure that governance remains aligned with evolving technologies and societal expectations.

Key Implication:

Digital Self-Determination should be understood as a long-term governance investment rather than a compliance overhead. There is no single line item that can represent DSD in its entirety. Instead, it is scattered across and built into every aspect of a project.

Without these commitments, a data space may be technically functional but politically fragile; vulnerable to loss of trust, contestation, and withdrawal of participation. With them, data spaces can achieve durable legitimacy, reduce institutional risk, and support responsible data reuse at scale.

Appendix II: Guidance on Costs for Digital Self-Determination **Implementation in a Data Space** includes additional options for assessing costs associated with a data space.

Central to DSD is a notion of control. It relates to the right of every person to freely decide how they wish to live. Exercising this right requires knowledge, the freedom to make decisions, and the ability to take action.[33] Both groups and individuals need to understand what is happening in the data space, express their preferences, and (in some cases) work with data space operators to design solutions. These digital spaces help communities participating in the data space better trust the work conducted on their behalf and it helps data spaces themselves fulfill legal and ethical requirements while eliminating the "friction" that might result if a community decides to oppose the data space.[34]

These spaces are the result of **participatory data governance**—the ways individuals, communities, and stakeholders can shape decisions about how data about or from them is accessed, shared, and reused. These approaches go beyond compliance with legal or regulatory requirements: they align data practices with the expectations, interests, and values of those affected. The resulting trust and legitimacy created by this alignment could bolster the data space's resilience by reaffirming that all parties have a shared interest in preserving it. Even if the methods used require some resources at the start, such engagements have the potential to improve focus and effectiveness long term. Organizations around the world use participatory data governance to ensure their work retains broad social support and that their work is seen as fair, beneficial, and trustworthy.

ESTABLISHING A SOCIAL LICENSE FOR DATA REUSE

One outcome of effective participatory data governance can be a **social license for data reuse**: the ongoing acceptance and approval of data activities by the relevant community. Such a social license can take many forms depending on context, risk, and institutional setting. The examples below illustrate how communities have shaped data reuse in practice. Each example emphasizes a distinct pathway through which legitimacy has been established and maintained over time.

New York City Data Assembly (The GovLab, 2020)

During the COVID-19 pandemic, The GovLab partnered with New York City public libraries to convene three remote Data Assembly mini-publics, bringing together. 55 randomly selected New Yorkers deliberated alongside policymakers, data holders, and civil rights advocates on concrete data reuse scenarios related to the pandemic. Participants articulated conditions, safeguards, and priorities for pandemic-related data use. The resulting recommendations informed a public framework for New York City's response.[35]

openSAFELY (UK NHS and partners, 2020–present)

openSAFELY is a secure health data analytics platform that enables large-scale reuse of sensitive patient data without providing researchers access to raw records. Public legitimacy was initially established through independently commissioned citizen juries during the COVID-19 pandemic and is sustained through a standing public advisory group known as the Digital Critical Friends. Ongoing workshops, regular engagement meetings and "office hours," a coding club, and extensive user support continue to shape boundaries, safeguards, oversight, and platform expansion decisions.[36]

Language Data Commons of Australia (LDaCA) (Australian Research Data Commons, 2024-)

LDaCA is a national research infrastructure initiative aimed at improving access to language data while respecting Indigenous data governance and cultural authority. The project has relied on co-design workshops and targeted consultations with Indigenous language custodians, researchers, and cultural heritage organizations to define acceptable uses, access conditions, and stewardship expectations. Planned cycles of public testing and consultation are intended to ensure the project remains responsive to community needs as they evolve.[37]

Liverpool City Region Civic Data Cooperative (University of Liverpool and LCRCA, 2023-)

The Liverpool City Region Civic Data Cooperative is a regional data stewardship initiative that connects public sector organizations, researchers, businesses, and residents to enable data reuse for health and social benefit. The Cooperative combines inclusive governance structures with ongoing public engagement, including residents' assemblies on data and AI, community conversations with equity-seeking groups, participatory research on local data hubs, and continuous patient and public involvement in health data initiatives.[38]

PHASE 2

IDENTIFYING PREFERENCES, INTERESTS, AND EXPECTATIONS

Phase 2 is about creating mechanisms that can allow for meaningful, structured engagement by a community affected by data (re)use. This work often involves:

- Stakeholder mapping and segmentation
- Participatory methodologies (e.g. forums, assemblies, surveys, deliberative processes)
- Methods for eliciting expectations, concerns, and boundaries within those methodologies
- Collective preference-formation
- Mechanisms for ensuring informed consent and refusal beyond individualized transactions.

This phase should take place once the governance structure has been created but before data collection or (re)use has started. One implementation tool can support practitioners here: Appendix III: Guidance on Public Engagement Mechanism Selection. This tool details various public engagement mechanisms and the circumstances under which they might be useful to deploy.

2.1 PARTICIPATORY DATA GOVERNANCE RANGES FROM LEVELS OF HIGH TO LOW CONTROL

There are a wide range of different participatory mechanisms that can be used to support data governance. These range from fairly low-cost engagements (using simply sharing information) to deeper commitments where authority and control are shared (see Figure 2). Each of these approaches has their own costs and benefits and can play a different role in operationalizing DSD.

Across this taxonomy, however, achieving the legitimacy promised by participatory data governance requires more than one-time or tokenistic communication. Meaningful participation requires sustained efforts to engage with stakeholders and offer them in practice the rights and responsibilities they expect. The "right" participatory engagement method will depend on the specific context, and data space operators will need to think critically about what makes sense given the circumstances they face.

2.2 DECIDING ON THE RIGHT TYPE OF PARTICIPATION: CONSIDERATIONS BEFORE STARTING

The circumstances described above are variable and difficult to define in the abstract. There is limited research specifically addressing how participatory data governance should operate within a data space. However, organizations such as the Ada Lovelace Institute,[39] OECD,[40] US Environmental Protection Agency,[41] Ostrom Workshop at Indiana University,[42] and the International Association for Public Participation[43] have developed guidance on how public-interest institutions can use participatory methods to empower communities. Several general considerations from these sources can be adapted to the context faced by Swiss data space operators.

The list below summarizes key questions to consider. Data space operators are encouraged to reflect on each point and discuss them with collaborators when determining which participatory mechanisms are appropriate.

LEVEL OF PUBLIC PARTICIPATION

Assess how much influence can be shared or delegated

Data space operators should clarify what they are prepared to open to external influence. They should consider the value that public input can provide to governance, such as identifying problems, proposing solutions, validating approaches, or expressing concerns. They should

also assess the risks of insufficient engagement, including loss of legitimacy or legal exposure. Regardless of the chosen approach, engagement should be genuine and proportionate. Outreach that is superficial, deceptive, or tokenistic can undermine trust rather than strengthen it.

PURPOSE OR GOAL

Identify the objective of the participatory activity

Operators should define the specific governance questions on which they seek input. Foundational issues concerning the purpose, direction, or societal role of the data space are likely to require more intensive engagement because they touch on core community interests. Procedural or operational matters may be suitable for lighter forms of consultation, particularly when they are more technical or limited in scope.

AUDIENCE

Map relevant stakeholders and their interests

Operators should identify who is affected by the decision or decisions under consideration. These stakeholders form the relevant audience for participation and are central to building social legitimacy. If the affected group is large or diffuse, operators may need to consider representative structures. They should also examine relationships within the community and assess whether certain groups risk exclusion or underrepresentation.

The broader legal and institutional context should also be considered. Some questions may already be shaped by existing law or contractual obligations. These constraints may influence both the scope of participation and the choice of methods.

TIME AND RESOURCES

Assess readiness, capacity, and constraints

Operators should evaluate what is feasible given available resources. Intensive engagement processes require specialized skills, sustained funding, and institutional commitment. If these are not immediately available, operators may consider what partnerships or internal support would be needed to pursue them, or whether alternative mechanisms could achieve similar objectives with fewer resources.

Timing is also important. Meaningful engagement requires preparation and coordination. Short timelines or external deadlines may limit the depth of participation that can be responsibly undertaken.

KEY CONSIDERATIONS BEFORE CHOOSING PARTICIPATORY MECHANISMS

LEVEL OF PUBLIC PARTICIPATION

Assess how much influence can be shared or delegated

- What influence are we prepared to open to external input?
- What value can public input bring to governance?
- What are the risks of insufficient engagement?

PURPOSE OR GOAL

Identify the objective of the participatory activity

- What governance questions are we seeking input on?
- Is this a foundational issue that affects core community interests?
- Is the matter procedural or operational, and more technical in scope?

AUDIENCE

Map relevant stakeholders and their interests

- Who is affected by the decision or decisions under consideration?
- Are there groups at risk of exclusion or underrepresentation?
- What legal, contractual, or institutional context shapes this question?

TIME AND RESOURCES

Assess readiness, capacity, and constraints

- Do we have the skills, funding, and commitment needed for intensive engagement?
- What partnerships or support are needed, or are alternative mechanisms appropriate?
- Do we have enough time for meaningful preparation and engagement?

2.3 A TAXONOMY FOR PARTICIPATORY DATA GOVERNANCE MECHANISMS

Below, we offer a taxonomy of participatory approaches, grouped from the lowest to the highest levels of community involvement. These mechanisms are drawn from public engagement literature, as there is little evidence of unique approaches pursued by data spaces. We suggest further research, including direct interviews with data space operators, to fill this gap.

Appendix III: Guidance on Public Engagement Mechanism Selection considers these approaches in more detail with additional details on each engagement mechanism type, the different forms they can take, and some suggestions on when they might be more or less relevant. It illustrates how different mechanisms—whether informational, consultative, deliberative, or collaborative—can be deployed to strengthen DSD and ensure that data systems evolve in line with societal values.

Participatory Data Governance Mechanism Type		What It Can Achieve for DSD
Informational		
Notices	Any written resource intended to explain a data initiative. includes brochures, fact sheets, public notes, press releases, newsletters, web sites, and social media posts.	Informing individuals of the activity being undertaken by the data space, their individual and collective rights, or the authority they can contact to further engage in the data space.
Briefings	Short presentations on a topic. Often accompanied by a brief question-and-answer period.	
Consultative		
Public Meetings	Virtual or in-person gatherings convened by a project sponsor with a broad group of stakeholders. Includes hearings, townhalls, and workshops.	Giving individuals the space to offer their perspectives, express their interests, or ask information about a data space. These are often one-off engagements and lack the depth for anything but immediate reactions or an interrogation of *why* members of a community feel a certain way.
Interviews and Focus Groups	Small one-on-one conversations or small group discussions with stakeholders about a topic.	
Surveys and Polling	Form-based tools that seek input from a set of community members on a specific set of questions. Can be used to gather qualitative responses or quantitative responses.	

Participatory Data Governance Mechanism Type		What It Can Achieve for DSD
Deliberative		
Deliberative Mini-Public	A randomly selected group of citizens who deliberate on issues and provide recommendations to inform public opinion and decision-making.	Allowing community members to validate a proposed data activity or suggest their own solutions. Deliberative engagements can allow opportunities for individuals to self-organize according to specialized needs and interests and allow for discussions around reasoning or motivation.
Digital Civic Engagement Platforms	A fusion of data-driven technologies and collective intelligence methodologies that allow community members to connect with one another, discuss issues of concern, develop collective responses to them, and (in some contexts) propose their own solutions.	
Advisory Boards	A standing group made up of community members who are regularly solicited to provide comments and advice on a project.	
Collaborative		
Collaborative Innovation and Co-Creation	An engagement with a diverse yet carefully selected group of stakeholders to design policies and programs. These groups are specifically chosen for their expertise or interest in particular areas. Common kinds of collaborative innovation methodologies are hackathons, idea “boot camps”, and various competitions.	Ceding formal power and authority to community members to develop solutions to challenges facing the data space. Collaborative mechanisms can offer the deepest realization of DSD—with group members necessarily needing to sort through their individual and collective interests, needs and expectations—but may be time consuming.
Oversight Committees	An institution empowered to oversee a project or organization and review its conduct. Committees may be empowered to conduct audits, manage service evaluation and redress mechanisms, make decisions on budgeting, and take other actions.	

PHASE 3

TRANSLATING EXPECTATIONS INTO GOVERNANCE PRACTICES

Phase 3 describes how the preferences solicited from a community previously can be translated into binding, enforceable, and reviewable policies and processes. This work involves:

- Stakeholder mapping and segmentation
- Translating expressed expectations into formal governance decisions
- Embedding those decisions into legal, organizational, and technical instruments
- Operationalizing consent, refusal, and conditions of use within governance frameworks
- Aligning contracts, policies, and system design with participatory outcomes

This phase should be done after engaging with community members to understand their preferences. It may be done after an initial engagement or between a series of engagements during which time these mechanisms are further developed, refined, and validated. It is supported by two tools:

Appendix IV: List of Governance Instruments in Data Spaces provides an overview of the legal, organizational, technical, and procedural instruments that can be used to translate participatory outcomes and governance decisions into operational practice.

Appendix V: Model Swiss Data Sharing Agreement with Digital Self-Determination Clauses provides a concrete example of how DSD-related rights, responsibilities, safeguards, and review mechanisms can be incorporated into a data sharing agreement .

Participation has governance value through how it shapes rules, contracts, and systems. The central task of Phase 3 is therefore translation: turning societal, individual, and collective expectations into governance practices that (co-)determine how data is accessed, shared, reused, and overseen across its lifecycle. Without this translation layer, participation often remains symbolic, and expressed expectations may lack enforceability and institutional traction.

Within a DSD framework, a data space relies on **a set of governance instruments** to perform this translation. These include legal agreements, organizational rules, technical controls, and oversight arrangements that together determine what data uses are permitted, under which conditions, and with what responsibilities and safeguards. Through these instruments, participatory inputs could be rendered binding and operational, anchoring expressed values and concerns in concrete artefacts that guide day-to-day decisions and system behavior.

3.1 EXPECTATIONS EMERGING FROM PARTICIPATION

Participatory and deliberative processes surface a wide range of preferences, concerns, and boundary conditions. These inputs are rarely articulated as ready-made governance requirements. More often, they are qualitative, contextual, and grounded in lived experience.

Themes raised through participation may include:

- acceptable purposes for data access and reuse;
- conditions under which consent should be requested, limited, withdrawn, or renewed;
- expectations for transparency, explanation, and traceability;
- safeguards against misuse, discrimination, or unintended impacts; and
- expectations of reciprocity, benefit-sharing, or avenues for redress.

For data space operators, the challenge lies not only in collecting these inputs, but in determining how they inform decisions that shape governance in practice. Without explicit translation into rules, contracts, and systems, participatory outcomes often remain disconnected from operational reality.

3.2 GOVERNANCE INSTRUMENTS AS TRANSLATION MECHANISMS

The documents and mechanisms that we call governance instruments provide the means through which expectations are encoded into practice. These instruments are not originally designed with DSD in mind and vary widely in scope, flexibility, and enforceability. Nevertheless, they constitute the primary levers available to data space operators for turning participatory input into binding outcomes.

This roadmap builds on instruments already in use across the Swiss data ecosystem. A detailed inventory is provided in Appendix IV: Governance Instruments in Swiss Data Spaces, which catalogs the legal, organizational, and technical tools available to data space operators.

For the purposes of Phase 3, these instruments can be grouped into six functional categories:

- **Foundational governance and participation instruments**, such as rulebooks, statutes, and accession agreements, which establish participation rights, decision-making authority, and accountability structures.
- **Contractual mechanisms**, including general terms and conditions, data sharing agreements, and licensing arrangements, which give legal force to governance decisions in specific data sharing contexts.
- **Policies, standards, and shared language**, such as codes of conduct, internal policies, standards, and glossaries, which stabilize shared expectations and support consistent interpretation across actors.
- **Technology and governance by design**, which embeds governance rules into system behavior through access controls, consent management, logging, auditability, and privacy-enhancing technologies
- **Trust, oversight, and compliance mechanisms**, including stewardship roles, audits, procurement requirements, and monitoring arrangements, which verify adherence and support correction over time.
- **Training and cultural change mechanisms,** which build the skills, literacy, and organizational norms required for governance instruments to function as intended.

3.3 CONSENT WITHIN A BROADER GOVERNANCE FRAMEWORK

Consent remains the key governance mechanism for data under Swiss data protection law. Within a DSD framework, however, it operates as part of a broader institutional arrangement instead of as a standalone transaction.

In practice, consent in data spaces can be shaped and constrained by surrounding governance instruments. Rulebooks, contractual terms, technical systems, and oversight processes can define when consent is required, what it covers, how it can be withdrawn, and how changes in context are handled. Consent can thus function within an institutional setting that structures choice and determines its practical consequences.

This means that:

- consent options (opt-in, opt-out, withdrawal, or renewal) are specified through governance documents and contractual clauses;
- changes in purpose, risk, or context trigger governance decisions that may require renewed consent or additional safeguards;
- collective expectations can shape when consent is requested, limited, or deemed insufficient on its own; and
- technical systems support enforcement, revocation, logging, and traceability of consent-related decisions.

Consent is therefore one mechanism among several through which expectations are translated into practice. Its legitimacy depends on how well it is embedded within governance arrangements that remain responsive as data uses, risks, and expectations evolve. Fully realizing this model alongside existing legal frameworks may require further legal and policy development.

3.4 MAPPING EXPECTATIONS TO INSTRUMENTS

The table below provides an overview of governance instruments commonly used in data spaces and the roles they can play in translating participatory input into practice. It illustrates how different instruments could be used to embed expressed expectations into binding governance decisions across legal, organizational, and technical layers, and where leverage exists to strengthen alignment with Digital Self-Determination.

Each row describes:

- The governance function of a given instrument, and
- potential leverage points for strengthening DSD alignment.

The table serves as a navigation aid for data space operators, governance authorities, and policymakers. When participatory processes surface concerns or priorities, it can help identify which instruments are relevant, where responsibility lies, and which levers can be adapted or combined. Many governance challenges require coordinated use of multiple instruments.

Governance instruments operate at different layers of a data space. Foundational instruments establish authority and accountability. Contractual instruments give legal force to conditions of access and use. Policies, standards, and shared language guide interpretation and consistency. Technical and governance-by-design mechanisms enforce rules in system behavior. Oversight, stewardship, audit, and training arrangements provide assurance and enable adaptation over time.

Within the Swiss data ecosystem, deployment of these instruments varies considerably. Some, such as the Code of Conduct for Trustworthy Data Spaces, already exist at the national level. Others are under development or not yet implemented at the level of individual data spaces. The table should therefore be read as a menu of governance levers rather than a prescriptive sequence, allowing operators to prioritize based on context, capacity, and policy objectives.

The instruments summarized here are described in greater detail in Appendix IV.

Note: While the table highlights data sharing agreements alongside other contractual instruments, their central role in governing data access and reuse warrants dedicated attention. The section following it therefore examines data sharing agreements in more detail.

Governance Instrument	Governance Function	DSD Leverage Points
Rulebook	Defines participation rules, roles, decision rights, interoperability obligations, and accountability structures	Co-create clauses with affected stakeholders; embed feedback loops for periodic revision
Statutes / Articles of Association	Establish legal mandate, governance bodies, membership structure, and allocation of powers	Reserve seats for public representatives; require periodic participatory review
Membership / Accession Agreement	Formalizes entry conditions and acceptance of governance obligations	Include explicit DSD commitments; link renewal to governance review
General Terms & Conditions (GTCs)	Set baseline rights, obligations, withdrawal procedures, and dispute mechanisms	Make access, portability, withdrawal, and complaint rights explicit
Data Sharing Agreements (DSAs)	Define enforceable terms for data exchange, purpose limitation, safeguards, and accountability	Use standardized templates; encode purpose limitation and consent signaling
Licensing	Use time-limited or conditional licenses; require machine-readable terms	Use time-limited or conditional licenses; require machine-readable terms
Policies & Guidelines	Translate principles into operational rules for data lifecycle decisions	Require DSD alignment review for new initiatives
Code of Conduct for Trustworthy Data Spaces	Articulate shared behavioral norms beyond legal minimums	Link reporting to participatory feedback; enable public monitoring of adherence
Standards and Vocabulary	Standardize protocols, metadata, and usage conditions to enable interoperability and consistency	Require machine-readable access conditions and provenance metadata
Glossary	Define shared terminology to support consistent interpretation across actors	Maintain a living glossary updated through stakeholder input

Governance Instrument	Governance Function	DSD Leverage Points
Technology & Governance by Design	Embed rules in system architecture through access controls, logging, consent management, and PETs	Apply privacy- and governance-by-design defaults; regularly update technical controls
Data Network Description	Document technical and organizational data flows and control points	Publish clear flow descriptions identifying responsible actors
Interoperability Specifications	Define secure exchange standards enabling portability and traceability	Standardize APIs for consent withdrawal and cross-domain portability
Data Stewardship & Institutional Arrangements	Assign responsibility for data quality, coordination, and compliance	Strengthen steward mandates; coordinate roles across domains
Audit & Compliance Mechanisms	Verify adherence through monitoring, logging, and review	Introduce DSD-focused audits; feed findings into governance updates
Procurement & Vendor Management	Extend governance requirements to external providers	Include DSD clauses in contracts; require audit and portability provisions
Training & Cultural Change	Build literacy and skills to exercise governance roles effectively	Embed DSD in training programs; support peer learning networks

3.5 DATA SHARING AGREEMENTS AS A CORE TRANSLATION MECHANISM

Contractual frameworks operate at multiple levels within a data space. Participation agreements and general terms bind members to shared rules and obligations. Use-case agreements govern access conditions for defined purposes. Transaction-level agreements regulate individual accesses or data products. Together, these layers allow data space operators to align overarching governance decisions with concrete data access arrangements, while maintaining flexibility across contexts.[44]

Within a Digital Self-Determination approach, data sharing agreements (DSA) are one of the primary governance instruments, giving legal force to expectations emerging from participation, oversight bodies, and other forms of collective input across the data lifecycle. Standard templates can reduce transaction costs and support scalability, but they do not

automatically reflect collective expectations, evolving social license, or the need for governance to remain legitimate as uses and risks change. A DSD-oriented approach should therefore treat DSAs as living governance instruments that can be revisited as uses, risks, and expectations evolve.

Participatory processes rarely feed directly into contractual drafting today. Yet many expectations raised through participation concern issues that data sharing agreements already regulate in practice: why data is shared and which outcomes are considered legitimate; which uses are acceptable over time; how risks and responsibilities are allocated; how authorization or consent is signaled and enforced; and how misuse, harm, and disagreement are addressed. This makes DSAs a practical leverage point for translating participatory outcomes into binding commitments, despite that translation not yet being common practice.

Building on the Contractual Wheel of Data Collaboration and existing Swiss templates, a DSD-aligned data sharing agreement should make explicit how it addresses recurring governance dimensions.[45]

- **Purpose (WHY):** The agreement should articulate the purpose of data sharing and link permitted uses to that purpose, including how changes in purpose are handled and who has authority to decide.
- **Data scope and boundaries (WHAT):** The agreement should define what data, data products, and relevant metadata are covered (and excluded), including how derived data and outputs are treated, and the boundaries that apply to reuse over time.
- **Control and conditions of use (HOW):** Conditions for access, reuse, redistribution, and derivation should reflect proportionality, safeguards, and relevant individual and collective expectations.
- **Agency and authorization signaling (HOW)**: Where consent or other forms of authorization are required, the agreement should clarify how they are obtained, renewed, limited, or withdrawn, and how these signals are enforced technically and organizationally.
- **Accountability and oversight (WHO)**: Responsibilities for compliance, monitoring, audit, and redress should be clearly assigned, including escalation paths in cases of breach.
- **Reciprocity and benefit (cross-cutting)**: Where relevant, agreements should reflect expectations around benefit-sharing, attribution, feedback, or access to results, particularly in public-interest data spaces.
- **Adaptation over time (WHEN)**: The agreement should include mechanisms for review, amendment, or termination that allow governance to evolve as contexts, risks, and expectations change.
- **Context and perimeter (WHERE):** The agreement should clarify the practical and legal perimeter of the arrangement (where data is accessed/used and under which

applicable requirements), including how cross-boundary sharing or downstream recipients are handled and how disputes are addressed.

This roadmap supports the use of DSD-aligned DSAs by building on existing Swiss templates developed under the mandate of the Federal Council and the Swiss Federal Institute of Intellectual Property (IPI). These templates already address practical barriers to data sharing, including legal certainty and interoperability. In Appendix V: Model Swiss Data Sharing Agreement with Digital Self-Determination Clauses, the roadmap presents an annotated version of the existing IPI *Subscription Agreement for Access to Technical Data*, illustrating how DSD considerations can be integrated into an established Swiss template through targeted clauses addressing purpose limitation, transparency, accountability, and adaptation over time.

Although the appendix focuses on a unilateral subscription agreement, the same approach can be applied to the other two types of agreements developed by the IPI, namely those governing data exchange or data transfer, as well as to sector-specific arrangements within individual data spaces. The aim is not to introduce entirely new contractual forms, but to demonstrate how existing templates can be adapted to better reflect governance decisions and participatory expectations.[46]

For data space operators, this implies treating DSAs as living governance instruments rather than static legal artefacts. In practice, this could involve reviewing agreements alongside governance decisions and participatory outputs, using standardized templates while retaining room for adaptation, aligning contractual terms with rulebooks, technical controls, and oversight mechanisms, and revisiting agreements as part of broader governance reviews or evaluation processes.

PHASE 4

ONGOING DIGITAL SELF-DETERMINATION ASSURANCE

Phase 4 emphasizes ongoing assurance of DSD as a core responsibility of data space operators. Digital Self-Determination cannot be assumed to last indefinitely; it depends on the effectiveness of governance arrangements, controls, and decision-making practices over time as data uses and risks evolve.

The purpose of Phase 4 is to assess whether the conditions that support DSD continue to hold, and whether the data space continues to merit trust as a result. It introduces:

- Continuous assurance as a routine governance function;
- Stress testing as a method for examining how DSD-relevant arrangements perform under challenging conditions;
- Pathways for translating evaluation findings into governance, contractual, and technical adjustments; and
- Ways of demonstrating, through evidence, that DSD commitments are upheld in practice.

As the phases are iterative, findings from phase 4 can lead to updates in earlier ones. Re-running the assessment provided in Appendix I is a practical approach for this review. Additional guidance can also be found in Appendix VI: Options for Stress Testing DSD.

Data spaces operate in dynamic environments. Data is reused across contexts, combined with new sources, and processed through increasingly complex analytical and AI-enabled systems. Governance responsibilities are distributed across multiple organizations, and decisions taken at one stage can have consequences well beyond their original scope.

Under these conditions, static measures are insufficient. One-time consent, initial certification, or upfront compliance checks do not adequately account for new forms of reuse, emerging risks, or shifting expectations. Governance arrangements that initially support agency and control may weaken if they are not periodically examined and adjusted.[47]

Continuous assurance provides a way for data space operators to check whether participants retain meaningful control, whether governance mechanisms still function as intended, and whether safeguards remain adequate as practices evolve. It supports learning and adaptation within governance structures, rather than assuming that alignment with DSD persists automatically.

4.1 EVALUATING DIGITAL SELF-DETERMINATION THROUGH CORE GOVERNANCE PRINCIPLES

Throughout this roadmap, Digital Self-Determination is treated as a normative governance principle in its own right, centered on agency, legitimacy, and accountability. For the purposes of evaluation, however, DSD must be assessed through observable properties of how a data space operates in practice.

Swiss policy guidance on trustworthy data spaces identifies four principles that characterize governance arrangements capable of sustaining trust over time.[48] These principles do not replace DSD. Instead, they provide operational lenses through which the functioning of DSD can be evaluated. Each captures a distinct aspect of whether agency is supported in practice, rather than only in formal design.

For this reason, Phase 4 uses the following four principles as evaluation anchors:

- **Effectiveness**: Governance arrangements must remain capable of responding to changing conditions. This includes the ability to adjust rules, procedures, and technical controls as data uses, risks, and participants change.
- **Fairness**: Data access and use must be governed in ways that avoid discrimination, balance competing interests, and apply safeguards proportionately. This includes attention to data quality, non-discrimination, and the treatment of vulnerable groups.
- **Control**: Participants must retain meaningful control over whether and how their data is used. This includes mechanisms for authorization, consent or refusal, security, and control over onward transfer or reuse.

- **Transparency**: Governance depends on intelligibility. Participants and affected parties must be able to understand how data is used, for what purposes, by whom, and under which conditions. Transparency supports oversight, accountability, and the exercise of agency.

These principles make it possible to examine whether a data space continues to support DSD in practice, and whether reliance on its governance remains justified.

4.2 STRESS TESTING DIGITAL SELF-DETERMINATION AS A GOVERNANCE PRACTICE

This roadmap proposes stress testing as one method for evaluating how DSD holds under demanding conditions. Stress testing examines governance arrangements and system behavior in scenarios that may strain agency, control, or legitimacy.[49]

Scenario-based tests may focus on situations such as expanded data reuse beyond original purposes, coordination failures across organizations, security incidents, disputes over authorization or withdrawal, or breakdowns in transparency and communication. The aim is to assess whether existing rules, roles, and technical controls continue to operate as intended when conditions deviate from the norm.

Within a data space, stress testing serves three functions:

- revealing weaknesses in governance, coordination, or system design that affect agency and control;
- informing targeted adjustments to rules, contracts, technical architecture, or oversight arrangements; and
- providing evidence that risks are anticipated and governed through established processes.

Stress testing can be most effective when embedded in routine governance practice. Tests can be conducted during design phases, major system changes, and periodic governance reviews. Each test targets specific components of the data space that have direct implications for DSD, such as access control, consent and preference management, data linkage, decision-making authority, oversight processes, or cross-organizational coordination. Findings should feed directly into rulebooks, contractual terms, system configurations, and review procedures.

Through this process, evaluation supports governance that remains responsive as data spaces evolve, reinforcing the conditions under which Digital Self-Determination can be exercised over time.

Appendix VI, Options for Stress Testing Digital Self-Determination, presents a set of illustrative methods organized around the principles of effectiveness, fairness, control, and transparency. These methods complement audits, certifications, and monitoring practices already used in data spaces. They are intended to be adapted to sectoral, legal, and organizational contexts, not applied as fixed or exhaustive requirements.

IV. Conclusion

Through this research, we have examined the concept of digital self-determination and its relevance to the governance of the Swiss data ecosystem. We have also outlined a roadmap that translates digital self-determination from an abstract principle into an operational governance framework. In closing, we highlight three central ideas for data space operators:

Digital Self-Determination Can Accommodate Modern Data Needs: Digital self-determination offers a governance approach suited to contemporary data environments. Traditional models rely heavily on static consent developed for a context of limited and predictable data collection and use. Today's decentralized and interconnected systems depend on combining data from multiple sources and reusing it beyond its original purpose. Digital self-determination addresses structural governance challenges that arise in this environment, including the burden placed on individuals, information asymmetries and opacity, the limits of one-off authorization, constrained choices, individualized risk framing, compliance treated as a substitute for trust, and gaps in governance capacity.

Digital Self-Determination Requires Operationalization: Digital self-determination has often been framed as an aspirational ideal. In practice, however, trust in complex data ecosystems depends on credible governance structures. As datasets are combined, linked, and repurposed, risks evolve and governance must adapt accordingly. Data space operators should examine whether their purpose, principles, processes, and practices provide tangible mechanisms for agency, accountability, and oversight. Without operational grounding, commitments to self-determination remain rhetorical.

Digital Self-Determination Aligns with the Interests of Data Space Operators: Digital self-determination is closely aligned with Switzerland's data strategy, which emphasizes coordinated but decentralized data spaces consistent with the country's federal structure. It addresses a central governance question: how decisions about data access, use, and reuse are made, justified, and revised over time. It complements legal compliance and technical interoperability by focusing on legitimacy, trust, and agency in practice. For individuals and communities, it clarifies how their interests are considered. For data space operators, it strengthens governance in complex, long-term initiatives without imposing a rigid model or displacing existing responsibilities.

To operationalize digital self-determination, data space operators should integrate it into core decision-making rather than treat it as an add-on. It should shape foundational aspects of how a data space defines its purpose and interacts with stakeholders. The phased approach presented in this roadmap provides one way to do so:

- **Establishing a Governance Structure for a Data Space:** Ensuring that community stakeholders are central in how a data space defines its purpose, principles, processes, and practices and policies.
- **Identifying Preferences, Interests and Expectations:** Deploying appropriate mechanisms that can be used to reach relevant stakeholders and maintain informed engagement.
- **Translating Expectations into Governance Practices:** Using legal instruments, codes of conduct, and other governance documents to convert community input into binding and operational commitments.
- **Ongoing DSD Assurance:** Assessing over time whether operations continue to reflect digital self-determination in practice.

We hope this guidance contributes to efforts to foster data-driven innovation while safeguarding the rights and interests of communities. Institutionalizing digital self-determination offers data space operators a pathway to strengthen legitimacy, address structural inequities, and support responsible data reuse over the long term.

APPENDIX I

Assessment for Data Space Governance

This assessment has been developed as a practical tool to support the design of governance arrangements for data spaces. It is structured around four interconnected pillars:

- **Purpose** defines the mission, scope, and beneficiaries of the data space, setting its long-term direction.
- **Principles** articulate the normative commitments and values (including transparency, accountability, and DSD) that should guide governance.
- **Processes** establish the institutional structures, decision-making mechanisms, and oversight functions needed to enact governance.
- **Practices & Policies** operationalize governance through concrete rules, standards, and tools across the data lifecycle.

Together, these pillars guide stakeholders through the key questions of governance: why the data space exists, what values underpin it, how decisions are made, and what operational rules are required to make it work in practice.

The questions are not intended to prescribe a single model. Instead, they are designed to support structured discussions and self-evaluation to help align diverse stakeholders to consider what they have done to incorporate digital self-determination into data space governance. Used in workshops, consultations, or internal planning, they can help ensure that governance frameworks are transparent, inclusive, and durable—and that they uphold digital self-determination as a core commitment.

ASSESSMENT

This assessment includes **72 questions**—14 for purpose, 18 for principles, 18 for processes, and 22 for practices and policies. The minimum point total is 72 and the maximum point total is 216.

To calculate their score, data space operators should go through the assessment, responding to the questions, writing down their score for each section. At the end, they should go back and add their total score together. A rubric below offers general guidance on how to interpret the total score, but data space operators may also find it useful to look at the category with the lowest score as an indicator of the kinds of governance issues they may want to specifically address.

RUBRIC

Point Total	Description
172–216 points (>80%)	The data space has strongly embedded digital self-determination across all four categories. There are multiple avenues by which community members and other stakeholders can make their interests known and see it acted upon. Barring other circumstances, the data space is likely to align with local needs and build trust across the community.
107–215 points (>50%)	The data space has taken some efforts to embed digital self-determination into governance—but there may be some gaps or limits to this work. Operators may have only focused on one or two aspects of governance or put limits on the degree to which public input informs activities. The data space may foster some amount of trust but more work needs to be done to ensure alignment with local interests and expectations.
70–106 points (<49.9%)	The data space may want to more seriously integrate digital self-determination into governance. Efforts to embed local needs may be lacking across all four categories. There may be a lack of knowledge of how the data space supports the community's interests or considers their perspective. The data space may have difficulty securing and sustaining high levels of trust.

1. PURPOSE

Objectives of the Data Space

The purpose section should help stakeholders clearly define **why the data space exists** and what collective objectives it aims to serve. This establishes legitimacy, alignment, and shared expectations.

GUIDING QUESTIONS

MISSION & PUBLIC VALUE

What overarching societal or sectoral challenges does this data space address?

- ☐ **3 Points:** There is a clear overarching societal or sectoral challenge that the data space addresses.
- ☐ **2 Points:** The data space only indirectly addresses some societal or sectoral challenge or there is a lack of consensus.
- ☐ **1 Point:** The data space has little to no relevance to a societal or sectoral challenge.

Does the intended goal of the data space align with some community priority or provide some other material support to community members?

- ☐ **3 Points:** The intended goal of the data space clearly aligns with the community's priorities or, if not, provides some tangible support to community members.
- ☐ **2 Points:** The intended goal of the data space aligns with the priorities of only some members in the community or offers some other support that is not universally valued.
- ☐ **1 Point:** The intended goal of the data space is unrelated to or directly at odds with the priorities of community members. Any support offered is irrelevant or has no value for the community.

SCOPE & BOUNDARIES

Does the community understand the proposed data lifecycle in its entirety (e.g. from the type of data that will be collected to how it will be used)?

- ☐ **3 Points:** The community understands the proposed data lifecycle in its entirety because information on the data has been delivered in a format and style it can understand.
- ☐ **2 Points:** While information is not broadly accessible, community members with specialized knowledge or a position of authority can understand the data lifecycle in its entirety.
- ☐ **1 Point:** Information on the data lifecycle is either unavailable or incomplete. It is not possible for any member of the community to meaningfully understand the data use.

Are there objections regarding any data types, analytic techniques, or applications? Are these absolute or can a data application be in any way justified?

- ☐ **3 Points:** If there are objections regarding any data types, analytic techniques, or applications, that element has been excluded from the data space or the community has agreed on a mitigating factor that can justify its inclusion.
- ☐ **2 Points:** If there are objections regarding any data types, analytic techniques, or applications, that element has been noted. The data space operators have tried to justify their decision in a clear and credible way, even if this justification is not broadly accepted.
- ☐ **1 Point:** The data space operator has either not sought to understand community objections or it has not tried to credibly justify its own decision-making to external parties.

What geographies, communities, or domains does the data space cover?

- ☐ **3 Points:** The data space operators have definitively outlined the geographies, communities, and domains that the data space covers.
- ☐ **2 Points:** The data space operators have offered general guidance on the geographies, communities, and domains that the data space covers but there remain some ambiguities in overall focus or direction.
- ☐ **1 Point:** Little to no attempt has been made to define the boundaries of the data space. The scope is vague, with a high potential for mission creep.

BENEFICIARIES & STAKEHOLDERS

Who are the intended direct beneficiaries and who may be indirectly impacted by data space activities?

- ☐ **3 Points:** The data space has identified intended direct beneficiaries and who also may be indirectly impacted by data space activities. It has ensured that the data space does not widen any disparities or exacerbate inexisting inequities.
- ☐ **2 Points:** The data space has identified intended direct beneficiaries but has not examined larger consequences or any indirect impacts. There has been limited work done to understand how benefits may impact the relationships between beneficiaries.
- ☐ **1 Point:** The data space has not identified any beneficiaries beyond the involved stakeholders. It cannot clearly identify the consequences of its activities nor whether the data space will exacerbate inequities.

Do these stakeholders see sufficient value in their involvement and, if not, what do they still need?

- ☐ **3 Points:** All stakeholders see sufficient value or a need met by their involvement in the data space, one that will sustain their involvement long-term.
- ☐ **2 Points:** Most stakeholders can connect their interests to the data space's success or there is sufficient political will (or other incentive) to motivate involvement in the short term.
- ☐ **1 Point:** The data space relies on the good will of stakeholders and there is little guarantee of sustained support in the long term.

How do stakeholders understand their relationship with one another? Do they see the data space as impacting them equitably?

- ☐ **3 Points:** Stakeholders understand who else is participating in the data space and their relationships to one another. They have no concerns about these other parties and see no equity, ethics, or conflict of interest concerns.
- ☐ **2 Points:** Stakeholders understand who else is participating in the data space even if the exact role or relationship is nebulous. There may be some concerns about certain participants that have not been fully addressed.
- ☐ **1 Point:** Stakeholders do not have full visibility on other data space participants or have serious objections to the involvement of certain parties that have not been addressed.

ALIGNMENT WITH BROADER GOALS

What goals are other institutions pursuing and to what extent does the data space align with these goals?

- ☐ **3 Points:** The goals of other institutions in the domain space or sector align with the goals of the data space.
- ☐ **2 Points:** The goals of the data space do not align with the interests of other institutions but they are not operating in competition or tension.
- ☐ **1 Point:** The goal of the data space is in tension with the goal of other institutions in the domain or sector.

Do the community and other stakeholders consider these other goals a priority?

- ☐ **3 Points:** The goal that the data space seeks to accomplish is highly salient within the community or among relevant stakeholders. It is considered a priority issue to be addressed.
- ☐ **2 Points:** The data space achieves a goal that some community members and stakeholders value, even if they have other interests that take higher precedence.
- ☐ **1 Point:** The data space addresses an issue or challenge that most stakeholders and community members see as unimportant or in direct opposition to higher priority interests.

Are the relationships between these goals clear and explicable to others?

- ☐ **3 Points:** The data space operators have clearly explained their goals and how these relate to other goals in the community of interest. This explanation is clear, concise, and easily accessible.
- ☐ **2 Points:** The data space operators have explained their goals but the information is not universally understandable because it is not in a format that is clear, concise, or easily accessible.
- ☐ **1 Point:** The data space operators have declined to communicate how their goals relate to others. Efforts to engage with other interests are tokenistic.

MEASURING SUCCESS

What short-, medium-, and long-term outcomes might result from the data space that the community considers important to justify the (re-)use?

- ☐ **3 Points:** The data space operators have clearly identified a set of short-, medium-, and long-term outcomes that align with what the community considers important to justify the (re-)use.
- ☐ **2 Points:** The data space operators have identified some short-, medium-, and long-term outcomes, but the set is incomplete, weakly linked to community priorities, or not sufficiently specific to justify (re-)use.
- ☐ **1 Point:** The data space operators have not articulated meaningful outcomes, or outcomes are disconnected from what the community considers important to justify (re-)use.

How does the community want this information communicated to ensure accountability?

- ☐ **3 Points:**These goals have been communicated in a format that the community prefers and in a language it can readily understand so as to ensure accountability.
- ☐ **2 Points:** The data space operators have communicated goals and outcomes, but the format, timing, or accessibility is uneven, limiting accountability for most community members.
- ☐ **1 Point:** Goals and outcomes are not communicated in an accessible way, leaving the community unable to track progress or hold operators accountable.

How do stakeholders evaluate trade-offs between competing interests? Are there any interests that supersede all others?

- ☐ **3 Points:** The data space operators understand how stakeholders and the community of interest evaluate trade-offs between interests. There is a clear prioritization of what to pursue if there is a conflict between two intended objectives.
- ☐ **2 Points:** The data space operators have some understanding of trade-offs, but prioritization is informal, contested, or not clearly documented when conflicts arise.
- ☐ **1 Point:** Trade-offs are handled ad hoc or implicitly; stakeholders cannot explain how conflicts are resolved or what interests supersede others.

SCORE TOTAL: PURPOSE: _____ of 42 TOTAL

2. PRINCIPLES

Guiding Values for the Data Space

Principles articulate the **normative foundation** of the data space and foster **trust** within a data space arrangement. They define what values and commitments will guide governance choices, partnerships, and data use. They also serve as benchmarks against which practices and processes can be tested and adapted.

GUIDING QUESTIONS

INCLUSIVITY AND REPRESENTATION

How does the community want to preserve its control in data governance?

- ☐ **3 Points:** The community has been meaningfully solicited and there are clear mechanisms to preserve its control in data governance.
- ☐ **2 Points:** Community input has been sought and some concrete arrangements exist to preserve influence, but key elements are incomplete or uneven (e.g., accessibility of channels, enforceability, clarity of representation/mandate, or demonstrable impact on decisions).
- ☐ **1 Point:** Community control is largely absent or informal; representation is unclear; participation relies on ad hoc engagement with limited visibility, limited influence on decisions, and no reliable way to preserve control as uses and risks evolve.

What degree of importance does it assign this work and its involvement in it?

- ☐ **3 Points:** These mechanisms reflect the level of importance that the community itself assigns to the work and its involvement in the data space.
- ☐ **2 Points:** Mechanisms exist, but they only partly reflect the level of importance the community assigns: involvement is under-scoped or inconsistent (e.g., consultation is periodic rather than continuous, representation/mandates are unclear, feedback is collected but not systematically responded to, participation is not resourced, or there is limited evidence that community input changes priorities, rules, or decisions).
- ☐ **1 Point:** Mechanisms do not reflect the level of importance the community assigns: involvement is minimal, symbolic, or ad hoc (e.g., one-off engagement, no defined channels or representation, no records of input or responses, no decision checkpoints requiring community input, no resourcing/ownership), and there is no credible evidence that community priorities shape governance outcomes over time.

Are there any relevant groups at risk of exclusion, underrepresentation, or marginalization? What specialized engagement is needed to reach them and represent their interests?

- ☐ **3 Points:** If there are any groups at risk of exclusion, underrepresentation, or marginalization, these groups have been identified and there are dedicated mechanisms to reaching them and preserving their interests.
- ☐ **2 Points**: Some groups at risk of exclusion, underrepresentation, or marginalization have been identified and there are some targeted steps to reach them, but the approach is incomplete or uneven (e.g., engagement is occasional rather than sustained, outreach relies on generic channels, representation is informal, dedicated capacity/resources are limited, or there is limited evidence that their input is reflected in governance decisions).
- ☐ **1 Point**: Groups at risk of exclusion, underrepresentation, or marginalization have not been identified, or identification is superficial, and there are no dedicated mechanisms to reach them or preserve their interests.

TRANSPARENCY AND COMMUNICATION

What do community members view as important when it comes to day-to-day and strategic operations of the data space (e.g. data provenance, access rights, governance decisions)?

- ☐ **3 Points:** Community priorities are elicited and documented, translated into governance requirements, and embedded into operations and strategic decision-making, with ongoing feedback/contestation and periodic updates as uses/risks evolve.
- ☐ **2 Points:** Some priorities are identified and reflected in practice, but coverage is partial (day-to-day vs strategic), enforcement/visibility is uneven, or feedback does not reliably change decisions.
- ☐ **1 Point:** Priorities are not identified or remain informal; operations and decisions are set by institutions/ad hoc processes with little visibility, influence, or adaptation for the community.

What mechanisms can the data space use to provide visibility onto these elements?

- ☐ **3 Points:** The data space provides sustained, practical visibility into these elements through documented, accessible mechanisms (e.g., clear records of data provenance and flows, transparent access conditions and changes, published governance decisions with rationales, and logs/registries that allow affected parties to understand what happened and why), and these visibility tools support feedback and contestation over time.

☐ **2 Points:** Some visibility mechanisms exist, but they are incomplete or uneven (e.g., limited to certain data/products or actors, hard to access or interpret, not regularly updated, missing rationales, or not linked to feedback/contestation), so community understanding and influence is only partial.

☐ **1 Point:** Visibility is largely absent or informal; key elements are opaque, scattered, or only available on request, with no reliable records, no systematic publication of decisions/rationales, and no practical way for affected parties to track or challenge what occurs.

How can important decisions be explained in an intelligible manner, given the community's limited time, resource, and knowledge of data activities?

☐ **3 Points:** Every important decision gets a short, plain-language note: what/why/who/impact + where to see the supporting record, with a clear channel to ask/contest.

☐ **2 Points:** Explanations exist but are inconsistent (missing why/impact/who, too technical, or hard to find), so most community members can't reliably understand or respond.

☐ **1 Point:** Explanations are absent or ad hoc; decisions are effectively opaque, leaving the community without practical understanding or influence.

ACCOUNTABILITY AND AUTONOMY

Who is ultimately responsible for what decisions? How is this tracked and communicated?

☐ **3 Points:** Decision rights and accountability are explicitly assigned (roles/mandates), and decisions are traceable and reviewable via documented governance processes plus records (e.g., decision logs/traceability, published rules, and clear communication of "who decided what and why").

☐ **2 Points:** Responsibilities exist on paper, but tracking/communication is partial (e.g., unclear decision rights, incomplete records, limited traceability, or inconsistent communication to participants/communities).

☐ **1 Point:** Responsibility is unclear or fragmented; decisions are not consistently tracked or communicated, leaving accountability and oversight weak in practice.

What do community members see as appropriate measures to ensure compliance with legal, ethical, and internal governance standards?

☐ **3 Points:** Community expectations are gathered and turned into clear rules and checks (training, monitoring/audits, reporting, and consequences) that are actually used.

☐ **2 Points:** Some rules and checks exist, but they don't fully match community expectations or are applied unevenly (limited monitoring, weak reporting, unclear consequences).

☐ **1 Point:** Compliance relies on vague principles or ad hoc effort; there are no clear checks, reporting, or consequences aligned with community expectations.

What grievance or redress mechanisms do they expect if a rule is violated?

☐ **3 Points**: There is a clear, simple way to report violations; complaints are reviewed by a defined body; timelines and outcomes are communicated; fixes and remedies are possible.

☐ **2 Points**: A reporting path exists, but it's hard to use, slow, unclear, or rarely leads to meaningful outcomes.

☐ **1 Point**: No reliable grievance path; handling is informal and opaque, with no clear remedy.

EFFECTIVENESS AND AGILITY

What kind of results can be reasonably expected from the data space and at what speed?

☐ **3 Points:** Expected results are clearly defined (what, for whom, and how success is measured) with realistic timelines; progress is reviewed regularly and adjusted when conditions change.

☐ **2 Points**: Results or timelines are stated but vague or optimistic; tracking exists but is irregular, so expectations are only partly reliable.

☐ **1 Point**: Results and speed are unclear or unrealistic; there is no consistent way to track progress or recalibrate expectations.

Are there certain obligations—legal, ethical, professional—that may impede these results? Does the community understand these?

☐ **3 Points**: Key obligations are identified and explained in plain language; trade-offs are transparent; the community understands how obligations limit speed/scope and how decisions balance them.

☐ **2 Points**: Some obligations are identified, but explanations are partial or too technical; trade-offs are not consistently communicated, so understanding is uneven.

☐ **1 Point:** Obligations are not clearly identified or explained; constraints appear unexpectedly, creating confusion and mistrust.

What would be the cost of trying to accelerate or expand work?

☐ **3 Points**: Costs are assessed and communicated before scaling (money, staff time, technical effort, governance overhead, and risk); the community can see what is gained and what is sacrificed.

☐ **2 Points**: Some cost discussion exists, but it is incomplete (focuses on budget only, or ignores governance/risk impacts), so decisions to accelerate/expand are only partly informed.

☐ **1 Point**: Acceleration/expansion happens without a clear cost or risk assessment; hidden burdens fall on participants or affected groups.

DURABILITY

What kinds of risks exist that might compromise the data space's continued operation (e.g. financial support, leadership succession, conflict of interests, erosion of trust)?

☐ **3 Points**: The main risks are clearly identified and documented, including funding stability, leadership continuity, conflicts of interest, and trust risks, and there is a practical plan for how each would be handled if it happens.

☐ **2 Points**: Some risks are identified, but the list is incomplete or too general, or it is not clear how the data space would respond if the risk occurs.

☐ **1 Point**: Risks are not clearly identified; when problems arise they are handled case by case, which makes continued operation and trust fragile.

What contingencies would the community accept to safeguard against these risks?

☐ **3 Points**: The community has discussed and agreed in advance what "fallback" measures are acceptable for the main risks (e.g., loss of funding, leadership change, conflicts of interest, loss of trust), and these measures are written down so people know what will happen and how core commitments will be protected.

☐ **2 Points**: Some fallback measures have been discussed, but agreement is partial (only some risks covered, not clearly written down, or not clear whether the wider community accepts them), so it's uncertain what will happen if a risk materializes.

☐ **1 Point**: No agreed fallback measures exist; safeguards are decided ad hoc when a problem occurs, with little community input and weak protection for core commitments.

How often should the data space and its governance be reviewed? By whom?

☐ **3 Points**: Review cycles are defined (regular schedule + trigger-based reviews), with clear responsibility, community participation, and public reporting of findings and changes.

☐ **2 Points**: Reviews happen, but timing is irregular, responsibility is unclear, or community involvement/reporting is limited.

☐ **1 Point**: No regular reviews; governance is "set and forget," with little accountability or adaptation over time.

BALANCING TRADE-OFFS

Which benefits and principles does the community prioritize above all others?

- ☐ **3 Points:** The data space operator has developed a comprehensive list of the community's interests and worked with them to rank those interests from most important to least important. The community and data space are in agreement that the data space operator will pursue these interests in the order identified when possible.
- ☐ **2 Points:** The data space operator has, with input from the community, developed a list of several of the communities most important interests and identified the most important of these. The data space has communicated that it will pursue these interests but there may be some other interest or priority that it will also consider.
- ☐ **1 Point:** The data space operator has not secured a clear understanding of the community's interests nor communicated with them about how to prioritize them. The data space operator is primarily pursuing its own interests or what it assumes the community's interests to be.

If two principles or benefits are in conflict, does one supersede the other?

- ☐ **3 Points:** The data space operator has a plan indicating which interests it will pursue and how it will communicate clearly to the public when conflicts arise.
- ☐ **2 Points:** The data space operator has a plan indicating which interests it will pursue but does not have a clear mechanism by which it can communicate these conflicts when they occur.
- ☐ **1 Point:** The data space operator has no plan for addressing conflicts between different interests and benefits

If the community cannot come to consensus on a priority, would it accept any deliberation or negotiation mechanism to resolve a dispute?

- ☐ **3 Points:** Through participatory engagement, the community and data space operator have developed a mechanism by which disputes can be handled. There is a means by which the community can involve itself in this mechanism and stay informed of decisions made after the fact.
- ☐ **2 Points:** Following participatory engagement, the data space operator has developed a mechanism to manage disputes. This mechanism is led by the data space operator and community members have no obvious way to involve themselves but can stay informed and exercise input after the fact.
- ☐ **1 Point:** The data space operator either has failed to develop a mechanism to sort through disputes or has developed its own approach that neglects to consider community interests or concerns.

SCORE — PRINCIPLES: _____ of 54 TOTAL

3. PROCESSES

Governance Structures and Decision-Making

Processes define the **"how" of governance**: the structures, roles, and mechanisms through which decisions about the data space are made, implemented, and reviewed. Strong processes ensure that principles are operationalized, stakeholders are engaged, and accountability is clear.

GUIDING QUESTIONS

GOVERNANCE BODIES AND ROLES

What governance bodies are needed given the community's interests (e.g., data collaborative board, technical committees, advisory panels, independent oversight boards)?

- ☐ **3 Points:** The data space has developed and launched a set of governance bodies that match the community's articulated interests and concerns. These each have a clear mandate, authority, and composition.
- ☐ **2 Points:** Some relevant bodies have been identified and erected to address the community's largest concerns and interests but the overall structure is incomplete or under-specified. Some roles and functions may be unclear.
- ☐ **1 Point:** Governance bodies are absent, minimal, or tokenistic. If there are structures, they are vague and generic, with no clear relationship between the functions they serve and the community's concerns.

What is the mandate, scope of authority, and line of accountability for these bodies? Is it clear and understandable to stakeholders?

- ☐ **3 Points:** The mandate, scope of authority, and lines of accountability for each governance body are well-defined, well-documented, and understandable to all stakeholders. Roles and rights are explicit and all stakeholders understand who decides what, on what basis, and how those decisions may be disputed or contested.
- ☐ **2 Points:** The mandate and authorities of governance institutions are partly defined. While there are some clear roles and responsibilities, these may overlap with other institutions or are unclear to outsiders. While stakeholders understand the process at a high level, engaging throughout the decision lifecycle is difficult.
- ☐ **1 Point:** Mandates, scopes of authority, and lines of accountability are undocumented or largely informal. How decisions are made is largely assumed as opposed to being clear and explicit. There is little to no understanding of who is practically responsible for how decisions are made or how these groups may be held accountable.

Does the community view these as sufficient to handle ethics, compliance, or trust assurance needs? If not, what are their objections?

- ☐ **3 Points:** The community largely views the governance bodies as sufficient to address ethics, compliance, and trust assurance needs. There is clear evidence that the governance bodies will be legitimate and effective and, where there are lingering objections or concerns, community members understand that opportunities still exist for feedback and revisions.
- ☐ **2 Points:** The community understands that there are governance bodies to address ethics, compliance, and trust assurance needs, even if acceptance of these bodies is not universal across the community. There may be serious objections that have been only partially addressed or a lack of compelling evidence that the data space will follow through on its commitments.
- ☐ **1 Point:** Governance bodies are absent or viewed as wholly insufficient, untrustworthy, or illegitimate for handling ethics, compliance, and trust assurance needs. There are major community objections that have gone unaddressed and there is a total lack of evidence that the systems are capable of responding to community needs.

DECISION-MAKING FRAMEWORK

What criteria will be used to approve new datasets, use cases, or partnerships?

- ☐ **3 Points:** Clear, documented approval criteria exist and are broadly understandable to all stakeholders and community members. These criteria are consistently applied in decision-making.
- ☐ **2 Points:** Approval criteria are defined but are partial or weakly documented (e.g. unclear exceptions, thresholds). While the criteria guide activities, governance bodies may deviate from these on occasion.
- ☐ **1 Point:** Approval criteria are informal or absent. It is not possible for outside stakeholders to understand how decisions were made and data space operations may appear entirely ad hoc.

How will evaluation balance purpose, risk, and public value?

- ☐ **3 Points:** There are defined criteria or decision processes that allow governance bodies to reasonably assess trade-offs between data space purpose, risk, and public value.
- ☐ **2 Points:** There are criteria or decision processes that allow governance bodies to assess trade-offs between data space purpose, risk, and public value but these may be uneven or weakly documented, offering limited clarity on how these affect decisions.
- ☐ **1 Point:** Evaluation criteria, if they exist, fail to consider purpose, risk, and public value simultaneously. Decisions are made on an ad hoc basis.

What mechanisms will guarantee structured input from both technical experts and affected communities?

- ☐ **3 Points:** There are well-defined mechanisms that allow for regular, structured input from technical experts and the affected communities. These mechanisms are well-documented, with all parties understanding their roles as well as the processes and information that informs decisions.
- ☐ **2 Points:** There are structured input mechanisms that incorporate both technical experts and affected communities but they may be uneven, irregular, or give excessive deference to one authority over another. There is some general guidance on how processes operate but parties lack specifics.
- ☐ **1 Point:** Structured input mechanisms are absent or informal, relying more on ad hoc decisions than any established process. There is little to no transparency and the mechanism fails to incorporate meaningful input from technical experts or the community.

How will decisions be documented (provenance, rationale, stakeholder input) to enable traceability?

- ☐ **3 Points:** Decisions are systematically documented with clear references to the provenance, stakeholders, and rationale—thus enabling clear review and accountability.
- ☐ **2 Points:** Decisions are partially accounted for or only major decisions are accounted for. This documentation offers some insight into the provenance, rationale, and stakeholders, but not enough to ensure accountability in all cases.
- ☐ **1 Point:** Decision documentation is tokenistic or absent. It is not possible to consistently trace decisions, understand the reasoning behind them, or verify stakeholder input.

STAKEHOLDER ENGAGEMENT AND PARTICIPATION

How will different stakeholder groups be engaged in ongoing governance (advisory committees, consultations, co-design workshops)?

- ☐ **3 Points:** Stakeholders are regularly and continuously engaged throughout the lifespan of the data space. Their input has a clear role in governance and evidence of their influence can be seen in the decisions that the data space makes.
- ☐ **2 Points:** Stakeholders are engaged through the data space but engagements may be uneven, irregular, or lack a direct connection to governance decisions.
- ☐ **1 Point:** Stakeholder input is minimal or tokenistic. There are no efforts to reliably solicit stakeholder input and there is no evidence that input received connects to governance.

Is this engagement "meaningful" and not tokenistic in the eyes of community members?

- ☐ **3 Points:** Community members view engagement as meaningful as there is clear evidence that their input is valued, responded to, and shapes data space outcomes.
- ☐ **2 Points:** Community members see some value in their engagement. While their input is not always acted upon, there is evidence that it is at least heard and considered.
- ☐ **1 Point:** Community members see no value in engagement because existing interactions are shallow and tokenistic. They do not see the data space as responsive to their concerns and see no real influence on governance decisions.

How will disputes among stakeholders be resolved (internal mediation, external arbitration, escalation to governance board)?

- ☐ **3 Points:** The data space has a set process for resolving disputes that it abides by in all circumstances. This mechanism is broadly accepted and well understood by all parties.
- ☐ **2 Points:** The data space has a process for resolving disputes but it may, at times, deviate from this process when operators find it convenient. There may be a lack of broad support and understanding.
- ☐ **1 Point:** Dispute resolution is handled in an ad hoc manner, with unclear procedures. There is no understanding of how decisions are made except among those making decisions.

OVERSIGHT, MONITORING, AND EVALUATION

What processes will track compliance with principles, legal frameworks, and contractual obligations?

- ☐ **3 Points:** There are systems that ensure all actions are monitored and subject to responsible oversight that can guarantee compliance with principles, legal requirements, and contractual obligations.
- ☐ **2 Points:** Actions are monitored and subject to oversight but this may be less due to established processes and more to the culture of the data space or involvement from an outside party.
- ☐ **1 Point:** Compliance tracking is absent, a concern of the data space only when problems arise. Data space operators cannot, in the course of normal business, ensure that there is meaningful compliance with principles, legal frameworks, and contractual obligations.

What indicators will be monitored to assess governance effectiveness (inclusivity, trust, efficiency, equity)?

- ☐ **3 Points:** There are clear, consistent indicators that are understandable and supported by all relevant parties. These indicators can be tracked with regularly received evidence and reporting and this reporting informs improvements to the data space.
- ☐ **2 Points:** There are indicators but they may not all be easily understandable or able to be consistently measured with objective evidence. The data space may not have a clear vehicle to facilitate improvements in response to its ability to meet indicators.
- ☐ **1 Point:** Few or no indicators are monitored. Evidence is not reliably received or objective. There are no mechanisms by which improvements can be incorporated into the data space.

How will findings be shared with stakeholders and the public?

- ☐ **3 Points:** Findings are regularly shared through channels that the community has access to and approves of. These findings are paired with clear information on methods, decisions, impact, involved stakeholders, and any other information that the public may need.
- ☐ **2 Points:** Findings are shared with the public through channels that the community could reasonably access. There may be some vagueness or limits on how much information is shared on methods, decisions, impact, and involved stakeholders that limit the ability of the community to engage.
- ☐ **1 Point:** Findings are rarely if ever shared, with there being no meaningful opportunities for stakeholders to respond or act on information.

ADAPTATION AND LEARNING

What processes will track compliance with principles, legal frameworks, and contractual obligations?

- ☐ **3 Points:** There are processes that reliably monitor compliance. These are paired with well-assigned roles and responsibilities, procedures, and mechanisms to detect, record, and correct violations.
- ☐ **2 Points:** There are processes that monitor compliance but these may have certain limitations or blindspots. The data space may lack specificity on roles, responsibilities, procedures, and mechanisms that can reliably guarantee violations are detected, recorded, and corrected.
- ☐ **1 Point:** Compliance tracking is ad hoc, informal, or absent, with little or no visibility into whether principles, laws, or contractual obligations are being met.

How will audits (internal and external) be conducted and acted upon?

- ☐ **3 Points:** Audits are regularly conducted, clearly structured, and findings are documented, communicated, and acted upon, with assigned responsibilities for follow-up and corrective actions.
- ☐ **2 Points:** Audits occur occasionally or partially, with inconsistent follow-up, unclear responsibilities, or incomplete implementation of recommendations.
- ☐ **1 Point:** Audits are rare, informal, or absent. Documentation on them is limited and there is little evidence that they inform governance.

FINANCIAL AND OPERATIONAL SUSTAINABILITY

How will resources be allocated to support governance operations?

- ☐ **3 Points:** There is a well-specified budget that denotes in clear, understandable language where funding is to be allocated. This is supported by evidence that ensures that funding is sufficient and can be sustained to ensure governance functions.
- ☐ **2 Points:** There is a budget, though it may lack some detail or be overly technical for most participants. It is unclear if the funding will be sufficient or sustainable long-term but it can ensure short-term operation.
- ☐ **1 Point:** The budget is clearly insufficient, with large gaps or contradictions. It is unlikely that the resources available can support short term or long term activity.

What funding models will sustain governance in the long term (public funding, membership fees, blended finance, value-sharing mechanisms)?

- ☐ **3 Points:** The funding model matches the context and can clearly be sustained in the long-term, giving all stakeholders confidence that the data space can be sustained as long as needed.
- ☐ **2 Points:** A funding model exists, though it may rely on short-term arrangements or be ill-fitting to the context. The data space will need to develop new systems to operate in the future.
- ☐ **1 Point:** There is no funding beyond initial seed funding. It is not clear that the data space can sustain itself beyond the initial launch.

How will risks and dependencies be mitigated?

- ☐ **3 Points:** The data space operators have proactively mapped all possible risks to the longevity of the data space and developed mitigation and contingency plans to counter these within reason.
- ☐ **2 Points:** The data space operators have identified several major risks to the longevity of the data space but this mapping is not comprehensive. The efforts to mitigate these

risks may be incomplete or ill-defined, requiring further refinement.

☐ **1 Point:** The data space operators have not tried to meaningfully identify risks to their activities. There is no plan if a major risk or crisis emerges.

SCORE — PROCESSES: _____ of 54 TOTAL

4. PRACTICES & POLICIES

Operational Mechanisms for Governance

Practices and policies provide the **concrete, enforceable rules, standards, and tools** that put governance into action. They translate principles and processes into daily operations, covering the entire data lifecycle (planning, acquisition, processing, sharing, reuse, archiving).

GUIDING QUESTIONS

DATA ACQUISITION, INVENTORY, AND PROVENANCE

How will data sources be identified, mapped, and categorized (e.g. public, private, community, crowdsourced) given community expectations?

- ☐ **3 Points:** There is a clear, transparent, and well-documented process for identifying, mapping, and categorizing data sources. These categories are clearly defined and reflect an approach in line with community expectations around data collection, processing, and (re-)use. There may be some form of direct community involvement in this work.
- ☐ **2 Points:** There is a process that can allow for data sources to be identified, mapped, and categorized—but this process may not be fully clear, transparent or well-documented, making it difficult to enforce standards. Community expectations are acknowledged but not fully reflected and there is no direct pathway to allow for community involvement.
- ☐ **1 Point:** There is no regular process for identifying, mapping, and categorizing data sources. Categories are vague, overlapping, or inconsistent and bear little relation to the expectations and aspirations of the community.

How will provenance (origin, transformations, usage) be tracked and made auditable?

- ☐ **3 Points:** The data space has a framework that allows data to be tracked in its origin, transformations, and usage across the data lifecycle. There is regular effort to ensure standardized, securely maintained, and accessible audit records.
- ☐ **2 Points:** The data space has a framework that allows some tracking of data in its origin, transformations, and usage across the data lifecycle, but there are some gaps that limit oversight. There is some effort to promote standardized, securely maintained, and accessible audit records but these may not be universally applied.
- ☐ **1 Point:** There is little to no systematic tracking of data provenance. Information about data origin, transformations, and usage is incomplete, undocumented, or inaccessible. Independent auditing is difficult or impossible, undermining trust.

What processes will ensure missing or underrepresented datasets are identified and addressed?

- ☐ **3 Points:** There are regular, ongoing processes that assess datasets and identify gaps or biases. These processes are informed by input from domain experts and the community as well as specific focus on issues of equity.
- ☐ **2 Points:** There are some processes that assess datasets and identify gaps or biases. These processes can incorporate input from domain experts and the community but may only be reactive, responding when objections are raised. There is no larger strategy that emphasizes equity.
- ☐ **1 Point:** There are no defined processes that identify missing or underrepresented datasets and gaps in knowledge are not assessed, resulting in blind spots in the data space.

ACCESS AND PERMISSIONING

Given the purpose, wider goals, and legal requirements what limitations need to be placed on use?

- ☐ **3 Points:** There are clear, well-defined limitations on data use that are explicitly linked to the stated purpose, societal goals, legal and regulatory requirements, and community expectations. These limits are communicated in a manner that is clear and accessible to all stakeholders and there is some mechanism that can enforce these limits.
- ☐ **2 Points:** There are limitations that implicitly relate to the stated purpose, societal goals, legal and regulatory requirements, and community expectations but these limits may be vague or incomplete. There is some communication but it may not penetrate deeply among stakeholders. Enforcement mechanisms are uneven and rely primarily on voluntary compliance.
- ☐ **1 Point:** There are few articulated limitations on data use beyond minimal legal requirements. Communication is minimal or non-existent and attempts to abide by requirements are unenforced. There is substantial risk of both mission drift and violation of community expectations.

How will access rights be tied to purpose, role, and compliance obligations?

- ☐ **3 Points:** Access rights are clearly defined and linked to set roles, purposes, or obligations. These restrictions are consistently applied and well-documented. Access credentials can be revoked or adjusted when conditions change.
- ☐ **2 Points:** Access rights are defined but may only be loosely connected to set roles, purposes, or obligations—instead relying on ad hoc or informal decisionmaking. Reviews of access are infrequent, manual, and reactive, which may lead to some excessive access or risk of exposure.

☐ **1 Point:** There are no clear access rights and no reliable way for access to be changed or modified. There is a high risk of inappropriate or non-complaint data use from actors who should not have access.

What monitoring (audit logs, anomaly detection, expiry dates) will ensure secure and appropriate data use and reassure the community?

☐ **3 Points:** There are comprehensive monitoring mechanisms—including audit logs, anomaly detection, and time-bound access or data controls. These measures are systematically implemented, affecting all data space stakeholders, and there are set steps that can be taken in response to violations of standards that can ensure the community's data remains secure.

☐ **2 Points:** Some monitoring mechanisms exist—such as basic audit logs and anomaly detection—but do not cover the full spectrum of risks or are inconsistently applied. While there are steps that can be taken in response to violations of standards, some review triggers may be manual or ad hoc.

☐ **1 Point:** There is little or no meaningful monitoring of data use. Audit logs are absent or rarely reviewed. There are few mechanisms to detect misuse. There is no reliable way to ensure that the community's data remains secure or that actors remain accountable.

PRIVACY, SECURITY, AND RISK MANAGEMENT

What are the risks that might arise from data collection, processing, storage, and use?

☐ **3 Points:** Data space operators have tried to comprehensively document and assess risks (e.g. legal, technical, community) across the data lifecycle with input from the community and other stakeholders. Responses to these risks have been identified, with certain likely or extremely dangerous risks having extensive mitigation measures. There is a regular process by which this assessment of risks can be regularly updated.

☐ **2 Points:** Data space operators have documented and assessed some high-concern risks (e.g. legal, technical, community) but these are not comprehensive or do not span the full length of the data lifecycle. There are some mitigation measures but these may not be appropriately prioritized or fully operationalized.

☐ **1 Point:** There has been little to no systematic effort to identify risks across the data lifecycle and potential harms are unacknowledged or undocumented. If there are mitigation processes, these are developed in response to threats emerging, leading to a high likelihood of community harm.

What steps to mitigate harm and risk does the community expect given previous outreach?

- ☐ **3 Points:** Community outreach has clearly identified the steps that the community expects and needs to minimize potential harms. These are clearly documented and communicated to the community in a language they understand.
- ☐ **2 Points:** The community has had to reach out to data space operators on their own behalf to raise their concerns, but the data space operator has taken some steps to address risk of harm. These have been translated into actionable documents but may not be broadly accessible or understandable.
- ☐ **1 Point:** Community outreach has not meaningfully informed harm or risk mitigation. Concerns are not gathered and outreach is tokenistic. If there has been any documentation, it is largely inaccessible and not transparent.

How will the data space respond to malicious activity from internal and external actors (e.g. data breaches, misuse, discrimination, harmful re-use)?

- ☐ **3 Points:** Clear, documented response processes exist for detecting, reporting, and addressing malicious activity, with defined roles and ways to escalate and pursue remediation as well as pathways to communicate clearly to affected stakeholders.
- ☐ **2 Points:** Some response mechanisms exist, but they are partial, reactive, or inconsistently applied, with unclear responsibilities, limited preparedness, or weak follow-through. Communication with affected stakeholders is limited or partial.
- ☐ **1 Point:** Response to malicious activity is ad hoc or undefined, with little capacity to detect incidents, coordinate action, or prevent recurrence. There is no communication to affected stakeholders.

LEGAL AND CONTRACTUAL FRAMEWORKS

What legal instruments govern the data space (e.g. MOUs, Data Use Agreements, NDAs, IP licensing)?

- ☐ **3 Points:** There is a set of commonly understood, commonly agreed upon legal instruments that are appropriate for the context and comprehensively address the needs of data space stakeholders and set obligations around major issues such as confidentiality, IP, data use standards.
- ☐ **2 Points:** There are some legal instruments but they may not fully match the context or otherwise fail to meet the full needs of stakeholders. Issues such as confidentiality, IP, and data use standards are only partially addressed.
- ☐ **1 Point:** Legal instruments are absent or completely irrelevant. There is little that can enforce standards on major issues other than the good will of participants.

How do the roles and responsibilities in these agreements impact different stakeholders?

- ☐ **3 Points:** The agreements set out clearly defined roles that equitably divide responsibilities and match the expectations of the community and other stakeholder groups. All participants understand what their duties are because the language is clear, precise, and as simplified as possible.
- ☐ **2 Points:** The agreements set out roles that define responsibilities, but these may not fully reflect community and stakeholder expectations or may impose undue burden on a handful of actors. The language may not be easily understandable to all and may require some technical expertise.
- ☐ **1 Point:** Roles and responsibilities are unclear, informal, or outright infeasible. The language in the agreement is not understood or agreeable to all data space participants.

How can this impact be clearly communicated and what steps can be taken to ensure all stakeholders comply with stated requirements?

- ☐ **3 Points:** The impact of the data space is clearly communicated to all stakeholders in a format and language they are familiar with. There are mechanisms (e.g. training, reporting) that reassure stakeholders that there is compliance with all requirements.
- ☐ **2 Points:** The impact of the data space is communicated externally but may not be available in a language and format that is broadly comprehensible. Mechanisms to reassure stakeholders may be partial or reactive.
- ☐ **1 Point:** The impact is poorly communicated or absent entirely. Community members are only informed on an ad hoc basis and not in a manner they can readily engage with.

INTEROPERABILITY AND STANDARDS

What technical standards (metadata, ontologies, APIs, federated models) will ensure interoperability?

- ☐ **3 Points:** Technical standards are clearly defined, widely adopted, and consistently applied leading to interoperability across systems and stakeholders.
- ☐ **2 Points:** Technical standards are present but they are inconsistently applied or lack sufficient depth, limiting interoperability in some cases.
- ☐ **1 Point:** Technical standards are minimal or absent, making interoperability impossible to guarantee.

How will alignment with broader values and interests be secured?

- ☐ **3 Points:** There is explicit alignment between broader societal goals, community values, and organizational aspirations and the technical standards. These are ensured through governance processes that embed stakeholder input and oversight.
- ☐ **2 Points:** There is some alignment between broader societal goals, community values, and organizational aspirations. There may be some conflicts that prevent stakeholders or community members from having their voices fully heard.
- ☐ **1 Point:** There is no alignment between broader values and interests and the technical standards, which are rote and developed with little consideration for the larger context.

CAPACITY BUILDING AND KNOWLEDGE SHARING

What training is needed for data stewards, policymakers, community representatives, and technical staff to align institutional culture with community expectations?

- ☐ **3 Points:** There is comprehensive, role-specific training that is routinely delivered and updated to match needs, ensuring all stakeholders understand community expectations.
- ☐ **2 Points:** There is some training but it is incomplete or irregular, leaving gaps in understanding that limit the ability of stakeholders to understand and address community expectations.
- ☐ **1 Point:** Training is minimal or tokenistic and there is little support between the guidance provided and community expectations.

How will best practices and lessons learned be documented and shared across stakeholders?

- ☐ **3 Points:** Best practices and lessons learned are systematically documented, accessible, and actively shared with all stakeholders, supporting continuous learning and improvement.
- ☐ **2 Points:** Best practices and lessons learned are only partially documented, focusing on only a handful of issues, limiting their value for stakeholders.
- ☐ **1 Point:** Best practices and lessons learned are not documented and any learning or improvement occurs only informally.

MONITORING, EVALUATION, AND CONTINUOUS IMPROVEMENT

How will governance practices be regularly audited (internal review, third-party evaluations, community-led oversight)?

- ☐ **3 Points:** Governance practices are routinely audited in a process that aligns with the overall purpose and community expectations. The process by which auditing occurs is documented and well-understood by all stakeholders.
- ☐ **2 Points:** Governance practices are irregularly or partially audited and this auditing supports but is not fully aligned with the purpose and community expectations. There is some documentation that can ensure that audits are consistently handled.
- ☐ **1 Point:** Audits are rare, informal, or absent. There is little evidence of review, oversight, or continuous improvement.

What KPIs will be used to measure the effectiveness of policies (trust, inclusivity, data quality, resilience)?

- ☐ **3 Points:** The data space has outlined various KPIs that can be used to evaluate trust, inclusivity, data quality and resilience. These are regularly monitored, reported, and used to inform policy improvements.
- ☐ **2 Points:** The data space has a few KPIs that could assess trust, inclusivity, data quality, and resilience, but they are incomplete or inconsistently applied. There is only a weak link to governance improvement.
- ☐ **1 Point:** KPIs are absent, poorly defined, or rarely monitored. There is little evidence of policy effectiveness or guidance that can lead to improvement.

How will feedback from evaluations be integrated into updated policies?

- ☐ **3 Points:** Feedback from evaluations is systematically reviewed and regularly incorporated into policy updates. There is a clear process that ensures learning informs governance.
- ☐ **2 Points:** Some feedback is considered but their integration is partial or informal. Lessons cannot be said to consistently shape governance.
- ☐ **1 Point:** Feedback from evaluations is rarely if ever used. There is no evidence that lessons are gathered or that any feedback shapes governance.

EXIT, ARCHIVING, AND END-OF-LIFE POLICIES

What does the community expect about data handling given the stated purpose and risks?

- ☐ **3 Points:** Community expectations are clearly understood, documented, and incorporated into exit, archiving, and end-of-life policies, ensuring data is handled responsibly, securely, and in alignment with purpose and risk considerations.
- ☐ **2 Points:** Some expectations are recognized, but policies for exit, archiving, or end-of-life are partial, inconsistent, or weakly aligned with community priorities and risk mitigation.
- ☐ **1 Point:** Community expectations are unclear, unassessed, or ignored, and exit, archiving, or end-of-life practices are ad hoc, inconsistent, or misaligned with stated purposes and risks.

How will data be archived, deleted, or transitioned at the end of its lifecycle?

- ☐ **3 Points:** There are clear, documented procedures for archiving, deleting, or transitioning the data space. These are consistently applied and there are opportunities for community review for accountability.
- ☐ **2 Points:** Some procedures exist but they may not capture all data. There are few opportunities for the community to exercise review.
- ☐ **1 Point:** Procedures for end-of-life data handling are absent and there is substantial risk of misuse or unwanted retention.

How will communities and stakeholders be consulted before data is retired or repurposed?

- ☐ **3 Points:** Communities and stakeholders are actively and systematically consulted through clearly defined mechanisms (such as surveys, advisory boards) before any decisions are made about what to do at the end of the data space's life. Feedback from these is documented, reviewed, and meaningfully incorporated into decisions—with transparency by the data space on how it is acting on the input.
- ☐ **2 Points:** Consultation occurs but not in a way that allows the full community to participate or imposes other limits (e.g. occasional, time-limited meetings, surveys that fail to capture all questions). Feedback is collected but the relationship between it and the actions taken is indirect and may be difficult for some stakeholders to understand.
- ☐ **1 Point:** There is no meaningful consultation. Feedback is disregarded or ignored and the data space operates without consideration for community needs.

SCORE TOTAL: PRACTICES: _____ of 66 TOTAL

OVERARCHING SCORE TOTAL: _____ of 219 TOTAL

APPENDIX II

Guidance on Costs for Digital Self-Determination Implementation in a Data Space

Purpose

This guidance explains how to scope, structure, and govern the costs required to implement Digital Self-Determination in a data space.

Implementation costing for DSD inside data spaces has, in practice, not yet been systematized: There is no settled "costing canon" that treats DSD as a lifecycle-wide governance investment with stable benchmarks. In that sense, data space operators are operating in a new space: the first defensible costing exercises will be those that (i) make DSD "budgetable" by decomposing it into the four governance capacities from Phase 1, Section 1.3, and (ii) attach those costs to a sustainability logic (multi-year, fundable, auditable, and resilient).

Participatory governance examples can be useful only as *intuition* for volatility, not as a reference point for DSD-in-data-spaces costing. For example, the Scottish Government's FOI release on citizens' assembly costs illustrates this variability: It records costs, including £1,966,776.76 (and notes that it does not include indirect staff costs).[50] Separately, Involve (a major UK participation practitioner) states that citizens' assemblies typically require £150,000–£750,000, with price driven by size, format, deliberation time, delivery modality, and the "creativity/support" and communication/follow-up wrapped around the process.[51] Those numbers show that "participation" is not a neat line item; it scales nonlinearly with design choices.

Crucially, however, DSD costing cannot be reduced to participation alone. The DSD model explicitly embeds enforceability, contestability/redress, and continuous assurance as ongoing operational capacities, meaning the cost structure is distributed across implementation and steady-state operations rather than concentrated in a single deliberative event.

The guidance below, therefore, starts from the idea that DSD is a **governance infrastructure**. It should be costed like infrastructure: with named owners, recurring operations, toolchains and processes, and clear evidence that the investment is sufficient to sustain legitimacy over time.

Making DSD "budgetable": one cost structure, four capacities

Costing DSD begins by treating the four core capacities as the top-level budget headings. These headings are designed to be stable across use cases and domains, while still allowing cost differences to be expressed through concrete design choices and operational scale.

- **Participation and Preference Expression**: the sustained ability of individuals and affected communities to articulate expectations, boundaries, and concerns about data use.
- **Translation into Enforceable Governance**: the conversion of social expectations into binding rules and enforceable technical controls across organizations and systems.
- **Transparency, Contestability, and Redress**: the accountability infrastructure that enables explanation, challenge, correction, and remedy.
- **Ongoing DSD Assurance**: the adaptive capacity to stress test governance, measure performance, revise rules, and keep governance aligned with changing technology and societal expectations.

For each capacity, DSD costs should be recorded explicitly across three cost types: people/roles, processes/operations, and systems/tooling (technical and documentary). This avoids a common failure mode in governance costing where roles are funded but processes are not operationalized, or tooling is purchased without staffing and cadence to run it.

From capacities to budget lines: why volume drivers matter

To move from a conceptual cost structure to a defensible budget, each capacity must be translated into budget lines tied to concrete volume drivers—the measurable quantities that determine workload and cost. Without volume drivers, the model remains descriptive rather than estimative.

For ***Participation and Preference Expression***, the main cost drivers are the *size and cadence* of engagement, not the mere fact of engagement. The relevant questions are how many stakeholder groups and publics are in scope; how often engagement cycles occur; how many participants are involved per cycle; what language and accessibility requirements apply; and what level of traceability is expected between input and decision ("you said → we did"). These drivers determine staffing (facilitation, community liaison, accessibility support), operational overhead (onboarding, representation mechanisms, recurring deliberation), and tooling (feedback capture, traceability, and—where relevant—preference interfaces).

For ***Translation into Enforceable Governance***, cost is driven by the number of governance artefacts and how often they change across a federated system: the number of policy/rule

sets; the revision cadence; the number of domains and systems that must implement controls; the number of contractual instruments (e.g., data sharing agreements) negotiated or updated; and the volume of exceptions/waivers. These drivers determine legal and policy drafting effort, technical control implementation (including configuration management and assurance), and the coordination overhead of cross-entity alignment.

For ***Transparency, Contestability, and Redress***, the key cost drivers are case volume and service levels. A data space must plan for expected inquiries and complaints, escalation rates, time-to-resolution targets, the volume of decision logging and audit activity, and what must be explainable to whom and when. These drivers determine staffing for support and review, the operational design of contestation workflows, and tooling for logging, audit trails, case management, evidence handling, and disclosure.

For ***Ongoing DSD Assurance***, cost is driven by the intensity and cadence of monitoring and adaptation: the number of KPIs, reporting frequency across domains, the number of audits/evaluations per year (internal and independent), the frequency of stress tests or tabletop exercises, and the governance revision cycle (review → update → re-adopt). These drivers determine evaluation spend, measurement and analytics support, monitoring dashboards, and the operational cost of iterative governance change management.

In practice, a robust DSD budget makes these drivers explicit because they serve as the defensible bridge between “what good governance requires” and “what it costs.”

Governing DSD costs: using the Financial & Operational Sustainability rubric as a gate

Once the cost structure exists, it should be assessed through a sustainability lens. Use the Appendix I Assessment for Data Space Governance, Section 3. Processes, guiding questions on Financial and Operational Sustainability as a **governance gate** to ensure the DSD cost structure is fundable, understandable, and resilient.

1) GATE 1 — ALLOCATION OF RESOURCES TO GOVERNANCE OPERATIONS

Question: *How will resources be allocated to support governance operations?*

- ☐ **3 points :** A **well-specified budget** describes allocations in **clear, understandable language** and is supported by evidence showing funding is **sufficient and sustainable** for governance functions.
- ☐ **2 points:** A budget exists but lacks detail and/or is overly technical; **sufficiency and long-term sustainability are unclear**, but short-term operations are possible.
- ☐ **1 point:** The budget is **insufficient**, with major gaps/contradictions; resources cannot credibly support short- or long-term activity.

DSD INTERPRETATION

A credible DSD budget must explicitly cover all four core capacities (A–D) with:

- Named owners
- Recurrence (monthly/quarterly/annual)
- "Run" vs "change" separation (ongoing operations vs evolution)

2) GATE 2 — LONG-TERM FUNDING MODEL(S)

Question: *What funding models will sustain governance in the long term (public funding, membership fees, blended finance, value-sharing mechanisms)?*

- ☐ **3 Points:** The funding model matches the context and can clearly be sustained in the long-term, giving all stakeholders confidence that the data space can be sustained as long as needed.
- ☐ **2 Points:** A funding model exists, though it may rely on short-term arrangements or be ill-fitting to the context. The data space will need to develop new systems to operate in the future.
- ☐ **1 Point:** There is no funding beyond initial seed funding. It is not clear that the data space can sustain itself beyond the initial launch.

DSD INTERPRETATION

Funding must cover **legitimacy operations** (participation, redress, evaluation) as first-class operational costs, not only technical platform operation.

3) GATE 3 — RISKS AND DEPENDENCIES MITIGATION

Question: *How will risks and dependencies be mitigated?*

- ☐ **3 Points:** The data space operators have proactively mapped all possible risks to the longevity of the data space and developed mitigation and contingency plans to counter these within reason.
- ☐ **2 Points:** The data space operators have identified several major risks to the longevity of the data space but this mapping is not comprehensive. The efforts to mitigate these risks may be incomplete or ill-defined, requiring further refinement.
- ☐ **1 Point:** The data space operators have not tried to meaningfully identify risks to their activities. There is no plan if a major risk or crisis emerges.

DSD INTERPRETATION

Include **political/legitimacy risks** (loss of trust, contestation, withdrawal) alongside financial, technical, vendor, and governance risks.

2) Evidence requirements (what to show to justify 3/2/1 ratings)

This section converts the rubric into concrete documentation expectations.

2.1 EVIDENCE FOR GATE 1 (BUDGET ALLOCATION)

To score **3**, maintain:

- A **budget narrative** readable by non-specialists (what is funded and why)
  - A **line-item table** mapped to capacities A–D, with:

    owner (role/body)

    recurrence

    cost type (people/process/system)

    baseline vs growth assumptions

- Evidence of **sufficiency and sustainability** (multi-year view; commitments; unit-cost logic; staffing plan)

To score **2**, typical gaps include:

- unclear mapping to A–D
- missing owners/cadence
- insufficient multi-year sustainability logic

To score **1**, typical failures include:

- absent funding for key DSD operations (e.g., contestability/redress, evaluation)
- contradictions between objectives and resourcing

2.2 EVIDENCE FOR GATE 2 (FUNDING MODEL)

To score **3**, maintain:

- A documented funding architecture (public funding, membership, blended, value-sharing)
- Justification of fit to context and stakeholder incentives
- Multi-year sustainability assumptions and triggers for adjustment

To score **2**, typical gaps include:

- reliance on short-term grants
- unclear allocation rules between participants
- no plan for scaling operations

To score **1**, typical failures include:

- “seed-only” funding with no operational runway

2.3 EVIDENCE FOR GATE 3 (RISKS & DEPENDENCIES)

To score **3**, maintain:

- A comprehensive risk register including political/legitimacy risks
- Mitigation owners and contingency plans
- Scenario testing cadence and escalation thresholds

To score **2**, typical gaps include:

- partial risk coverage
- mitigations not operationalized

To score **1**, typical failures include:

- no risk register, no contingencies

3) Decision rule (readiness to implement and scale)

Use the rubric as a gate for implementation readiness.

- If **any gate scores 1** → treat as **not ready to scale**. Proceed only with a remedy plan and the limited-scope pilot.
- If all gates score **≥2** → allow pilot/initial operation with a time-bound plan to reach 3.
- Target **3/3/3** before broad onboarding, expansion to high-stakes use cases, or significant participant growth.

4) Minimal "DSD Cost Governance Pack" (deliverables)

A data space implementing DSD should maintain, at a minimum:

DSD Cost Structure

- Capacities A–D; line items; owners; recurrence; people/process/system split; run vs change.

Financial & Operational Sustainability Scorecard

- 3/2/1 ratings for the three Appendix I questions, with evidence links.

Risk & Dependency Register

- Including legitimacy risks and contingency plans.

Governance Operations Calendar

- Participation cycles, policy revision cycles, audits/evaluations and reporting.

The Case of the Swiss Health Data Space (SwissHDS)

This guidance should be applicable—and likely useful—to SwissHDS because SwissHDS is defined as a virtual health data space spanning the processes and IT systems of specialized domains and actors, designed for secure, legally compliant, standardized exchange, with a stated timetable (initialization until 2026; implementation from 2026) and federal sponsorship via FOPH.[52] Federated and virtual designs predictably amplify governance cost drivers: more boundary crossings (organizations, domains, infrastructures),[53] greater heterogeneity (rules, cultures, maturity),[54] and more points where legitimacy can fail (opacity, perceived unfairness, limited redress).[55] Feasibility is therefore not constrained by the framework (which is intentionally generic) but by whether SwissHDS can provide the minimum inputs required to translate the four capacities into budget lines and to score sustainability with evidence.

In advance, SwissHDS would need to clarify scope and boundaries (which specialized domains, actor groups, and use cases are in scope in the next 12–24 months versus later, and what is centrally delivered versus domain-owned), operating model and decision rights (who owns and approves rulebooks/policies, who runs complaints/redress, who commissions audits/evaluations, and where enforcement sits), the financial envelope and funding mechanics (central versus co-funded components, CAPEX versus OPEX, build versus run, and what happens after initial program funding), and an operational risk and dependency view (including legitimacy risks such as contestation, loss of trust, and withdrawal of participation). With those inputs, our four core governance capacities model can be populated with volume drivers and translated into a credible multi-year cost structure.

ANNEX A

Working template (capacity × cost line item table)

Use this table structure to operationalize costing.

DSD capacity	**Line item**	**Cost type** *(people/ process/ system)*	**Owner** *(role/body)*	**Recurrence**	**Evidence for sufficiency**	**Funding source**	**Notes**
Participation & Preference Expression							
Translation into Enforceable Governance							
Transparency, Contestability & Redress							
Ongoing DSD Assurance							

ANNEX B

Scorecard (Appendix I rubric)

Question	Score (1/2/3)	Rationale	Evidence references	Remediation actions
Budget allocation How will resources be allocated to support governance operations?				
Funding model What funding models will sustain governance in the long term?				
Risks & dependencies How will risks and dependencies be mitigated?				

APPENDIX III

Guidance on Public Engagement Mechanism Selection

In **Phase 2 – Identifying Preferences, Interests, and Expectations**, we describe participatory data governance as the ways individuals, communities, and stakeholders can shape decisions about how data about or from them is accessed, shared, and reused. We describe how these mechanisms can be vital to digital self-determination and the steps data space operators can take to identify which type of mechanism is most appropriate for their and the communities needs.

In the below, we elaborate on each of the engagement types and several examples of the forms this outreach can take. This information is drawn from a variety of documents offering guidance on public engagement—most prominently the *OECD Guidelines for Citizen Participation* and the US Environmental Protection Agency's Public Participation Guide (though additional useful readings can be found in the "Sources and Further Reading" at the conclusion of this addendum).[56] We guide the reader through each of these using the considerations that we consider most relevant for data space operators.

- **LEVEL OF PUBLIC PARTICIPATION:** Assess how much influence data space operators can share or delegate with the community
- **PURPOSE OR GOAL:** Identify the purpose of this activity for the data space
- **AUDIENCE:** Map who the relevant parties for the data space are and their likely interests
- **TIME AND RESOURCES:** Assess the resources, readiness, capacity, and time available to launch a participatory data governance mechanism

Details on each of these questions can be found in the relevant chapter. Data space organizers may also wish to consider the kinds of questions they can ask during the process to advance the agency of participants. This may include questions such as:

- To what extent can this method advance digital self-determination?
- How and where can this method be operationalized in the context of a data space?

Informational

LEVEL OF PUBLIC PARTICIPATION: Assess how much influence data space operators can share or delegate with the community

All informational approaches are a one-way flow of information to communicate what is happening to a group of stakeholders. It cedes little to no control to others but can inform participants of their rights and the options available to them to exercise those rights.

Informational mechanisms are low-engagement strategies to bring information about data to the public's attention. This information may include details not only about the data activity itself but also community members' own rights, responsibilities, and options within an engagement. The aim is to give community members a clear, complete, and comprehensive understanding of the data space or other data project. As such, data space organizers must understand the general level of knowledge within the community they seek to engage with and avoid terms and jargon that is beyond their understanding. Simple messages, not complex ones, tend to be most effective.

As the name would suggest, informational mechanisms are a one-way flow of information from the project sponsors to those affected by it. There are no formal opportunities for feedback, nor for the community to express their own preferences. This lack of dialogue can be a problem if the community has objections to the approach or the provided information is too technical or difficult to understand. Pure informational approaches may also struggle to identify the degree to which their information has been received. While metrics like site traffic, flyers distributed can give an indication of what the project sponsor did, these do not indicate the degree to which community members read or digested the content.

Informational outreach can include:

NOTICES

Public notices refer to any written resource intended to explain a data initiative—including brochures, fact sheets, public notes, press releases, newsletters, web sites, social media posts and other content. As they are more likely to be scanned than thoroughly read, notices are best for short, concise summary of an issue or project.[57]

PURPOSE OR GOAL: Identify the purpose of this activity for the data space

Notices are most effective when they are about issues that are low salient or low importance as there is no guarantee that the materials will be read. Information should be clear and direct.

AUDIENCE: Map who the relevant parties for the data space are and their likely interests

Notices tend to be best for a general audience that needs to be informed of quick, clear facts (e.g. what data is being collected, for what purpose).

TIME AND RESOURCES: Assess the resources, readiness, capacity, and time available to launch a participatory data governance mechanism

Notices are often one of the easiest ways to engage with the public because they are cheap to produce. Costs consist of the cost of printing and mailing or, in the case of digital communication, digitally publishing that information. They can often be produced under short notice.

BRIEFINGS

Briefings are short presentations on a topic to a community or its representatives. They are often oral, though they may make use of visual aids (e.g. a slide deck). Briefings are often accompanied by a brief question-and-answer period, where individuals can ask follow-up questions about the information provided.

PURPOSE OR GOAL: Identify the purpose of this activity for the data space

Briefings are useful when there is a clear audience (e.g. a patients group) and agenda (e.g. explaining to those patients what their rights are in a data space). While briefings can be more detailed than notices, the information should still be concise and action-oriented. Data space organizers should ask themselves, “What information will be useful to this group? What do I expect the audience to do with this information?”

AUDIENCE: Map who the relevant parties for the data space are and their likely interests

Briefings are often best when they are designed for a clear set of stakeholders so that the organizer can know what topics might be of interest and which questions to prepare for. It is much easier to manage a smaller audience for a briefing than a large one.

TIME AND RESOURCES: Assess the resources, readiness, capacity, and time available to launch a participatory data governance mechanism

Briefings are a very low cost, taking less than an hour to deliver, and requiring minimal resources beyond that required to plan remarks or design any visual aids.

Consultative

LEVEL OF PUBLIC PARTICIPATION: Assess how much influence data space operators can share or delegate with the community

Consultative approaches involve inviting community members to share their own attitudes and opinions on a set of actions. They allow groups and individuals to express their opinions without any formal obligation to act upon it. They may be useful in the early stages of a data space launch, allowing for a data space's sponsor to receive feedback as a model is put into practice.

Consultative approaches are interactions that allow a data space organizer to gain insights about the community's attitudes. It is about asking questions from stakeholders, seeking to understand their perspectives and interests. Consultations can be done at various parts of a project. They can be done prior to a project's launch (to inform how the project sponsor approaches the work), during the work (as a feedback mechanism), or at the conclusion of a project (to improve the deployment of future initiatives). Effective consultations establish an ongoing dialogue where public feedback actively shapes policy development.

While consultations can be useful in increasing transparency between actors—allowing a dialogue that can allow each side to understand their interests—this participatory approach is often considered "minimal". It does not provide the ability for the community or citizens to engage with other stakeholders and does not provide the ability to be part of the decision-making process.

Consultative outreach can include:

PUBLIC MEETINGS

A public meeting is a virtual or in-person gathering convened by a project sponsor with a broad group of stakeholders. Public meetings may include a hearing (where a data space organizers testifies on their work and addresses questions from an institution's representatives), a townhall meeting (where a data space organizer answers questions from community members themselves), or a workshop (where a data organizer gathers the community to discuss specific topics and participate in hands-on activities).

PURPOSE OR GOAL: Identify the purpose of this activity for the data space

Public meetings offer a way for many different kinds of people to come forward to express their opinions without a set script or agenda. They are good for surfacing concerns, though they provide no formal means of defusing conflict.

AUDIENCE: Map who the relevant parties for the data space are and their likely interests

While public meetings can be any size, they are generally used for large gatherings with a broad group of stakeholders. The more diverse the group, the easier it is to understand competing interests and obligations.

TIME AND RESOURCES: Assess the resources, readiness, capacity, and time available to launch a participatory data governance mechanism

Public meetings may be resource-light but often require some preparation work to be successful. Organizers need to be able to ensure a safe space, where all people can speak comfortably, without concern of retaliation. They also need some degree of facilitation, so that those with the most power or the most domineering verbal style don't overwhelm others trying to participate.

INTERVIEWS AND FOCUS GROUPS

Interviews and focus groups refer to one-on-one conversations or small group discussions with stakeholders about a topic. These engagements are more resource intensive (the data space organizer is giving their full attention to one person at a time) but can provide a chance to get reactions and opinions in a small, tight-knit space.

PURPOSE OR GOAL: Identify the purpose of this activity for the data space

Interviews and focus groups are useful for allowing a project organizer to delve deeply into the attitudes of an individual or small group of individuals. Because they are private and involve intense interactions, they can often be useful in bolstering trust and defusing conflict.

AUDIENCE: Map who the relevant parties for the data space are and their likely interests

Focus groups and interviews are, by their nature, small. They are most effective when engaging with a highly knowledgeable group of community members or with community members otherwise empowered to speak on behalf of the larger whole.

TIME AND RESOURCES: Assess the resources, readiness, capacity, and time available to launch a participatory data governance mechanism

These types of civic engagement processes tend to be more resource intensive in that they require skilled facilitators/interviewers and preparation to identify and recruit participants. The engagements themselves can also be time-consuming and resource-intensive relative to the small audience they reach. As noted, the organizer is giving their full attention to one person or a small set of people at a time.

SURVEYS AND POLLING

Surveys and polls are form-based tools that ask input from a set of community members on a specific set of questions. Polls and surveys can be used to gather qualitative responses (e.g. asking participants to explain their attitudes in their own words) or quantitative responses (e.g. asking them to gauge their opinion based on a set of responses or rankings).

PURPOSE OR GOAL: Identify the purpose of this activity for the data space

Polls and surveys are useful for soliciting input from a large number of stakeholders asynchronously—which can be useful if the issue is low salience or the organizer is having difficulty convening all available parties.

AUDIENCE: Map who the relevant parties for the data space are and their likely interests

Surveys and polls are best to try and reach a large cross section of a general population (e.g. a large group of patients or doctors, an entire municipality). It may be useful to have an audience that has been previously engaged, as “cold calling” may lead to a lower participation rate.

TIME AND RESOURCES: Assess the resources, readiness, capacity, and time available to launch a participatory data governance mechanism

Good surveys require substantial time and resource investments to design compelling questions and format, identify an appropriate sample, secure feedback, and analyze results. The more complicated the analysis and the more people targeted, the greater the cost.

Deliberative

LEVEL OF PUBLIC PARTICIPATION: Assess how much influence data space operators can share or delegate with the community

Deliberative mechanisms involve inviting community members to negotiate with the data space sponsor and one another to advance their interests. They allow for community members to figure out trade-offs between different actions, come to decisions on their interests, and propose their own solutions. Deliberative mechanisms balance power between the data space operator and the community, giving the two parties space to express themselves and their respective solutions.

Deliberative engagements are an "intermediate" level of engagement. These mechanisms include efforts to provide communities and citizens with the opportunity to be a part of decision-making in the form of regular, ongoing conversations where they have the opportunity to express their interests, coordinate with other stakeholders, and develop their own proposed solutions. While decision-making rests in the hands of the project organizer, the expectation is that their actions will reflect the information and feedback given.

This approach allows not merely for organizers to understand the public's attitudes but to benefit from their skills, expertise, and insights as well. Individuals are called to draw on what they know and to serve as active participants in a discussion instead of passively responding to queries or completing forms. Though they do not require consensus, deliberative engagements can nonetheless allow participants to raise possible conflicts among themselves and the organizer and resolve them.

This format can allow for more robust and meaningful inputs but also requires solicited stakeholders to provide more time and effort to the engagement. As such, organizers may want to think critically about when and where to engage community members and on what. Excessive requests to participate in deliberative conversations can be exhausting, particularly if they do not involve highly salient or contentious issues.

Deliberative outreach can include:

DELIBERATIVE MINI-PUBLIC

A mini-public involves a small, randomly selected group of citizens who deliberate on issues and provide recommendations to inform public opinion and decision-making. Ideally, they are designed to be small enough for genuine deliberation while representative enough to ensure democratic engagement. They may be held in person or virtually.

PURPOSE OR GOAL: Identify the purpose of this activity for the data space

Mini-publics are useful when trying to secure a generally representative cross-section of a larger population and have them discuss their perspectives with one another. Mini-publics can make organizers aware of the issues important to interest groups that exist within a larger community, how those interest groups feel about one another, and the solutions they might suggest to resolve disputes. They can also bolster trust within a community, communicating that the project organizer is trying to solicit unvarnished opinions from the larger group instead of seeking input from participants they know will give them a green-light on their activities.

AUDIENCE: Map who the relevant parties for the data space are and their likely interests

A mini-public is not self-selected but recruited from a larger population. They are, to the extent possible, a randomly selected, representative group that reflects the diversity of the community they are selected from.

TIME AND RESOURCES: Assess the resources, readiness, capacity, and time available to launch a participatory data governance mechanism

Mini-publics are meant to stand in for a much larger population group but often involve more than 100 people.[58] Given the random selection, they often require some comprehensive database of the larger community that select participants can be drawn from. Recruiting a large number of people who are willing to participate in an extended or regular conversation with their peers, can take weeks if not months. Briefing participants, securing a space, and hosting the discussion can involve a substantial amount of resources.

DIGITAL CIVIC ENGAGEMENT PLATFORMS

Digital civic engagement platforms are a fusion of data-driven technologies and collective intelligence methodologies. These are platforms that allow community members to connect with one another, discuss issues of concern, develop collective responses to them, and (in some contexts) propose their own solutions.

PURPOSE OR GOAL: Identify the purpose of this activity for the data space

Digital civic engagement platforms are useful for engaging a large community over an extended period of time and fostering “consensus-building social networks”. They can quickly gather and synthesize large volumes of input that can be useful in identifying areas of agreement and disagreement, clustering opinion, and promoting productive dialogue.

AUDIENCE: Map who the relevant parties for the data space are and their likely interests

Civic engagement platforms are useful for large groups, such as the general public. Many successful deployments of these platforms have had thousands to tens of thousands of users. They are less effective if a particular subset of actors needs to be highlighted or elevated, as their inputs may get lost within the larger community.

TIME AND RESOURCES: Assess the resources, readiness, capacity, and time available to launch a participatory data governance mechanism

Digital civic engagement platforms are significant investments. While they can be facilitated over existing platforms (e.g. Slack, Microsoft Teams, Discord), most use dedicated, purpose-built platforms that persist for months if not years. Organizations pursuing a platform approach should also be aware of the need to moderate channels to promote safe spaces for participants. They will also need to conduct regular technical maintenance. Discussions that occur on the platform need to be matched with specific actions from the project sponsor, lest the platform no longer appear useful and relevant for participants.

ADVISORY BOARDS

Advisory boards—also known as committees, task forces, and groups—are a standing body made up of community members who are regularly solicited to provide comments and advice on a project. Boards may be appointed by data space sponsors or selected by the community itself (e.g. through an election, as designated representatives of larger institutions, or through some other means).

PURPOSE OR GOAL: Identify the purpose of this activity for the data space

Advisory boards are useful to raise the concerns of specific groups within the community and develop consensus-based recommendations. As the members of advisory boards tend to be senior members of their respective constituencies, they tend to possess some level of in-depth knowledge and expertise on a project or issue, which can be useful for developing substantive recommendations.

AUDIENCE: Map who the relevant parties for the data space are and their likely interests

As noted, advisory boards tend to be composed of senior representatives of certain subsets within a population. These representatives can speak on behalf of their organization or constituency.

TIME AND RESOURCES: Assess the resources, readiness, capacity, and time available to launch a participatory data governance mechanism

Advisory boards are long-term commitments. While individual meetings may be brief (and, indeed, can be self-organized by the board itself), organizers need to ensure that members are regularly briefed and aware of project updates. They may need to assist in the development of internal rules and processes (e.g. bylaws). They will also need to ensure that the input of the advisory board is, in some way, acted upon to ensure it does not get dismissed as a "rubber stamp" meant to legitimize actions the organizer was already planning to take.

Collaborative

LEVEL OF PUBLIC PARTICIPATION: Assess how much influence data space operators can share or delegate with the community

Collaborative mechanisms require giving community members explicit power and authority to make decisions about how others handle their data. They are explicitly empowered to set the agenda—even if the decisions they arrive at are not what the data space operator would pursue. These approaches tend to be most useful at the beginning or end of a project lifespan, to decide whether the effort should be maintained, what changes should be made, and whether any stakeholders' interests have shifted since discussions first began.

The final rung of engagement types are those engagement mechanisms where formal power is shared by members of the community and the project organizer. These groups agree to plan and take part in how a project is realized, collaborating with the project sponsor to figure out solutions. Alternatively, some amount of authority is delegated from the project organizer to the community itself in later stages of deployment, allowing the community to sustain work.

Collaborative processes are resource and time-intensive for the organizer and the community itself. While it offers the greatest opportunity for empowerment, that comes with a great level of responsibility. Organizers need to ensure that the way they delegate authority is done in a fair, legitimate, and inclusive manner while community members need to remain engaged long-term to ensure their interests are acted upon.

Collaborative outreach can include:

COLLABORATIVE INNOVATION AND CO-CREATION

Collaborative innovation and co-creation involve institutions engaging with a diverse yet carefully selected group of stakeholders to design policies and programs. Unlike mini-pub-

lics, which aim to represent a broad and statistically accurate cross-section of the population, these groups are specifically chosen for their expertise or interest in particular areas. Common kinds of collaborative innovation methodologies are hackathons, idea "boot camps", and various challenges and competitions.

PURPOSE OR GOAL: Identify the purpose of this activity for the data space

Collaborative innovation and co-creation is useful when trying to rapidly develop solutions to a specific problem.

AUDIENCE: Map who the relevant parties for the data space are and their likely interests

This engagement type is useful when there is a set of highly trained experts with a specialized knowledge of a particular field or sector.

TIME AND RESOURCES: Assess the resources, readiness, capacity, and time available to launch a participatory data governance mechanism

While collaborative innovation models can take place over a short period of time (a few hours to a week), they often require substantial preparation time. Participants also need some motivation for working on the problem, whether that be financial, recognition, or fulfillment of some other interest.

OVERSIGHT COMMITTEES

An oversight committee, as the name would suggest, is an institution empowered to oversee a project or organization and review its conduct. Committees may be empowered to conduct audits, manage service evaluation and redress mechanisms, make decisions on budgeting, and take other actions.

PURPOSE OR GOAL: Identify the purpose of this activity for the data space

Oversight committees are among the most significant accountability bodies that can be formed and are often done so with the support of a government agency. The goal is to not only ensure transparency but to reinforce a sense of community ownership. They may be particularly useful in contexts where there are very low levels of trust.

AUDIENCE: Map who the relevant parties for the data space are and their likely interests

Oversight committees consist of a small number of people, usually gathered from the general public or identifiable constituencies who have a particular interest in the success of the project. They may be elected or assembled with the support of a government institution.

TIME AND RESOURCES: Assess the resources, readiness, capacity, and time available to launch a participatory data governance mechanism

Oversight committees are highly intensive, requiring organizers cede some of their authority over project timelines, budgets, and staff. Oversight committees need to be able to look at all aspects of a project to be fully legitimate.

SOURCES AND FURTHER READING

Accountability Research Center. (2024). Participatory oversight institutions. https://accountabilityresearch.org/participatory_oversight_institutions

Ada Lovelace Institute. (2021). Participatory data stewardship: Principles, practices and policy options [Policy report]. https://www.adalovelaceinstitute.org/wp-content/uploads/2021/11/ADA_Participatory-Data-Stewardship.pdf

Agence Française de Développement. (2024). Participatory climate finance and the public policy dialogue (AFD Research Paper No. 76). https://www.afd.fr/sites/default/files/2024-03-10-51-48/RT_76_VA_2_BAT_Web.pdf

Agence Française de Développement. (2025). Towards a multidimensional definition of collective action in sustainable development and climate change (AFD Research Paper No. 78). https://www.afd.fr/sites/default/files/2025-05-01-53-37/RT_78_VA_BAT.pdf

Arnstein, S. R. (1969). A ladder of citizen participation. Journal of the American Institute of Planners, 35(4), 216–224. https://doi.org/10.1080/01944366908977225

International Association for Public Participation. (n.d.). IAP2 spectrum of public participation (evolution). https://www.iap2.org/page/SpectrumEvolution

Organisation for Economic Co-operation and Development. (2022). OECD guidelines for citizen participation processes. OECD Publishing. https://www.oecd.org/en/publications/2022/09/oecd-guidelines-for-citizen-participation-processes_63b34541.html

U.S. Environmental Protection Agency. (n.d.). Public participation guide: Introduction to the guide. https://www.epa.gov/international-cooperation/public-participation-guide-introduction-guide

APPENDIX IV

List of Governance Instruments in Data Spaces

1. PURPOSE AND SCOPE

This appendix provides an overview of the governance instruments that are commonly used to design, operate, and oversee data spaces. It is intended as a reference for data space operators, governance authorities, and policymakers who are responsible for translating governance principles into concrete, enforceable arrangements.

The appendix catalogs the main legal, organizational, technical, and procedural instruments through which data space governance is implemented in practice. For each instrument, it describes its function and summarizes its current status within the Swiss data ecosystem

2. SOURCES AND ANALYTICAL FRAMEWORK

This appendix draws on two primary sources that provide complementary perspectives on data space governance.

First, it builds on the **Data Space Playbook – Governance Guideline** developed by Beyond Civic. The Guideline offers a detailed framework for governing data spaces in Switzerland and similar decentralized contexts. It emphasizes federated governance, neutrality, interoperability, and adaptability, and introduces key governance artefacts such as rulebooks, participation agreements, and governance authorities. This appendix follows the Guideline's classification of governance instruments and uses it as the main reference for describing how these tools function within Swiss data spaces.[59]

Second, the appendix incorporates relevant elements from the **UN Broadband Commission's Data Governance Toolkit**, which provides an international, cross-sector perspective on operational data governance. The Toolkit organizes governance around functional mechanisms across the data lifecycle, including stewardship, contractual tools, standards, audit, and capacity-building. These mechanisms complement the Beyond Civic framework by highlighting operational and institutional considerations that support long-term trust and sustainability.[60]

Where relevant, both sources are aligned with the structure of the Swiss Data Ecosystem and its Data Space Building Blocks, which adapt the Data Spaces Support Centre (DSSC) model to the Swiss context.

3. GOVERNANCE TOOLS FOR DATA SPACES

3.1. FOUNDATIONAL GOVERNANCE AND PARTICIPATION

This category covers the instruments that create the basic structure of a data space. They define its purpose, its legal form, who may join, and the rules that govern participation. These tools provide the backbone for accountability, transparency, and meaningful involvement of all actors, including patients and public-interest groups in the health domain.

3.1.1. Rulebook

Governance Instrument	Purpose / Function	How It Enables Digital Self-Determination (DSD)	Key Leverage Points (Systemic Interventions)
Rulebook (Beyond Civic)	Central reference defining participation, interoperability, and accountability	Clarifies rights and responsibilities, ensuring patient agency, consent, and transparency	**Organisational Form & Governance Authority Building Block:** Co-create the rulebook with patient councils and hospital consortia; embed "feedback loops" so user concerns update governance clauses dynamically

The rulebook is the central governance framework of a data space. It sets the fundamental rules for the design of data spaces so that actors can know what constitutes participation and what duties they are responsible for fulfilling. A rulebook should be developed collaboratively so that all parties have ownership of the governance framework. In a health data space, this could mean working directly with patient councils and hospital consortia.

A rulebook does not need to take the form of a single document; it is better understood as a set of linked reference materials that together define participation rules, roles and responsibilities, interoperability expectations, and contractual arrangements. In the DSSC Blueprint, the rulebook brings together the outputs of the broader governance framework by specifying semantics, business and financial rules, contractual conditions, and decision-making structures.[61] It is overseen by the DSGA and is binding on all participants. Because organizations may join several data spaces, they may need to comply with multiple rulebooks—some general, others domain-specific. This structure supports DSD by making rights, duties, and decision points explicit, helping participants understand both the scope of their commitments and the agency available to them.

The *Guideline* places rulebooks within an international landscape and references models such as the SITRA Rulebook, the IDSA Rulebook, and the DSSC Blueprint. While these offer solid foundations, Beyond Civic argues that they do not fully address the needs of cross-border or cross-sector collaboration, especially in public-private settings. Its own reference documents are therefore tailored to Swiss law and designed to operate as a coherent set.

Switzerland does not yet have a national rulebook template. Beyond Civic notes that a Rulebook for Data Collaboratives is in development, but for now, high-level ecosystem tools, such as the Code of Conduct for Trustworthy Data Spaces, the Role Model of Actors, and the Swiss Data Ecosystem Building Blocks, provide the basic scaffolding.[62] These set principles and interoperability requirements but do not replace full rulebooks, which will need to be designed and adopted.

3.1.2. Statutes / Articles of Association

Governance Instrument	Purpose / Function	How It Enables Digital Self-Determination (DSD)	Key Leverage Points (Systemic Interventions)
Statutes / Articles of Association	Foundational legal document of governance authority	Embeds participatory governance and accountability	**Organisational Form & Governance Authority Building Block:** Reserve board seats for patient or public representatives; require annual participatory review of statutes

Statutes or Articles of Association form the core legal foundation when a data space is constituted as its own legal entity. They set out the initiative's purpose, define membership rights and obligations, and specify how governance bodies operate. As described in the DSSC Blueprint, statutes are one form of founding agreement: they establish the governance authority, regulate admission and exit, clarify responsibilities and liabilities, and set the rules for collective decision-making.[63]

If a separate legal entity is not required, comparable instruments—such as consortium, joint venture, or cooperation agreements—can fulfill the same function. Regardless of format, a founding agreement must identify initial members, detail the governance model, and outline how new participants can join. Statutes provide the most comprehensive framework by supporting onboarding and codifying binding conditions for participation.

Statutes offer several levers for embedding DSD. They can mandate participatory governance, require representation of affected groups, and introduce periodic reviews to reassess mandates, responsibilities, or accountability mechanisms.

In Switzerland, statutes are typically drafted under national association law and tailored to the organizational form selected for the data space's governance authority. Because statutes govern a specific entity rather than the ecosystem as a whole, each data space must develop its own founding document. The Beyond Civic Governance Guideline notes that a standardized Swiss template is under development to support future implementations.[64]

3.1.3. Membership Application / Accession Agreement

Governance Instrument	Purpose / Function	How It Enables Digital Self-Determination (DSD)	Key Leverage Points (Systemic Interventions)
Membership / Accession Agreement	Formal onboarding and compliance commitment	Ensures new entrants respect DSD principles and transparency	**Regulatory Compliance Building Block:** Add a "Digital Self-Determination Pledge" and periodic member re-certification audits

The Membership Application or Accession Agreement is the instrument through which new participants formally join a data space. It anchors the onboarding process by requiring applicants to accept the statutes or founding agreement and to comply with the governance structures, standards, and operational rules defined in the rulebook. By aligning newcomers with the obligations and rights of existing members, the agreement creates a consistent and predictable participation framework.

Because it outlines both commitments and entitlements, the agreement can also reinforce DSD. For example, it can clarify participant rights relating to transparency and agency, or introduce a DSD-aligned commitment that members periodically renew as part of ongoing compliance checks.

In the DSSC Blueprint, accession agreements sit within the onboarding process managed by the Data Space Governance Authority (DSGA). Applicants are assessed for legal, technical, and organizational readiness; once approved, they receive a membership credential that can also support cross-space federation and simplified onboarding elsewhere.

In Switzerland, a membership application template tailored to national law exists and can be adapted for different member categories, though no standardized version has yet been issued for ecosystem-wide adoption.[65]

3.2. CONTRACTUAL MECHANISMS

Contractual mechanisms provide the legal backbone for data collaboration. They define rights, obligations, permissible uses, and liability, turning governance principles into binding commitments. As such, they are one of the clearest routes for operationalizing DSD, by making transparency, consent, reciprocity, and redress legally enforceable.

Beyond allocating responsibility, contracts influence incentives, define permissible reuse, and embed governance safeguards. Tools such as the Contractual Wheel of Data Collaboration, developed by The GovLab, split agreements into modular elements (purpose, data type, access rights, retention periods, dispute mechanisms), helping organizations tailor protections while maintaining consistency and fairness.[66]

Contractual mechanisms cover a broad family of instruments: DSAs, Memorandums of Understanding (MOUs), Service-Level Agreements (SLAs), End-User License Agreements, platform terms of service, and API usage policies. They operate both at the institutional level, binding participants to the governance framework, and at the transactional level, governing individual data exchanges.

3.2.1. General Terms & Conditions

Governance Instrument	Purpose / Function	How It Enables Digital Self-Determination (DSD)	Key Leverage Points (Systemic Interventions)
General Terms & Conditions (GTCs)	Baseline legal framework for joining and operating the data space	Codifies rights to access, portability, withdrawal, and complaint mechanisms	**Contractual Framework Building Block:** Integrate social license and "DSD impact assessments" at renewal cycles to adjust terms with evolving norms

The General Terms and Conditions (GTCs) form the core contractual framework that participants must accept to join and remain in a data space. In the Governance Guideline, GTCs set out the conditions for fair, transparent, and legally compliant participation. They explain how the arrangement aligns with applicable law (such as GDPR or national data protection rules) and outline procedures for decision-making, membership, and dispute resolution. They also help operationalize DSD by making explicit the rights stakeholders can exercise, including access, portability, withdrawal, and complaint mechanisms.

In the *DSSC Blueprint*, GTCs sit within the Contractual Framework building block, alongside founding and accession agreements (see Figure 3). These agreements formalize the relationship between the governance authority and participants by translating components of

the governance model into enforceable obligations. They define participant roles (governance authority, data providers, users, and service providers), set admission and exit criteria, and codify rules for intellectual property, confidentiality, data protection, cybersecurity, and interoperability. They also provide a vehicle for embedding community-driven requirements, such as renewal cycles that update terms in line with evolving norms or expectations.

GTCs can extend beyond institutional governance to the transaction level by providing standardized clauses and licensing models for data product contracts. This alignment across layers supports consistent and predictable interactions within a data space. In Switzerland, no national-level GTC template has yet been published

Figure 3: Structure of Contractual Framework building block

Three types of agreements give the governance framework legally binding form

Institutional agreements

PARTIES	Data space governance authority ↔ each participant / member
FUNCTION	Legal implementation of the governance framework (Rulebook)
EXAMPLE INSTRUMENTS	Founding agreement · General terms & conditions

Data sharing agreements

PARTIES	Data space participants / members, between one another
FUNCTION	Legal implementation of the governance framework between participants
EXAMPLE INSTRUMENTS	Data product contract

Service agreements

PARTIES	Data space governance authority ↔ service provider
FUNCTION	Contracting of services for data space functionality
EXAMPLE INSTRUMENTS	Defined per data space (e.g., service-level agreements)

Source: Data Spaces Support Centre,Contractual framework.[67]

3.2.2. Data Sharing Agreements

Governance Instrument	Purpose / Function	How It Enables Digital Self-Determination (DSD)	Key Leverage Points (Systemic Interventions)
Data Sharing Agreements (DSAs)	Define rights and duties in data exchange	Operationalize consent, reciprocity, and proportionality	**Access & Usage Policies Enforcement Building Block:** Integrate smart-contract or API-based consent tracking; enforce reciprocity (benefit-sharing) clauses

A Data Sharing Agreement (DSA) sets the contractual terms for exchanging data within a data space. It defines rights of use, restrictions, and obligations, ensuring that exchanges follow the governance framework established in the rulebook. DSAs reduce uncertainty, clarify accountability, and support trust across participants by addressing legal, organizational, semantic, and technical aspects of sharing. They also can advance DSD by formalizing how parties communicate consent, apply proportionality, and, where appropriate, commit to reciprocal exchanges of value or insight.

In Switzerland, the Swiss Federal Institute of Intellectual Property (IPI) has issued standardized model agreements, developed by id est avocats (2024) at the request of the Federal Council. These templates aim to lower barriers, especially for SMEs, by providing ready-to-use contracts.[68] They apply to non-personal "technical data" (machine data, environmental data, anonymized statistics) and explicitly exclude personal or mixed datasets unless fully anonymized.

The IPI provides four templates covering different sharing scenarios:

Agreement for the Transfer of Technical Data (Unilateral, ad hoc)

- For one-time transfers such as test datasets or pilot projects.
- May be free or fee-based
- Allows providers to impose use restrictions (e.g. no resale or onward sharing)
- Data provided "as is," without warranty on quality or fitness
- Includes confidentiality and baseline compliance clauses

Subscription Agreement for Access to Technical Data (Unilateral, ongoing)

- For continuous or regular access (e.g. via API or portal)
- May involve subscription fees; for SMEs, fees cannot exceed the provider's cost of making the data available
- Provider may set use restrictions and retain audit rights
- Access is non-exclusive

Agreement for the Exchange of Technical Data (Mutual, bilateral)

- For reciprocal sharing arrangements
- Access is typically free of charge
- Parties may agree whether to share results generated from the data
- Includes confidentiality and compliance obligations
- Optional audit rights for verifying adherence to restrictions

API Terms of Use

- Specifies conditions for technical access through an API
- Defines licensed uses and restrictions (e.g. no harmful activity, no exceeding quotas)
- Allows suspension or termination for breach
- Often used alongside one of the above agreements to govern the access mechanism itself

All four model agreements use electronic templates and checkbox structures to simplify adoption and support consistency across actors. They also anticipate alignment with European regulatory development, including interoperability expectations under the EU Data Act, facilitating cross-border technical and legal compatibility.

3.2.3. Licensing

Governance Instrument	Purpose / Function	How It Enables Digital Self-Determination (DSD)	Key Leverage Points (Systemic Interventions)
Licensing	Define data reuse permissions and obligations	Balances openness with control and attribution	**Contractual Framework Building Block:** Adopt dynamic licenses (e.g., time-limited or community-benefit clauses) for health-data reuse

Licensing mechanisms define the permissions, restrictions, and obligations that govern how data may be reused or redistributed. They clarify what recipients may do with data—copy, transform, analyze, commercialize, or share it further—and help balance openness with protection. Licensing is a key tool for making governance rules enforceable across the data lifecycle and can embed DSD by linking reuse conditions to safeguards such as time limits, attribution, or community-benefit provisions.

While licenses and DSAs both define rights and limits, they operate at different levels:

- **Licenses** specify permissible uses once access has been granted.
- **DSAs** define the broader exchange relationship, including roles, liability, transfer conditions, and interoperability requirements.

The IPI model agreements incorporate licensing in several ways. The API Terms of Use grant a revocable right to integrate and display data through an API while distinguishing between data access (via a DSA) and data use (via license conditions). The Data Transfer, Subscription, and Data Exchange Agreements each include a *Limited License* clause that grants a non-exclusive right to use the covered data for the agreed purpose and term, without transferring ownership. They also allow for *Additional Terms*, such as separate API licenses or platform terms of service, that govern the tools used for exchange. Interoperability provisions require dataset content, use restrictions, licensing terms, and data quality to be described clearly enough for recipients to find, access, and reuse the data effectively.

3.3. POLICIES, STANDARDS, AND SHARED LANGUAGE

This category includes the governance tools that define the shared expectations—ethical, procedural, semantic, and organizational—that make a data space legible, trustworthy, and interoperable. These instruments set the normative and interpretive foundations for collaboration, providing the common language and value commitments that other governance tools rely on.

3.3.1. Policies and Guidelines

Governance Instrument	Purpose / Function	How It Enables Digital Self-Determination (DSD)	Key Leverage Points (Systemic Interventions)
Policies & Guidelines	Convert high-level principles into operational policies	Create shared ethical reference points	**Regulatory Compliance Building Block:** Mandate DSD alignment assessments for every new data initiative under DigiSanté

Policies and guidelines translate broad governance principles into day-to-day expectations for responsible data management. They can take many forms, including open data policies, AI ethics frameworks, data responsibility guidelines, and human-rights-aligned principles such as OECD Data Ethics Principles, the UN CEB Principles, and FAIR/CARE. These instruments provide common ethical anchors and can delineate how concepts like DSD should inform decision-making. Organizations can also use policy to require DSD-alignment assessments when launching new data initiatives.

Across the data lifecycle, institutional policies shape standards for privacy, consent, interoperability, quality, and inclusion. Sector-specific frameworks, such as the WHO Data Principles or the Pan-American Health Organization's governance guidance, illustrate how high-level values are translated into operational practice. Additional reference points

from ITU, UNDP, UNESCO, and ASEAN help promote consistent and adaptive governance across jurisdictions.[69]

In Switzerland, the *Code of Conduct for the Operation of Trustworthy Data Spaces* and the *Swiss Data Ecosystem Building Blocks* serve as the central anchors. Together, they provide shared expectations for transparency, trust, interoperability, and responsible behavior.

3.3.2. Code of Conduct

Governance Instrument	Purpose / Function	How It Enables Digital Self-Determination (DSD)	Key Leverage Points (Systemic Interventions)
Code of Conduct for Trustworthy Data Spaces	Defines ethical and behavioral norms for participants	Institutionalizes fairness, transparency, and user control beyond legal minimums	**Participation Management Building Block:** Create public dashboards tracking adherence; enable citizen reporting mechanisms (bottom-up feedback loops)

A code of conduct (CoC) sets out the cultural and normative expectations that guide behavior within a data space. It articulates shared values, defines expectations for both the governance authority and participants, and strengthens trust by establishing standards that go beyond statutory obligations. CoCs are well suited to expressing general goals, principles, and indicators that can then be monitored by the public or civil society.

In Switzerland, this approach has been formalized through the *Code of Conduct for the Operation of Trustworthy Data Spaces*, approved by the Federal Council in December 2023 following consultation with government, industry, academia, and civil society.[70] The Code defines four guiding principles—transparency, control, fairness, and effectiveness—supported by recommended measures for governance authorities, intermediaries, providers, and users.

- **Transparency** calls for accessible documentation, organizational openness, clear and comprehensible information, provenance traceability, and machine-readable metadata.
- **Control** covers mechanisms for managing data use, oversight of transfers outside the space, voluntary participation, and security risk management.
- **Fairness** emphasizes proportionality, non-discrimination, balancing of interests, high data quality to prevent bias, and protections for children and young people.
- **Effectiveness** focuses on implementation, interoperability, agility, and ecological, social, and economic sustainability.

The Code also promotes peer exchange among providers and requires organizations to publish periodic reports on their implementation progress.

3.3.3. Standards and Vocabulary

Governance Instrument	Purpose / Function	How It Enables Digital Self-Determination (DSD)	Key Leverage Points (Systemic Interventions)
Standards and Vocabulary (Toolkit)	Ensure interoperability, quality, and shared understanding	Promotes clarity on data meaning, access, and rights	**Data, Services & Offerings Descriptions (Building Block):** Require machine-readable usage conditions and provenance metadata in all offering descriptions

Standards and shared vocabularies make governance rules executable across systems. Common protocols and definitions reduce friction, support quality, and enable secure re-use. Examples include ISO 27001 for information security and DCAT for cataloguing. The Toolkit highlights interoperability, metadata discipline, and portability as foundations for trustworthy data exchange.

In the Swiss context, the *Swiss Data Ecosystem Building Blocks* specify FAIR-aligned, DCAT-structured catalogs and federated publication practices linked to national assets such as i14y (federal API/interoperability platform), LINDAS (Linked Data Service), and opendata.swissswiss. Offering descriptions should include machine-readable access and usage controls, provenance information, and quality attributes expressed through ODRL and related standards.[71] Offering descriptions could improve DSD through machine-readable access and usage controls, provenance information, and quality attributes (via ODRL and related standards).

The SwissHDS adopts a standardized data model, a national interoperability layer, and FHIR-compatible formats to support consistent communication across healthcare systems.[72]

3.3.4. Glossary

Governance Instrument	Purpose / Function	How It Enables Digital Self-Determination (DSD)	Key Leverage Points (Systemic Interventions)
Glossary & Role Model	Establishes shared terminology and minimal roles	Reduces ambiguity, clarifies who safeguards users' interests	**Data, Services & Offerings Descriptions Building Block:** Continuously update the glossary through multi-stakeholder input (patients, hospitals, insurers) to align language with DSD values

A glossary provides a common vocabulary for how a data space operates. It standardizes key terms, reduces ambiguity, and helps participants interpret governance rules, technical standards, and roles in a consistent way. Clear terminology lowers onboarding barriers, supports interoperability, and helps participants understand how responsibilities are distributed. Because language shapes expectations, a glossary can also advance DSD by making concepts transparent and accessible, especially for smaller actors.

Glossaries may be ecosystem-wide—such as those included in the DSSC Blueprint or IDSA Rulebook—or tailored to a specific data space.

In Switzerland, no standalone glossary exists yet, but two instruments partially fulfill this function. The *Data Space Building Blocks – Swiss Data Ecosystem* define core components of a data space and their interdependencies. The *Roles in the Swiss Data Ecosystem* document provides a minimal role model, clarifying the tasks, competencies, and responsibilities necessary for the operation of data spaces and their coordination within the national ecosystem. It outlines six essential roles: data providers, data users, intermediaries/brokers, service providers, the Contact Point, and Communities of Practice. Together, these documents create a baseline for interoperability and help distribute responsibilities in a consistent way.

3.4. TECHNOLOGY & GOVERNANCE BY DESIGN

Governance Instrument	Purpose / Function	How It Enables Digital Self-Determination (DSD)	Key Leverage Points (Systemic Interventions)
Technology & Governance by Design	Embed safeguards and controls into system architecture	Hard-codes privacy, consent, and accountability	**Access & Usage Policies Enforcement Building Block:** Integrate federated learning, PETs, and continuous DSD compliance monitoring as system defaults

Governance by design embeds safeguards directly into the technical architecture so that compliance, accountability, and user protection are built into system behavior rather than added through policy alone. Core measures include privacy-enhancing technologies (PETs) such as differential privacy, homomorphic encryption, secure multi-party computation, and synthetic data; federated learning; encryption; role-based access controls; and technical protection measures that enforce rules at the infrastructural level. These are supported by operational controls such as provenance tracking, audit trails, multi-factor authentication, secure deletion, and continuity procedures.

Privacy-by-design complements these measures by applying data minimization, encryption or anonymization at the point of collection, consent management, and early bias detection.

In Switzerland, the clearest illustration is the SwissHDS under the DigiSanté program. Its reference architecture adopts a Zero Trust approach based on NIST SP 800-207, requiring authentication, authorization, and logging for every access request. It also provides common governance services—authentication, consent management, authorization, pseudonymization, and secure logging—as shared components within the infrastructure. These elements operationalize governance through the system itself, reducing reliance on manual enforcement and helping align technical behavior with emerging DSD expectations.[73]

3.4.1. Data Network Description

Governance Instrument	Purpose / Function	How It Enables Digital Self-Determination (DSD)	Key Leverage Points (Systemic Interventions)
Data Network Description	Describes architecture, mechanisms, and standards of data access.	Clarifies how data moves and who is involved	**Provenance & Traceability Building Block**: Publish a machine-readable data flow map; include a public summary of intermediaries, access points, and controls.

The Data Network Description defines the architecture of a data space by outlining its components, participants, and data exchange mechanisms. It explains how data sharing is technically and organizationally arranged, including transfer methods, applied standards, and trust and accountability structures. By making data flows explicit, it can support DSD by giving participants a better understanding of how data travels, which entities handle it, and where decisions occur.

3.4.2. Interoperability Specifications

Governance Instrument	Purpose / Function	How It Enables Digital Self-Determination (DSD)	Key Leverage Points (Systemic Interventions)
Interoperability Specifications	Define semantic and technical standards	Enable user portability and system-to-system autonomy	**Provenance & Traceability Building Block**: Standardize APIs for real-time consent revocation and data traceability (auditable provenance chain)

Interoperability Specifications set the technical, semantic, organizational, and legal standards that allow participants to exchange data securely and consistently. They define how systems communicate, how data is structured, and how compliance with shared rules is verified. These specifications provide the basis for cross-organizational compatibility and support portability across domains.

Interoperability can also operationalize DSD. When systems offer standardized APIs that support real-time consent withdrawal or provide traceability of data uses, individuals gain practical means to monitor and influence how their data is handled.

3.5. TRUST, OVERSIGHT, AND COMPLIANCE

Trust, oversight, and compliance mechanisms provide the assurance layer that keeps a data space dependable and legitimate over time. These instruments clarify who is responsible for safeguarding data, verify that governance rules are followed, and make sure outsourced or third-party systems meet the same expectations as the data space itself. They reinforce accountability, reduce risk, and create the operational feedback loops that support evolving DSD expectations.

3.5.1. Data Stewardship & Institutional Arrangements

Governance Instrument	**Purpose / Function**	**How It Enables Digital Self-Determination (DSD)**	**Key Leverage Points (Systemic Interventions)**
Data Stewardship & Institutional Arrangements	Assign roles for data quality, trust, and compliance	Ensures continuous oversight and representation	**Organisational Form & Governance Authority Building Block:** Expand on the roles of *Data Stewards and Custodians* as fiduciaries for citizens; establish a federation of stewards

Data stewardship and institutional arrangements determine who is responsible for data quality, compliance, and coordination within a data space. Clear stewardship roles strengthen accountability and create a human layer of governance that complements technical and legal controls.

In Switzerland, the *Roles in the Swiss Data Ecosystem* document identifies two key stewardship-related roles:

- **Data Custodian**: Responsible for storing, maintaining, and securely transmitting data in line with instructions from the data steward. This role can sit within a data provider or be outsourced to intermediaries
- **Data Steward**: Responsible for harmonizing and standardizing data within an organization, implementing quality and security measures, and coordinating with internal governance bodies.

The Contact Point supports these functions by coordinating roles across domains. These arrangements create the conditions for ongoing oversight and, especially if strengthened, could support DSD through fiduciary-like responsibilities on behalf of affected groups.

3.5.2. Audit & Compliance Mechanisms

Governance Instrument	Purpose / Function	How It Enables Digital Self-Determination (DSD)	Key Leverage Points (Systemic Interventions)
Audit & Compliance Mechanisms	Verify adherence, detect misuse, assure trust	Builds transparency and accountability loops	**Organisational Form & Governance Authority Building Block:** Introduce independent DSD audits feeding directly into rulebook revisions

Audit and compliance mechanisms help verify that governance rules are carried out in practice. They provide transparency on how obligations are met, identify risks or breaches, and support continuous improvement. Over time, audits can create feedback loops that strengthen DSD by prompting revisions in response to transparency or accountability gaps.

Relevant Swiss Data Ecosystem Building Blocks highlight this function across several areas:

- **Organisational Form & Governance Authority**: Calls for guidelines and monitoring mechanisms, including audit procedures and possible certification.
- **Provenance & Traceability:** Specifies the need to log actions performed on data (e.g., use, modification, consent changes) and to define retention and access rules.
- **Regulatory Compliance**: Emphasizes ongoing identification of applicable laws, implementation of safeguards, and (where appropriate) providing tools and support services to help participants meet regulatory obligations.
- **Trust Framework:** Highlights trust anchors, transparency logs, and verification

mechanisms to validate participant credentials.

3.5.3. Procurement & Vendor Management

Governance Instrument	Purpose / Function	How It Enables Digital Self-Determination (DSD)	Key Leverage Points (Systemic Interventions)
Procurement & Vendor Management	Integrate governance requirements into sourcing and outsourcing	Aligns external providers with DSD, privacy, and interoperability standards	**Contractual Framework Building Block**: Embed standard DSD, portability, and audit clauses in framework contracts and public tenders

Procurement and vendor management integrate governance requirements into the sourcing of external systems, services, and technologies. They help prevent gaps between internal policy and outsourced implementation by requiring suppliers to meet standards for security, privacy, interoperability, auditability, and data portability. Contract terms can include audit rights, minimum logging and metadata requirements, and clear conditions for continuity and exit. In this way, procurement can extend DSD protections to third-party components by embedding safeguards for consent, transparency, and user control.

3.6. TRAINING & CULTURAL CHANGE

Governance Instrument	Purpose / Function	How It Enables Digital Self-Determination (DSD)	Key Leverage Points (Systemic Interventions)
Training & Cultural Change	Build capacity and literacy for responsible data use	Enables individuals to understand and exercise control	**Participation Management Building Block:** Embed DSD literacy in medical, policy, and citizen training curricula to shift norms and behaviors

Training and cultural change mechanisms build the human and organizational capability needed for governance frameworks to function effectively. Technical and legal tools rely on a culture of responsibility, literacy, and ongoing learning. Embedding DSD concepts into training can help individuals understand their rights, exercise control, and set expectations for transparency and accountability. Over time, these practices influence norms and support more participatory governance cultures.

APPENDIX V

Model Swiss Data Sharing Agreement with Digital Self-Determination Clauses

This appendix reproduces an existing IPI Subscription Agreement for Access to Technical Data (Unilateral) and illustrates how considerations related to Digital Self-Determination can be reflected within an established contractual framework. The clauses in orange were added as part of this project to demonstrate how DSD-aligned governance elements such as transparency, purpose limitation, accountability, and review mechanisms can be embedded in data sharing agreements. Text shown in blue and red originates from the original IPI template and has not been substantively altered.

This model is provided as a reference example to support data space operators and legal teams in exploring how DSD considerations may be translated into contractual practice. While the example focuses on a subscription agreement for access to technical data, similar adaptations could be made to the other IPI template agreements for data exchange and data transfer.

IPI – Subscription Agreement (commented)

VERSION: OCTOBER 2023

SUBSCRIPTION AGREEMENT FOR ACCESS TO TECHNICAL DATA (UNILATERAL)

COVER SHEET

Date	[date]
Data Holder	[name / company name / address] Contact: [name] [email address]
Data Recipient	[name / company name / address] Contact: [name] [email address]
Designated Data Steward / Contact Point	Name, function, and email of the Data Holder's Data Steward. Name and email of the Data Recipient's operational contact.
Context Change Review	[Yes/No: Parties intend to use the Context Change Review mechanism. Frequency (if any): annually / upon notice only.]
Covered Data	[describe the Data to which Data Recipient shall have access under this agreement, including documentation relating to such Data, their format, etc.]
Access	[specify the platform on which the Data Recipient subscribes to obtain regular access to the Covered Data or the API made available to the Data Recipient to allow access to the Covered Data, or any other technical means by which access will be provided]

Subscription Term and Notice	[specify the duration of the initial term for which the Data Recipient subscribes, e.g. 1 month, 1 year, etc.] Termination Notice: [*specify the duration of the advance notice that must be given to terminate the agreement, e.g. 1 week, 1 month, etc. – it must be shorter than the Term*]
Subscription Fee	[select an option and insert the amount and recurrence of the Subscription Fee if access is granted against a fee] [Alt.1] CHF [insert price] [+ taxes] of [yearly] / [quarterly] / [monthly] Subscription Fee [Alt.2] Free
Use Restrictions	[specify the restrictions that will apply to the use of the Covered Data; multiple boxes may be checked] No Commercial Use of the Covered Data No Commercial Use of the Results No Distribution of the Covered Data No Distribution of the Results Research-only Internal use only

1. DEFINITIONS

The capitalized terms in this Agreement have the following meanings:

Commercial Use	any use of the Covered Data and/or of the Results by the Data Recipient or a Downward Recipient that is primarily intended towards a monetary compensation or commercial advantage.
Confidential Information	any proprietary and/or non-public information provided by either party, in particular but not limited to trade secrets or know-how or other related proprietary business information and data, whether such information is provided in tangible or intangible form, written, oral, graphic, pictorial or recorded form or stored on computer discs, hard drives, magnetic tape or digital or any other electronic medium.

Context Change	any material change in the intended use or purpose of the Covered Data, in the technical or societal environment in which the Covered Data is used, or in the risks, impacts, or expectations associated with such use, including new foreseeable effects on individuals, groups or communities represented in or affected by the Covered Data.
Covered Data	any Data made available under this Agreement as defined on the cover sheet, to the exclusion of any communication Data automatically generated by the parties for the purpose of allowing the Data Recipient to access the Covered Data.
Data	any digital representation of acts, facts or information and any compilation of such acts, facts or information, to the exclusion of Personal Data, of any type and in any format.
Data Steward	the individual or individuals designated by each Party as responsible for overseeing responsible data practices, reviews alignment with Digital Self-Determination principle, and serving as the primary point of contact for all notices, concerns, or matters relating to the responsible use, governance, review, or modification of the Covered Data.
Digital Self-Determination	the principle that individuals, groups or communities whose interests may be affected by the Covered Data retain agency, clarity and control over how such data is accessed, used, shared and interpreted. This includes transparency regarding the Covered Data and its use, contextual purpose limitation, the ability to review or request modification of certain uses if risks change, and where appropriate the involvement of relevant stakeholders in governance or review processes.
Distribute	make all or part of the Covered Data available to third parties in unmodified form or in such modified form that would still allow such third party to retrieve the original Covered Data.
Downward Recipient	any person or entity to whom the Covered Data is made available by the Data Recipient, directly or indirectly.
Harm or Misalignment	any use, effect, or outcome of the Covered Data or the Results that contradicts the legitimate expectations, interests, or rights of individuals, groups or communities represented in or affected by the Covered Data, including newly emerged risks not reasonably foreseeable at the time of the Agreement. It triggers the review/mitigation mechanisms in this Agreement and is not a stand-alone restriction outside the agreed process.
Intellectual Property Rights	all intellectual property rights, whether registered or not, and anchored in either national or international law, in and to the Covered Data, including without limitation copyright, trademark right, patent right and database right.

Interoperability	the ability of two or more data spaces or communication networks, systems, products, applications or components to exchange and use Data in order to perform their functions.
Personal Data	any data or information relating to an identified or identifiable person within the meaning of article 3 let. a of the Swiss Data Protection Act (DPA – RS 235.1).
Restrictions	the restrictions on use specified on the cover sheet.
Results	any results obtained, developed, created or improved by the Data Recipient based on its use of the Covered Data.

2. GENERAL PROVISIONS

2.1 Access. Subject to the terms of this Agreement, the Data Holder grants the Data Recipient access to the Covered Data in accordance with the access modalities set forth on the cover sheet for the Term, in the format set forth on the cover sheet. Access to the Covered Data includes access to any updates of such Covered Data or newly collected Covered Data, if any. To support Digital Self-Determination, the Data Holder shall provide, in a clear and accessible manner, the information reasonably necessary for the Data Recipient to understand the structure, limitations, provenance and context of the Covered Data, including any known impacts the Covered Data may have on identifiable groups or communities.

[**Drafting comment:** "Reasonably necessary" becomes not subjective or vague: it refers only to the information specified in the Cover Sheet, the defined terms in Section 1, the elements expressly listed in this clause (structure, limitations, provenance, context and known impacts), and the Data Holder's existing documentation and actual knowledge. It is therefore a limited, evidence-based standard and not an open-ended obligation.]

2.2 Subscription Fee. [Alt.1] Access to the Covered Data is provided against payment of the non-refundable Subscription Fee, payable in advance and at the frequency mentioned on the cover sheet. [Alt.2] No Subscription Fee shall be charged to provide access to the Covered Data and each party shall bear its own costs relating to implement and maintain the relevant tools allowing for such access.

[**Comment:** select Alt.1 if the access is granted against payment of a fee and Alt.2 if access is granted for free.]

[**DSD addition (optional)**: Upon request, the Data Holder shall provide a short explanation of the elements composing the Subscription Fee to support transparency and informed decision-making.]

2.3 [Fee Calculation. The Subscription Fee shall not exceed the costs directly related to making the Covered Data available to the Data Recipient.]

[**Drafting comment:** section 2.3 reflects the principle applicable under art. 9 of the Data Act. This provision states that when the data recipient is a SME, the agreed compensation shall not exceed the costs directly related to making the data available and that are attributable to the data request of the data recipient.]

2.4 No-Exclusivity. The Covered Data is provided on a non-exclusive basis and the Data Recipient acknowledges that the Data Holder may grant access to the Covered Data to third parties or may continue to use the Covered Date itself.

2.5 Restrictions on Use. The use of the Covered Data by the Data Recipient and/or any Downward Recipient, if any, shall be limited by the Restrictions.

2.6 Prohibited Use. In addition to any Restrictions, the Data Recipient and the Downward Recipient, if any, shall not:

a) deploy any coercive means or abuse any evident gaps in the technical infrastructure of the party holding the Covered Data, to obtain access to Data;

b) use any Covered Data or Result to derive insights about the economic situation, assets and production methods of, or use by the Data Holder, that could undermine the commercial position of the Data Holder on the markets in which such party is active unless such party has consented to such use and has the technical possibility to withdraw that consent at any time;

c) use any Covered Data or Result to develop a product or service that competes with the product or service from which the Covered Data originate or share such Data with a third party for that purpose.

[**Drafting comment:** this section addresses potential risks related to the use of Covered Data by the data recipient. It is based on obligations applicable under the Data Act to the data recipient or data holder, as the case may be (e. g. art. 5 and 6 of the Data Act). Since this agreement is bilateral, does not involve any individual and is not based on any legal requirement to share data or any access right, the obligations fall upon the data recipient only.]

DSD additions:

d) use the Covered Data or Results to infer sensitive attributes, behavioral patterns or profiling information relating to identifiable groups or communities, unless explicitly authorized and supported by appropriate safeguards;

e) use the Covered Data in a manner that creates foreseeable Harm or Misalignment, as defined in this Agreement;

f) continue a specific use if the Data Holder notifies the Data Recipient that a Context Change has occurred and the Parties have not yet reached agreement on appropriate safeguards or whether the use may continue.

[**Note:** These refinements integrate DSD's harm mitigation, group-level protection, and dynamic governance.]

2.7 Limited License. This Agreement does not aim at addressing or governing possible ownership or property rights in or to the Covered Data. To the extent that the Covered Data shall however be subject to Intellectual Property Rights, the Data Holder hereby grants the Data Recipient a non-exclusive license to the Data Recipient to use the Covered Data in accordance with this Agreement, for the Term.

2.8 Confidentiality. The Covered Data may contain Confidential Information of the Data Holder or third parties and the Data Recipient agrees that this Agreement does not constitute permission to obtain or reveal Confidential Information, whether by way of reverse-engineering or decompiling, or any other technical or non-technical mean allowing access to such Confidential Information. The Data Recipient shall treat as confidential any Confidential Information it may receive or be granted access to unwillingly or fortuitously by the Data Holder. The Data Recipient shall also refrain from any use of Covered Data or Confidential Information that would reasonably be expected to undermine the trust, expectations or self-determination interests of individuals, groups or communities represented in the Covered Data.

2.9 Compliance. Nothing in this Agreement shall restrict, limit or otherwise affect any rights or obligations that the Parties may have under any applicable laws or regulations, such as (without limitation) competition and antitrust laws, or in relation to data sharing or data access requests of users.

[**Drafting comment:** this section reserves any obligations a party may have under the Data Act or other laws or regulations, since the Data Act imposes specific data sharing obligations on data holders. Even if the Data Act is not directly applicable to the relationship between the parties under this agreement, it may nevertheless apply to a party depending on the circumstances (e.g. if such party provides connected products or services in the EU).]

DSD addition: For the avoidance of doubt, the Parties acknowledge that this Agreement is intended to operate consistently with principles of Digital Self-Determination as defined herein and shall cooperate in good faith to address any new regulatory requirements or sector-specific standards that reinforce such principles.

2.10 [Audit. The Data Recipient agrees that the Data Holder may, at any time during the Term, but no more than once a year, access the Data Recipient's books, records, infrastruc-

tures, databases and Results in order to ensure compliance with the present Agreement. Any Confidential Information of the Data Recipient to which the Data Holder may have access in that context shall be treated as confidential.]

[**Comment:** this section 2.10 is mainly relevant in case strict restrictions on use are selected, in order to allow the Data Holder to verify compliance with such restrictions. It can typically be removed in case no restrictions on use are selected by the parties.]

DSD addition: Any such audit shall be proportionate, limited to verifying compliance with this Agreement, and conducted in a manner that minimizes operational disruption and respects confidentiality, including any DSD-related obligations.

[**Note:** this adds proportionality and purpose-limitation to the audit's scope.]

3. ADDITIONAL SERVICES

3.1 Services. [Alt.1] In addition to the access to the Covered Data, the Data Holder may provide additional services to the Data Recipient. [Alt.2] The parties acknowledge that no additional services shall be rendered by the Data Holder, who offers no warranty of continuous availability nor of continuous access to the Covered Data and does not provide any support to the Data Recipient.

[**Comment:** Select Alt.1 if the Data Holder is also offering additional services (e.g. support, analysis, etc.) or Alt.2 if no additional services are contemplated.]

DSD Additions (compatible with either Alternative):

If the Data Holder provides additional services, it shall do so in a manner that:

a) offers clear and accessible explanations of the methodologies, tools, and processes used;

b) avoids creating unintended inferences about individuals, groups, or communities represented in the Covered Data;

c) allows the Data Recipient to understand any limitations or uncertainties associated with the services;

d) supports the safe and context-appropriate use of the Covered Data in accordance with the principles of Digital Self-Determination.

[Note: These additions anchor the services in transparency and responsible use but do not create new obligations of performance.]

3.2 Additional Terms. Any additional services or tools that may be offered to the Data Recipient shall be governed by additional terms, whether in the form of an API license agreement, terms of use of a platform or any services agreement that may be entered into by the parties.

DSD Additions:

The Data Holder shall ensure that such additional terms:

a) are made available in clear and accessible language,

b) describe any limits, risks, or context assumptions relevant to the additional services, and

c) include a point of contact for questions concerning responsible use, data limitations, or potential Context Changes.

[**Note:** ensures that add-on tools cannot undermine the DSD alignment of the main contract.]

3.3 Interoperability. The Parties shall use their best efforts to facilitate the Interoperability of Covered Data, data sharing mechanisms and data services, if any, as follows:

a) the dataset content, use restrictions, licenses, data collection methodology, data quality and uncertainty shall be sufficiently described to allow the Data Recipient to find, access and use the Covered Data;

b) the data structures, formats, vocabularies, classification schemes, taxonomies and code lists shall be sufficiently described in a consistent manner;

c) the technical means to access the Covered Data, such as any API, and their terms of use and quality of service, shall be sufficiently described to enable automatic access and transmission of data between parties, including continuously or in real-time in a machine-readable format;

d) the means to enable the interoperability of smart contracts, if any, within their services and activities shall be provided.

[**Drafting comment:** this section 3.3 reflects the interoperability essential requirements under art. 28 of the Data Act, but on a best-efforts basis.]

DSD Enhancements to Interoperability (Important)

To support DSD, the Parties shall also:

e) ensure that metadata and documentation are provided in a manner understandable to non-technical stakeholders where appropriate;

f) avoid implementing interoperability in a way that creates new risks of inappropriate inference or re-identification, including risks affecting identifiable groups or communities;

g) notify the other Party if interoperability features introduce or reveal any new Context Change, limitations, or potential Harm or Misalignment, and suspend the relevant functionality until mitigations are agreed.

(**Note:** This ties the Interoperability clause to governance and responsible risk mitigation, not just technical compatibility.)

4. ATTRIBUTION

[Alt.1] The origin of the Covered Data and identity of the Data Holder shall systematically be made available to third parties to whom the Covered Data and/or the Results have been Distributed. [Alt.2] The Data Recipient shall always seek prior written authorization from the Data Holder to mention the origin of the Covered Data and the identity of the Data Holder in case of authorized Distribution of the Covered Data and/or Results.

[Comment: select Alt.1 if the Data Holder wishes that its identity and the origin of the data be automatically communicated when such data is being distributed to third parties; select Alt.2 if the Data Holder wishes to check and confirm prior to the distribution whether its identity should be mentioned or not.]

DSD Enhancements (compatible with either alternative)

To support DSD and the responsible interpretation of the Covered Data:

a) Accuracy & Contextual Integrity

Any attribution shall be accompanied by a clear and accurate description of the nature, scope, limitations, and original context of the Covered Data, so that third parties do not misunderstand or misinterpret its meaning or purpose.

b) Group & Community Sensitivities

The Data Recipient shall refrain from attribution practices that may misrepresent, stereotype or negatively affect identifiable groups or communities reflected in the Covered Data, or that may imply endorsement or involvement by such groups where no such endorsement exists.

c) Restrictions Flow-Down

Where attribution is made, the Data Recipient shall also communicate any relevant Restrictions and use limitations attached to the Covered Data, unless the Data Holder instructs otherwise.

d) Attribution as Non-Endorsement

Unless expressly agreed by the Data Holder in writing, attribution of the Covered Data shall not be presented or implied as an endorsement, certification, or validation of the Results by the Data Holder or by any groups or communities represented in the Covered Data.

e) Context Change Notifications

If the Data Recipient becomes aware that attribution—whether in form or content—may create a Context Change or newly introduce potential Harm or Misalignment, it shall promptly notify the Data Holder and, where necessary, suspend such attribution until both Parties agree on mitigations.

5. SECURITY

5.1 IT Security. The Data Recipient shall comply with all laws and regulations applicable to the privacy or security of the Covered Data.

DSD Additions (practical and minimal):

The Data Recipient shall also implement security measures that are appropriate to the nature, sensitivity, and potential impacts of the Covered Data, including the potential for indirect impacts on individuals, groups, or communities represented in the Covered Data.

Such measures shall include, at minimum:

a) access controls and authentication appropriate to the access modality;

b) industry-standard technical and organizational measures to prevent unauthorized access, alteration, or misuse;

c) safeguards to avoid inference, reconstruction, or linkage attacks that may create Harm or Misalignment;

d) internal procedures that ensure the Covered Data is used only for the purposes permitted under this Agreement.

(**Note:** This aligns security with contextual integrity and group-level protection.)

5.2 Breach Monitoring. In the event of an actual or suspected security incident involving its information systems, the Data Recipient shall immediately notify the Data Holder and comply with any applicable notification obligations.

DSD Additions:

Upon becoming aware of an actual or suspected incident, the Data Recipient shall provide the Data Holder with:

a) a brief description of the nature of the incident;

b) an assessment of whether the incident may result in Harm or Misalignment;

c) a description of immediate containment measures taken;

d) follow-up actions planned to prevent recurrence.

Where the Covered Data relates to identifiable groups or communities, the Parties shall in good faith assess whether any **context-specific mitigations** or communication measures may be appropriate.

(**Note:** supports agency, transparency and harm mitigation, without introducing new statutory obligations.)

5.3 Suspension for Risk Mitigation *(new DSD clause)*

If either Party reasonably believes that continued access to or use of the Covered Data may create a material risk of Harm or Misalignment, including due to a security incident, inference vulnerability, or newly discovered dataset sensitivity, the concerned Party may temporarily suspend access or use of the Covered Data.

Such suspension shall be:

a) promptly communicated to the other Party;

b) limited to what is strictly necessary;

c) reviewed jointly by the Parties in good faith to determine appropriate safeguards or conditions for resuming access.

(**Note:** key to dynamic governance and contextual integrity under DSD).

5.4 Security and Use Review Mechanism (optional)

Upon reasonable request, the Parties shall meet to review applicable security and governance measures to ensure continued alignment with:

- the permitted purposes of this Agreement,
- evolving best practices, and
- principles of Digital Self-Determination.

(**Note:** This is non-auditory, non-intrusive, and preserves the voluntary nature of the agreement.)

6. REPRESENTATIONS AND WARRANTIES

6.1 Each party represents that it will perform its obligations under this Agreement in compliance with applicable laws. In addition, each party shall act in good faith to ensure that its use of the Covered Data remains consistent with the principles of DSD, including transparency regarding the context and limitations of the Covered Data and the prevention of foreseeable Harm or Misalignment.

6.2 The Data Holder offers no warranty that the Data Recipient shall not be granted access to Personal Data in the performance of this Agreement and should the Data Recipient be granted access to Personal Data in the framework of this Agreement, the Data Recipient acknowledges that it may be subject to additional obligations to comply with privacy and data protection laws and commits to take the relevant measures to comply with such obligations, if any. The Data Recipient shall promptly notify the Data Holder if it becomes aware that the Covered Data contains, or could reasonably allow the inference of, Personal Data or sensitive group-level characteristics, so that the Parties may assess appropriate safeguards or limitations on use.

(**Note:** to connect privacy obligations with contextual and collective DSD risks).

6.3 The Covered Data is provided on an "as is" and "as available" basis, without warranties or conditions of any kind, either express or implied including, without limitation, any warranties or conditions of title, non-infringement, merchantability or fitness for a particular purpose. Both Parties acknowledge that the Covered Data may contain limitations, uncertainties or biases inherent to its collection or processing. The Parties shall cooperate in good faith to clarify any such issues if identified during the Term, in order to support responsible and context-appropriate use of the Covered Data.

(**Note:** clarifies DSD without implying data-quality warranties.)

6.4 Within the limits of applicable law, the Data Holder shall have no liability for any direct or indirect damages (including without limitation lost profits), however caused and on any theory of liability, whether in contract, strict liability, or civil liability (including negligence or otherwise) arising in any way out of the covered data, even if advised of the possibility of such damages. Nothing in this Section shall prevent either Party from raising concerns or requesting a review under this Agreement where it reasonably believes that continued use of the Covered Data may lead to Harm or Misalignment. Such review shall be handled through the governance mechanisms set forth in this Agreement and shall not be construed as an admission of liability.

(**Note:** preserves full limitation of liability while enabling DSD governance dialogue.)

7. DURATION AND TERMINATION

7.1 Duration. This Agreement enters into force on the date first written above and for the duration of the subscription term mentioned on the cover sheet. It shall be automatically renewed, at the same conditions, for additional terms of the same duration unless terminated in accordance with this Agreement. The initial subscription term and all renewal terms shall together constitute the Term. During each renewal, the Parties may, upon request, review whether the context of use or the sensitivity of the Covered Data has materially changed and whether additional safeguards or adjustments are appropriate.

(**Note:** this adds an optional governance review without creating an obligation.)

7.2 Voluntary Termination. Each party may terminate this Agreement without cause with a Termination Notice as set forth on the cover sheet. Upon voluntary termination by either Party, the Parties shall cooperate in good faith to ensure a responsible wind-down of any ongoing uses of the Covered Data that might affect identifiable groups or communities, consistent with the principles of Digital Self-Determination.

(**Note:** adds a soft governance duty, not a performance or service obligation.)

7.3 Automatic Termination. This Agreement shall automatically terminate in case of breach of any of the terms and conditions of this Agreement by the Data Recipient or a Downward Recipient. **(DSD Addition):** For the avoidance of doubt: a) an automatic termination shall not require prior notification where the breach presents a material risk of Harm or Misalignment; b) where the breach does not present such risk, the Data Holder may, but is not obliged to, provide an opportunity to cure the breach before termination.

(**Note:** preserves the Data Holder's discretion and adds DSD aligned language about harmful uses.)

7.4 Effect of Termination. Upon termination of this Agreement for any reason whatsoever, the Data Recipient shall no longer be granted access to the Covered Data nor be authorized to make any use of the Covered Data. The Data Recipient shall remain entitled to use the Results and sections 2.8, 4, 6.4 and 8 shall survive the termination of this Agreement.

DSD Additions:

The Data Recipient shall, upon termination:

a) delete, return, or render inaccessible any Covered Data in its possession, except where expressly required by law to retain it;

b) refrain from any further use of the Covered Data, including uses that could reasonably lead to Harm or Misalignment;

c) retain the Results only to the extent that the Results do not enable reconstruction, reverse engineering, or inference of the Covered Data;

d) document any outstanding issues that may be relevant to the Data Holder's assessment of risks or to future contextual integrity.

(**Note:** This ensures responsible wind-down, preserves Result rights, and prevents misuse after termination.)

8. MISCELLANEOUS

8.1 Entire Agreement. This Agreement contains all of the terms and conditions agreed upon by the parties relating to its subject matter and supersedes all prior agreements, negotiations, correspondence, undertakings and communications of the parties, whether oral or written, with respect to such subject matter. The Parties acknowledge that governance mechanisms relating to Digital Self-Determination, Context Changes, and prevention of Harm or Misalignment are integral to the interpretation and implementation of this Agreement.

8.2 Form. Any reference to the written form in this Agreement, and any reference to any notice or document to be delivered in writing, shall be deemed to be satisfied by email or any form of electronic signature service such as PDF or DocuSign. Notices relating to concerns regarding DSD, Harm, Misalignment, or Context Change shall be sent to the Data Steward or to another designated point of contact identified by each Party.

(**Note:** This operationalizes the Data Steward and ensures governance notices don't get lost.)

8.3 Severability. If any provision of this Agreement is held to be unenforceable for any reason, it shall be adjusted rather than voided, if possible, in order to achieve the intent of the parties to the fullest extent possible. In any event, all other provisions of this Agreement shall remain valid and enforceable to the fullest extent possible. In adjusting any unenforceable provision, the Parties shall consider how the adjusted provision can continue to support the principles of Digital Self-Determination and maintain the Agreement's overall governance structure.

(**Note:** Soft; no legal risk; ensures DSD does not disappear if one clause is invalid.)

8.4 No Waiver. The failure of any of the parties to enforce any of the provisions of this Agreement or any rights with respect thereto shall in no way be considered as a waiver of such provisions or rights or in any way affect the validity of this Agreement. The waiver of any breach of this Agreement by any party shall not be construed as a waiver of any other prior or subsequent breach. A Party's decision not to invoke a governance mechanism or raise a DSD-related concern at any specific time shall not be construed as a waiver of its right to do so later.

(**Note:** avoids "you didn't raise the risk earlier, so you waived it.".)

8.5 Governing Law. This Agreement shall be governed by and construed in accordance with Swiss substantive law, without reference to its conflict of laws provisions.

Nothing in this Section prevents the Parties from considering relevant international soft-law frameworks concerning Digital Self-Determination, responsible data use, or data governance where helpful to interpret the context or intent of specific provisions of this Agreement.

8.6 Jurisdiction. [Alt.1] Any dispute, controversy or claim arising out of or in relation with this Agreement shall be submitted to the ordinary courts at the domicile or the registered seat of the Data Holder, subject to appeal to the competent superior authority. Alt.2] Any dispute, controversy or claim arising out of or in relation with this Agreement shall be resolved by arbitration in accordance with the Swiss Rules of International Arbitration of the Swiss Arbitration Centre and the ITDR–Institution for IT and Data Dispute Resolution Recommendations for Arbitration, both in force on the date on which the Notice of Arbitration is submitted in accordance with these Rules and Recommendations. The number of arbitrators

shall be one or three. The seat of the arbitration shall be the seat of the Data Holder. The arbitral proceedings shall be conducted in English. Notwithstanding the above, the parties may agree at any time to submit the dispute to mediation in accordance with the Swiss Rules of Mediation of the Swiss Arbitration Centre and the ITDR – Institution for IT and Data Dispute Resolution Recommendations for Mediation, both in force on the date on which the request for mediation is submitted in accordance with these Rules and Recommendations. Notwithstanding the above, the parties may agree at any time prior to submitting the dispute to arbitration or mediation to submit the dispute to assessment by an expert opinion in accordance with the ITDR – Institution for IT and Data Dispute Resolution Rules of Procedure for Expert Opinions in force on the date on which the request for assessment by an expert opinion is submitted in accordance with these Rules.

[**Comment:** select Alt.1 if the parties wish to subject potential disputes relating to the agreement to ordinary Swiss courts, without a specific expertise in the field; this corresponds to the ordinary route in case of disputes; select Alt. 2 if the parties wish to subject potential disputes to arbitration by experts in the field, as well as benefit from the ability to ask an expert to intervene before initiating an arbitration or mediation.]

DSD Addition (applies to both alternatives):

Prior to initiating litigation, arbitration, mediation or expert proceedings, the Parties shall meet in good faith, unless the circumstances make such meeting impossible, to determine whether the dispute relates in whole or in part to a Context Change, Harm, Misalignment or other DSD governance issue and whether it may be resolved through the collaborative mechanisms set out in this Agreement.

(**Note:** This is procedural, non-binding, and aligns dispute resolution with DSD governance.)

Data Holder	Data Recipient
_____	_____
_____	_____

APPENDIX VI

Options for Stress Testing Digital Self-Determination

This appendix provides a set of stress testing and evaluation methods that data space operators can use to assess whether Digital Self-Determination is being upheld in practice over time. The methods are intended to support the continuous assurance described in Phase 4 of the roadmap.

Each method examines how governance arrangements, contractual commitments, and technical controls perform under conditions that may strain agency, accountability, or legitimacy. These conditions include operational surges, contested decisions, system changes, security incidents, or shifts in data use and reuse.

The methods are organized around four principles used in Swiss guidance on trustworthy data spaces: transparency, control, effectiveness, and fairness. For each method, the appendix describes the objective, scope, preconditions, procedure, indicators, common failure modes, and reference sources. This structure is intended to help operators understand what a method tests, what is required to apply it, and what kinds of insights it can produce.

The methods presented here are illustrative rather than exhaustive. They draw on practices from data governance, cybersecurity, public administration, and AI oversight, adapted to the federated and multi-actor nature of data spaces. Data space operators are expected to select, adapt, and combine methods based on context, maturity, and risk profile, and to integrate findings into existing governance, review, and improvement processes.

1. Transparency

PURPOSE

Transparency concerns the ability of a data space to make decisions, data flows, and policy applications visible and understandable—particularly when conditions are changing or stressed. It enables auditability, meaningful explanation, and timely disclosure to participants and affected communities. In federated settings, transparency is essential to preserving legitimacy across organizational boundaries where no single actor has full visibility by default.

WHAT "GOOD" LOOKS LIKE

- End-to-end decision provenance: traceable inputs, applicable rules and versions, accountable actors, timestamps, and outcomes, presented in both machine-verifiable form and plain language.
- Complete and timely operational records: logs, lineage, model and policy change histories, and incident timelines that can be correlated across participants.
- Proactive disclosures: clear notifications and status updates when material changes or incidents occur, including the scope of impact and next steps.

TYPICAL ROLES AND RESPONSIBILITIES

- Data stewards: maintain dataset documentation, lineage, quality declarations, and contact points.
- Governance owners: manage rule sets and their versions; coordinate decision forums.
- Security/engineering: implement logging, signatures, time synchronization, and integrity controls.
- Communications and service desks: publish notices, status updates, and responses.
- Auditors (internal or external): verify evidence, completeness, and tamper-evidence.
- Affected parties and community representatives: receive explanations and, where appropriate, participate in review or appeal processes.

Method T1

Decision Provenance Drill

Objective

Assess the ability to reconstruct and communicate a complete, tamper-evident narrative for a significant governance or access decision, including who decided, which evidence and rules were applied, and the rationale for the outcome.

Scope

One recent, high-impact decision that crosses at least two organizations (for example, an approval or denial of a data access request, a policy exception, or a model deployment affecting downstream services).

Preconditions

- Policy or rule repositories with version control and immutable identifiers.
- Append-only, time-synchronized logs and signatures to ensure tamper-evidence.
- Named roles and an established channel for affected-party communications.

Procedure

- Select a decision taken within the last quarter and freeze associated artifacts (request, approvals, rule versions, timestamps, logs).
- Assemble a provenance pack that correlates inputs, rules, actors, timestamps, and the final outcome across all participating nodes.
- Produce a concise explanation suitable for non-specialist readers, summarizing what was decided, why, by whom, and which rule versions applied, with references to evidence.
- Verify integrity by checking signatures, hashes, and time coherence; record any gaps or inconsistencies.
- Conduct an appeal simulation in which stewards respond using the provenance pack and the plain-language explanation.

Indicators and suggested thresholds

- Time to assemble provenance pack: ≤ 4 hours for cross-organizational decisions.
- Completeness: ≥ 95% of required fields present (inputs, ruleset identifier, actors, timestamps, outcome, rationale, evidence links).
- Explainability: average usability rating ≥ 4 out of 5 from a small panel of non-experts.
- Tamper-evidence: 100% verification of signatures and hashes across artifacts.
- Appeal response time: ≤ 5 business days to provide a reasoned response referencing evidence.

Evidence to retain

Provenance bundle, plain-language explanation, integrity verification results, appeal record, and a checklist with indicator scores.

Common failure modes and remedies

- Missing rule versions: mandate inclusion of policy commit identifiers in decision records.
- Clock skew and inconsistent timestamps: enforce synchronized time sources and record acceptable skew.
- Explanations that are overly technical: require standard templates that define terms and avoid acronyms without definitions.

Scoring rubric (0–5)

0–1 ad hoc evidence; 2 partial logs; 3 consistent internal packs; 4 cross-organizational packs plus user-facing explanations; 5 automated, signed provenance with self-service access for authorized parties.

Real-world Examples

- W3C PROV (provenance data model and ontology for who/what/when/why): https://www.w3.org/TR/prov-overview/ and https://www.w3.org/TR/prov-o/
- W3C Verifiable Credentials (signed attestations to anchor actors/claims in decision trails): https://www.w3.org/TR/vc-data-model-2.0/
- ODRL (W3C Open Digital Rights Language) to represent policies/permissions referenced in decisions: https://www.w3.org/TR/odrl-model/
- ISO/IEC TS 27560 (machine-readable consent record lifecycle, linkable to access decisions): https://www.iso.org/standard/80392.html
- Certificate Transparency-style append-only logs (Merkle trees) as a pattern for tamper-evident decision logs: https://www.rfc-editor.org/rfc/rfc6962
- OpenLineage (standardized lineage events to connect inputs → processes → outputs across systems): https://openlineage.io/

Method T2

TRAC-Inspired Repository Audit (Transparency Controls)

Objective

Adapt the principles of Trustworthy Repositories Audit & Certification to stress-test documentation quality, integrity controls, and disclosure practices for datasets under change or incident.

Scope

One data product (dataset, metadata, and associated policies) with at least two maintainers across organizations, including one material change (for example, a schema modification) and one incident in the past 90 days.

Preconditions

- Dataset cards and policy summaries with clear ownership and contact points.
- Versioning with fixity (checksums or signatures) and chain-of-custody records.
- Defined change-notification and incident-disclosure procedures, including subscriber channels and status pages.

Procedure

- Conduct a documentation sweep to verify completeness and freshness of dataset cards, lineage, policy summaries, and contacts.
- Verify integrity through fixity checks for the last two stored versions and confirm chain-of-custody details.
- Review how the last material change was communicated: audience, timing, clarity, and catalog updates.
- Trace the most recent incident from detection to containment, notification, and lessons learned; confirm evidence of each step.
- Record non-conformities and corrective actions with owners and deadlines.

Indicators and suggested thresholds

- Documentation completeness: Documentation is largely current and filled out. Target: at least 90% of required fields updated in the latest release cycle.
- Fixity coverage: Stored artifacts include tamper checks and validate in practice. Target: 100% covered; audit validations mostly successful (≈98% or higher).
- Change-notice timeliness: ≤ 5 business days from approval to subscriber notification and catalog change log.
- Incident post-mortem: Incidents are analyzed and recorded with actions to prevent recurrence. Target: internal write-up within 15 business days; brief external note when the incident is material.

- Contactability: Published steward or contact point responds through the official channel. Target: first meaningful response within one business day.

Evidence to retain

Completed control checklist with links, fixity report, version diffs, change notices, incident post-mortem, and the corrective-action register.

Common failure modes and remedies

- Silent changes breaking downstream services: require catalog notices and subscriber webhooks for any material change.
- Stale documentation: link documentation checks to release gates; block promotions on missing or outdated records.
- Incomplete fixity: compute checksums on ingest and schedule periodic verification jobs.

Scoring rubric (0–5)

0–1 minimal documentation; 2 basic versioning; 3 fixity with change notices; 4 incident transparency with service-level targets; 5 continuous compliance dashboards and periodic transparency reports where appropriate.

Real-world Examples

- TRAC — Trustworthy Repositories Audit & Certification criteria/checklist: https://www.crl.edu/sites/default/files/2025-01/trac.pdf
- CoreTrustSeal — Trustworthy Data Repositories Requirements and certification process: https://www.coretrustseal.org/why-certification/requirements/
- OAIS Reference Model (ISO 14721) — conceptual framework for archival transparency & preservation: https://public.ccsds.org/pubs/650x0m2.pdf
- CCSDS 652.0-M-2 — Audit & Certification of Trustworthy Digital Repositories (current practice): https://ccsds.org/Pubs/652x0m2.pdf
- PREMIS Data Dictionary — preservation metadata for provenance, fixity, and events: https://www.loc.gov/standards/premis/
- BagIt (RFC 8493) — packaging with checksums for verifiable versioning/fixity during audits: https://www.rfc-editor.org/rfc/rfc8493

Method T3

Data Quality Drift Drill — Transparency Variant

Objective

Evaluate whether quality degradation becomes visible quickly to both producers and consumers, whether its impact is understandable, and whether remediation steps are documented as part of the dataset's public or participant-visible record.

Scope

One multi-source dataset in active use by downstream services. Over 48–72 hours, inject three drift types: missing values, delayed freshness, and semantic shift (for example, changed value ranges).

Preconditions

- Declared quality targets for freshness, completeness, and validity.
- Monitoring and alerting aligned to those targets.
- Subscriber communication channels (for example, webhooks, email, or portal notifications) and a status page.
- A mapping from dataset fields to dependent dashboards, APIs, or reports to support impact tagging.

Procedure

- Define a drift-injection plan specifying the type, timing, and magnitude of each drift.
- Introduce the drifts and record ground truth.
- Observe detection latency, alert routing, and receipt by subscribers.
- Publish a status update and annotate affected fields and dependent assets in the catalog.
- Apply remediation, update lineage to reflect both drift and fix, and publish a final note summarizing cause, impact, and prevention steps.
- Collect feedback from a small sample of consumers on clarity and timeliness of notices.

Indicators and suggested thresholds

- Detection latency: freshness drift detected within 30 minutes; completeness or semantic drift within 2 hours.
- Notification coverage: at least 95% of subscribers notified within 1 hour of detection.
- Impact annotation: at least 90% of affected fields and dependent assets tagged in the catalog within 1 business day.
- Status cadence: initial notice within 1 hour, with daily updates until resolution.
- Provenance update: lineage reflects drift and remediation within 1 business day.

Evidence to retain

Alert timelines, subscriber delivery logs, status page records, catalog annotations, lineage snapshots before and after remediation, and consumer feedback.

Common failure modes and remedies

- Long-tail consumers miss alerts: mandate subscription on first access and maintain a broadcast fallback channel.
- Unclear scope of impact: maintain an up-to-date field-to-dependency map; automate tagging of affected dashboards and APIs.
- Slow posting of updates: use a prepared status template and pre-approved wording blocks for rapid publication.

Scoring rubric (0–5)

0–1 ad hoc discovery; 2 basic alerts; 3 consumer notifications; 4 end-to-end provenance with status pages; 5 automated dependency tagging, consistent public or participant disclosures, and structured post-mortems.

Real-world Examples

- Principles from the Data Spaces Support Centre and EU's EHDS governance framework.
- ISO/IEC 25012 (Data Quality Model) — dimensions/attributes to define visible quality targets: https://standards.iso.org/ittf/PubliclyAvailableStandards/c061298_ISO_IEC_25012_2008(E).zip
- ISO 8000 (Data quality series) — governance for master and reference data quality: https://www.iso.org/committee/54756.html
- Great Expectations (declarative data validation with human-readable "expectations" and docs): https://greatexpectations.io/
- See also Gille et al. (2025) on trustworthiness as dependent on the reliable, transparent implementation of data handling principles, and the limitations of trust indicators that fail to capture operational degradation.
- Amazon Deequ (constraint-based data quality checks at scale): https://github.com/awslabs/deequ
- Data Contracts (schema + SLOs + change control to make drift and impacts visible): https://datacontracts.org/
- OpenLineage + dbt tests (lineage-aware impact analysis and test failures surfaced to consumers): https://openlineage.io/ and https://docs.getdbt.com/docs/build/tests

2. Control

PURPOSE

Control concerns the practical ability of individuals and communities to set conditions on data use, grant or withdraw permission, obtain copies or move data, exit a data space, contest outcomes, and shape collective boundaries for acceptable use. In federated environments, meaningful control requires that rights and preferences propagate reliably across organizational lines and remain enforceable under stress.

WHAT "GOOD" LOOKS LIKE

- Consent and permission changes propagate quickly and halt further processing where required, with clear confirmation to affected parties.
- Portability and exit are feasible without loss of context, including metadata and provenance needed for continued use elsewhere.
- Collective voice is embedded through social license or equivalent community conditions, with routes to escalate ambiguous cases for deliberation.
- Contestation and redress processes exist, are understandable, and lead to timely, reasoned outcomes tied to evidence.

TYPICAL ROLES AND RESPONSIBILITIES

- Data stewards and access managers: implement permission changes, exports, and exits; verify completion.
- Governance owners and community representatives: define conditions for allowable use and adjudicate contested cases.
- Security/engineering: ensure permissions, tokens, and policies are enforced consistently across participants.
- Service desks and communications: provide confirmations, guidance, and appeal routes.
- Auditors: verify evidence of enforcement and timeliness.

Method C1

Consent Revocation Flood

Objective

Assess whether large volumes of permission withdrawals (revocations) are propagated and enforced across all relevant participants and downstream services under stress, such that further processing of affected data is halted in a timely and verifiable manner.

Scope

A coordinated batch of revocations affecting multiple datasets and purposes across at least two independent organizations or nodes, including at least one downstream consumer (for example, an analytics job, dashboard, export, cache, or model pipeline).

Preconditions

- A structured "revocation object" that clearly identifies scope (subjects or records, dataset identifiers, purpose or policy tags, effective time, originating authority).
- A federation-wide propagation mechanism (event bus, API, or trust service) discoverable by obligated processors.
- Enforcement points that are revocation-aware (access control, policy/usage control, schedulers, and data processing jobs).
- An inventory of downstream consumers (dashboards, scheduled jobs, APIs, models, caches, mirrors/exports).
- Agreed contacts and escalation paths for the test window.

Procedure

- Launch the wave: issue a high volume of revocations within a short interval, covering varied data products and purposes.
- Observe propagation: confirm delivery to all obligated processors and access control points; capture delivery receipts or logs.
- Check enforcement: attempt normal reads/processing at enforcement points; expected outcome is denial or safe fail.
- Verify downstream suppression: inspect dashboards, jobs, caches, models, and exports for continued use after the effective time; expected outcome is no access or use.
- Record exceptions and apply fixes: log any residual access or processing; assign remediation with owners and deadlines.

Indicators and suggested thresholds (streamlined)

- Propagation time: revocations reach obligated processors within hours, not days.
- Coverage: nearly all targeted processors act on revocations; isolated misses are corrected during the exercise.
- Confirmation quality: plain-language confirmations issued that processing/access has been halted.
- Residual access: none detected in sampled downstream services after the effective time.

Evidence to retain

- The revocation batch description (scope, counts, effective times) and originating authority.
- Delivery receipts or logs from processors and enforcement points.
- Enforcement confirmations (denials, halted jobs, updated access rules).
- Downstream verification notes/screenshots or job logs showing suppression.
- Exception list with remediation actions and completion status.

Common failure modes and remedies

- Unregistered consumers (missed subscribers) → maintain a living dependency map; mandate subscription on first access; add a broadcast fallback channel.
- Stale caches/mirrors or exported copies → add cache-invalidation hooks; require periodic permission re-checks; tag exports with revocation callbacks.
- Batch jobs that bypass checks → enforce policy checks at use time (not only at ingest); instrument schedulers to query current permission state.
- Ambiguous scope in revocation objects → standardize identifiers and purpose tags; require effective-time semantics; digitally sign revocation objects.

Scoring rubric (0–5)

0–1 ad hoc handling; 2 partial propagation with manual steps; 3 consistent cross-org propagation; 4 end-to-end enforcement including downstream suppression; 5 automated propagation with self-service confirmations, dependency-aware suppression, and continuous monitoring.

Real-world Examples

- Privacy and data protection: withdrawal of consent under GDPR Articles 7 and 21, with downstream suppression akin to “right to be forgotten” practices.
- Web consent signals: Global Privacy Control (GPC) / “do not sell/share” signals used to propagate opt-outs across services.

- Email ecosystems: “List-Unsubscribe” mechanisms and suppression lists to prevent further messaging after opt-out.
- Payments: card chargeback/stop-payment instructions propagate across networks to halt further settlement.
- Software/package registries: security advisories and revocation of compromised packages trigger downstream build failures and cache purges.

Real-world Examples

- ISO/IEC 27560 (machine-readable consent record lifecycle for revoke/withdraw workflows): https://www.iso.org/standard/80392.html
- Global Privacy Control (GPC) signal for propagating revoke/opt-out across services: https://globalprivacycontrol.github.io/gpc-spec/
- OpenID Shared Signals & Events (SSE) / CAEP for near-real-time risk and consent state changes: https://openid.net/specs/openid-sse-framework-1_0.html and https://openid.net/specs/openid-caep-specification-1_0.html
- SCIM 2.0 Deprovisioning (revocation of identities/entitlements across systems): https://www.rfc-editor.org/rfc/rfc7644
- UMA 2.0 (User-Managed Access) for user-centric authorization and revocation: https://docs.kantarainitiative.org/uma/rec-uma-core.html
- XACML / Policy-as-Code (OPA/Rego) to enforce revoke conditions at decision points: https://docs.oasis-open.org/xacml/xacml-3.0-core-spec-os-en.html and https://www.openpolicyagent.org/

Method C2

Portability & Exit Drill

Objective

Evaluate whether individuals or organizations can obtain a complete, usable export of their data and associated context, and terminate participation with verifiable deletion or access removal across the federation.

Scope

One participant (or cohort) requesting both data portability and full exit. At least one complex dataset with dependencies (linked tables, files, or models) spanning two or more organizations.

Preconditions

- Defined export format(s) for data, metadata, and provenance (for example, CSV/ Parquet plus machine-readable metadata, policy references, and lineage).
- Exit procedure with roles, steps, and required confirmations.
- Mechanisms for deletion or access termination, including logs and attestations from processors.
- Neutral test environment for import validation.

Procedure

- Initiate a portability request and a termination-of-participation (exit) request.
- Produce export packages that include data, essential metadata, and provenance sufficient to re-use elsewhere.
- Execute deletion or access termination where applicable; capture confirmations from all obligated processors.
- Import the export package into a neutral environment to validate completeness and usability.
- Document any gaps and assign remediation actions.

Indicators and suggested thresholds (streamlined)

- Time to complete export and exit: measured in days rather than weeks.
- Export completeness: data plus key metadata and provenance sufficient for re-use.
- Deletion/access termination: confirmed by all obligated processors.
- Import usability: successful reconstruction of core context in the test environment.

Evidence to retain

- Export packages and manifests, checksums, and format descriptions.
- Deletion/termination confirmations and relevant logs.
- Import validation notes and outcomes.
- Exception register with remediation owners and deadlines.

Common failure modes and remedies

- Missing metadata/provenance → extend export scope to include schemas, code lists, policies, and lineage pointers.
- Orphaned access after exit → enforce permission revocation and token invalidation as part of exit workflow.
- Proprietary formats only → add open, documented formats or include conversion tools and schemas.

Scoring rubric (0–5)

0–1 ad hoc exports; 2 partial export without metadata; 3 complete export or exit but not both; 4 complete export plus verified termination; 5 repeatable, automated export/exit with self-service status and cross-org confirmations.

Real-world Examples

- Data Transfer Project (interoperable, service-to-service export/import protocol): https://datatransferproject.dev/
- Solid Protocol (user-controlled data pods with export/import interfaces): https://solidproject.org/
- GA4GH Data Repository Service (DRS) for portable access to research data objects: https://ga4gh.github.io/data-repository-service-schemas/
- DCAT-AP (interoperable metadata for portable datasets across catalogs): https://joinup.ec.europa.eu/collection/semic-support-centre/dcat-ap
- BagIt (RDF 8493) packaging for verifiable, checksummed export bundles: https://www.rfc-editor.org/rfc/rfc8493
- ISO/IEC 19944-1 (cloud data flow and roles for portability and exit): https://www.iso.org/standard/74437.html

Method C3

DSAR/SAR Surge Drill (Rights Exercise Under Load)

Objective

Validate that mass requests to access, rectify, or erase personal data are acknowledged and fulfilled reliably across the federation, with consistent quality, clear communication, and effective escalation when backlogs occur.

Scope

A surge scenario reflecting heightened public attention or coordinated campaigns, involving multiple request types and at least two independent organizations or nodes.

Preconditions

- Defined processes and service targets for acknowledgment, clarification, and fulfillment.
- Cross-organization routing for requests touching multiple processors.
- Templates for responses and a mechanism for secure delivery of results.
- The data space operator provides a shared interface, routing, or coordination layer for rights requests, or participation agreements assign the operator a role in rights-handling.

Procedure

- Submit a large, time-bounded set of requests covering access, rectification, and erasure.
- Track acknowledgments, clarifications, and fulfillment events across participants.
- Monitor queues, backlogs, and use of escalation or fallback procedures.
- Sample responses for completeness, clarity, and appropriateness of redactions.
- Summarize throughput, bottlenecks, and prioritized improvements.

Indicators and suggested thresholds (streamlined)

- Acknowledgment and completion times: within published service targets.
- Handling consistency across participants: minimal variance for similar cases.
- Response quality: clear, complete responses meeting the request type.
- Escalation effectiveness: predictable pathways with visible ownership.

Evidence to retain

- Request logs with timestamps and routing history.
- Copies of acknowledgments, clarifications, and final responses.
- Queue and backlog metrics, plus escalation records.
- Quality review notes and action items.

Common failure modes and remedies

- Fragmented fulfillment across participants ➜ implement centralized coordination or shared case IDs.
- Incomplete responses or unclear redactions ➜ standardize response templates and redaction criteria.
- Queue saturation ➜ introduce pre-triage, automation for common cases, and surge protocols.

Scoring rubric (0–5)

0–1 ad hoc handling of rights requests; 2 basic acknowledgments with delays; 3 consistent processing meeting targets in normal conditions; 4 reliable performance under surge with clear communications; 5 surge-ready operations with automation and coordinated cross-org workflows.

Real-world Examples

- EDPB Right-of-Access operational guidance (case handling methodology): https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf
- ISO/IEC 27701 (PIMS) mapping of roles and processes for rights handling: https://www.iso.org/standard/71670.html
- NIST Privacy Framework (Identify–Govern–Control–Communicate methodology): https://www.nist.gov/privacy-framework
- Consumer Data Standards (Australia CDR) request/consent API patterns for scale: https://consumerdatastandards.gov.au/
- SRE-style runbooks and queue triage (incident/surge methodology applied to rights ops): https://sre.google/sre-book/incident-response/
- Playbooks for secure file delivery and redaction QA (records release methodology): https://support.atlassian.com/statuspage/docs/incident-communication-tips/ (communication pattern)

3. Effectiveness

PURPOSE

Effectiveness concerns whether a data space can carry out its governance framework reliably in practice. It focuses on the ability of rules, roles, and controls to operate as intended across organizations, respond to incidents and change, and support ongoing data use without breakdowns or excessive friction. An effective data space turns governance decisions into timely, coordinated action and adapts its arrangements as conditions evolve.

WHAT "GOOD" LOOKS LIKE

- **Governance execution under pressure:** decisions, approvals, escalations, and controls function predictably during incidents, surges, or novel use cases.
- **Policy-to-practice alignment:** governance rules are implemented consistently across participants and enforced by operational and technical controls.
- **Cross-organizational coordination:** handoffs between actors occur without ambiguity, duplication, or delay.
- **Corrective capacity:** incidents, complaints, or failures lead to remediation that updates governance, contracts, or systems.
- **Operational continuity:** growth in participation or data use does not undermine response times, control effectiveness, or compliance.

TYPICAL ROLES AND RESPONSIBILITIES

- **Governing body or steering committee:** approves governance rules, mandates corrective actions, and oversees system-wide performance.
- **Data stewards and governance owners:** execute governance decisions, coordinate across participants, and maintain evidence of implementation.
- **Operations and engineering teams:** operate enforcement mechanisms, monitoring, and incident response processes.
- **Compliance and legal functions:** manage regulatory obligations and external reporting under time constraints.
- **Auditors or assurance functions:** verify that governance arrangements function as intended and that corrective actions are completed.

Method E1

Accountability Chain & Role Assignment Stress Test

Objective

Verify that responsibilities are unambiguous and actionable under stress by tracing a real decision from request to outcome, showing who was accountable at each step and how authority was delegated or escalated.

Scope

One cross-organization decision (for example, high-impact access approval/denial or policy exception) with at least two hand-offs.

Preconditions

- Published role catalog (e.g., RACI/DAI) and delegation-of-authority register.
- Decision registers with approver identities and timestamps.
- Policy repository with versioning.

Procedure

- Select a recent decision; map every step to a role and named person/team.
- Validate that each step had legitimate authority per the register.
- Confirm escalation path and timing where ambiguity or conflict occurred.
- Produce an accountability chain (who decided, on what basis, and why).
- Record gaps (missing owner, unclear mandate, conflicting approvals) and assign corrective actions.

Indicators and suggested thresholds (streamlined)

- Role coverage: all steps mapped to accountable roles/persons.
- Authority match: approvals align with delegation register.
- Escalation timeliness: escalations resolved within agreed windows.
- Documentation quality: decision pack complete and verifiable.

Evidence to retain

Role catalog, delegation register excerpt, decision pack, accountability chain diagram, corrective-action log.

Common failure modes and remedies

- Dual ownership or gaps → revise RACI; add explicit tie-break and backup roles.
- Shadow approvals → require system-enforced approver lists and signature checks.
- Version drift between policy and practice → bind approvals to policy commit IDs.

Scoring rubric (0–5)

0–1 unclear roles; 2 partial mapping; 3 consistent mapping; 4 consistent mapping with timely escalations; 5 automated checks and self-serve accountability views.

Real-world Examples

- UK NHS "Caldicott Guardian" role (clear data responsibility and decision authority in health settings): https://www.gov.uk/government/publications/the-caldicott-guardian-manual
- ICO (UK) Accountability Framework (assigning roles, documenting decisions, demonstrating compliance): https://ico.org.uk/for-organisations/accountability-framework/
- RACI/Responsibility mapping used in government service delivery (roles and escalation clarity): https://www.gov.uk/service-manual/agile-delivery/writing-user-stories#roles-and-responsibilities and general method overview: https://www.atlassian.com/team-playbook/plays/roles-and-responsibilities
- EU research infrastructures with documented governance roles (ELIXIR example — data access/governance committees): https://elixir-europe.org/about-us/how-governed
- ISO 37301 Compliance Management Systems (role clarity and governance responsibilities in compliance programs): https://www.iso.org/standard/75080.html

Method E2

Policy-to-Enforcement Consistency Audit ("Policy Parity")

Objective

Test whether written policies are consistently enforced by technical controls and procedures across participants (no divergence between "paper" and "practice").

Scope

Two high-value policies (for example, purpose limitation and access approval thresholds) across at least two organizations and two control planes (human process + technical gate).

Preconditions

- Machine-readable policy artifacts or testable rules (e.g., OPA/Rego, XACML).
- Access logs and decision records; change control linking policy to deployment.

Procedure

- Extract the current policy text and the enforced rule set.
- Run parity tests (unit tests or sampled cases) comparing expected vs. actual decisions.
- Inspect change tickets to ensure rule deployments match approved policy versions.
- Record divergences and implement hot-fixes; document root causes.

Indicators and suggested thresholds (streamlined)

- Parity rate: high alignment of test cases across organizations.
- Traceability: each enforced rule links to a policy version/commit.
- Time to correct divergences: within a defined window (e.g., days).
- Negative test handling: prohibited cases correctly blocked.

Evidence to retain

Policy texts, rule artifacts, test cases and results, change tickets, parity report.

Common failure modes and remedies

- Policy text too vague → introduce normative, testable clauses.
- Drift after emergency changes → require post-incident parity checks.
- Local overrides → enforce central policy import with signed bundles.

Scoring rubric (0–5)

0–1 untested assumptions; 2 occasional manual checks; 3 routine parity tests; 4 cross-org automated tests; 5 continuous parity with signed policy supply chain.

Real-world Examples

- Policy-as-Code with Open Policy Agent (OPA) / Gatekeeper to keep runtime controls aligned with written policies: https://www.openpolicyagent.org/docs/latest/ and https://openpolicyagent.org/docs/latest/gatekeeper/
- XACML in regulated environments for fine-grained, testable authorization aligned to policy text: https://docs.oasis-open.org/xacml/xacml-3.0-core-spec-os-en.html
- Kubernetes admission control with OPA Gatekeeper (preventive policy enforcement matching governance rules): https://open-policy-agent.github.io/gatekeeper/website/
- GitOps change control linking approved policy versions to deployed rules (policy version ➜ runtime parity): https://opengitops.dev/
- NIST Internal Control assessments (mapping policy requirements to implemented controls and evidence): https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Method E3

Incident Reporting & Regulatory Notification Drill

Objective

Exercise legal and supervisory reporting obligations under time pressure (e.g., cybersecurity, privacy), ensuring signals reach competent authorities and affected parties with required content and timing.

Scope

At least one incident type requiring external notification (e.g., significant service disruption, security incident involving personal data) with cross-organization coordination.

Preconditions

- Mapped obligations (who reports what, to whom, by when) and templates.
- Evidence capture and approval workflows.
- Contact lists for CSIRTs/authorities and affected recipients.

Procedure

- Trigger a timed simulation with evolving facts.
- Produce early warning/initial notification, then intermediate and final reports as required.
- Coordinate cross-org facts, approvals, and evidence; deliver to authorities and affected parties.
- Record timing, completeness, and any retractions/updates.

Indicators and suggested thresholds (streamlined)

- Timeliness: notifications within prescribed windows.
- Completeness: required fields present; updates issued as facts evolve
- Coordination: single source of truth established quickly.
- Proof of delivery: confirmations from authorities/recipients retained.

Evidence to retain

All report versions, timelines, approvals, delivery receipts, and post-exercise review.

Common failure modes and remedies

- Unclear lead reporter → pre-assign lead roles and alternates.
- Conflicting versions of facts → adopt shared incident fact sheet with version control.
- Missed audience (e.g., customers) → maintain audience matrices and checklists.

Scoring rubric (0–5)

0–1 ad hoc reporting; 2 late or incomplete notices; 3 on-time basic reports; 4 on-time, multi-stage reporting; 5 rehearsed cross-org reporting with dashboards and evidence packs.

Real-world Examples

- NIS2 Directive multi-stage incident reporting (early warning, notification, intermediate, final): https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
- ENISA guidance on national incident reporting and CSIRT coordination: https://www.enisa.europa.eu/topics/csirt-cert-services/national-incident-reporting
- GDPR data breach notification (supervisory authority and affected-party notices): https://ico.org.uk/for-organisations/report-a-breach/ and EDPB examples: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012021-examples-personal-data-breach_en
- NCSC (UK) incident management guidance for coordinated reporting: https://www.ncsc.gov.uk/collection/incident-management
- Financial sector crisis/incident simulations (TIBER-EU threat-led exercises with reporting flows): https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html

Method E4

Grievance & Redress Mechanism Effectiveness Exercise

Objective

Assess whether complaint and redress channels are effective in practice against recognized criteria, and whether outcomes lead to corrective action and learning.

Scope

Two pathways tested end-to-end: an individual complaint (e.g., contested access decision) and a community complaint (e.g., alleged breach of a social license condition).

Preconditions

- Documented procedure; public contact points; case management tooling.
- Defined performance targets and publication norms (what is disclosed to whom and when).

Procedure

- Submit representative complaints; track acknowledgment, investigation, and outcome.
- Evaluate against effectiveness criteria (legitimate, accessible, predictable, equitable, transparent, rights-compatible, learning-oriented, dialogic).
- Verify linkage from decisions to actions (policy updates, sanctions, remediation).
- Publish appropriate summaries and close the loop with complainants.

Indicators and suggested thresholds (streamlined)

- Timely acknowledgment and predictable milestones.
- Procedural fairness (access to information; equitable treatment).
- Transparency proportional to sensitivity; learning captured and reused.
- Actionability: outcomes drive concrete remediation.

Evidence to retain

Case files, communications, decisions, implementation records, and learning notes.

Common failure modes and remedies

- Performative channels with low uptake → simplify access, protect from retaliation, publicize outcomes.
- No link to change → bind decisions to tickets and policy/version updates.
- Narrow scope → include community/collective grievances, not only individual ones.

Scoring rubric (0–5)

0–1 channel exists on paper only; 2 inconsistent handling; 3 consistent handling with basic transparency; 4 meets effectiveness criteria with learning loop; 5 independently reviewed with regular public summaries.

Real-world Examples

- UN Guiding Principles on Business and Human Rights (effectiveness criteria for non-judicial grievance mechanisms): https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf
- World Bank Grievance Redress Service (project-level complaint intake, handling, and escalation): https://www.worldbank.org/en/projects-operations/products-and-services/brief/grievance-redress-service
- IFC Performance Standard 1 (stakeholder engagement and grievance mechanisms in projects): https://www.ifc.org/wps/wcm/connect/Topics_Ext_Content/IFC_External_Corporate_Site/Sustainability-At-IFC/Policies-Standards/Performance-Standards
- OECD Due Diligence Guidance (stakeholder engagement and remediation expectations): https://mneguidelines.oecd.org/due-diligence-guidance-for-responsible-business-conduct.htm
- National ombudsman models (example: European Ombudsman — handling complaints on maladministration): https://www.ombudsman.europa.eu/en/home

Method E5

Speak-Up & Whistleblowing System Live Test

Objective

Demonstrate that concerns about misconduct can be safely reported, assessed, addressed, and closed with protections for reporters and subjects, and with traceable outcomes.

Scope

A controlled test of the speak-up channel from intake to closure, including cross-organization routing and confidentiality safeguards.

Preconditions

- Whistleblowing policy, secure intake channels (anonymous where lawful), case handling roles, anti-retaliation measures.
- Training and communication materials.

Procedure

- Submit test reports (varying severity and scope) through available channels.
- Track triage, investigation, interim controls, and resolution.
- Verify reporter protection and confidentiality controls.
- Document corrective and preventive actions and communication to stakeholders.

Indicators and suggested thresholds (streamlined)

- Intake reliability and confidentiality preserved.
- Triage and investigation within targets; fair and impartial handling.
- Protection against retaliation evidenced; reporter informed of outcome as appropriate.
- CAPA quality: corrective and preventive actions implemented and verified.

Evidence to retain

Intake logs, case files, protection assessments, CAPA records, and close-out reports.

Common failure modes and remedies

- Chilling effects or fear of retaliation → reinforce protection measures and independent oversight.
- Channel fragmentation → unify intake and routing; publish clear instructions.
- Action drift post-investigation → require CAPA tracking to closure.

Scoring rubric (0–5)

0–1 informal, risky channel; 2 basic hotline; 3 documented systems; 4 protected, timely handling with CAPA; 5 ISO-aligned systems with regular effectiveness tests and reporting.

Real-world Examples

- ISO 37002 Whistleblowing Management Systems (receive → assess → address → conclude): https://www.bsigroup.com/en-GB/standards/iso-37002-whistleblowing-management-systems/
- EU Whistleblower Protection Directive (minimum standards for safe reporting and anti-retaliation): https://eur-lex.europa.eu/eli/dir/2019/1937/oj
- NHS “Freedom to Speak Up” Guardians (speak-up network improving safety and accountability): https://nationalguardian.org.uk/
- World Bank Integrity Vice Presidency — confidential reporting channels: https://www.worldbank.org/en/about/unit/integrity-vice-presidency/reporting
- Transparency International — practical guidance and tools for whistleblowing systems: https://www.transparency.org/en/projects/whistleblowing

4. Fairness

PURPOSE

Fairness concerns the equitable distribution of benefits and burdens within a data space, including who participates, whose data is represented, who gains access to value, and who bears risk. It requires detecting and correcting disparate impact across groups, ensuring inclusive decision-making, and honoring community-defined boundaries.

WHAT "GOOD" LOOKS LIKE

- Equitable access and participation: onboarding, service levels, and decision turnarounds do not systematically disadvantage particular groups or smaller organizations.
- Outcome parity: automated and procedural decisions avoid unjustified disparities across protected or vulnerable groups; discrepancies are explainable and correctable. Depends on lawful access to group attributes and context-specific baselines.
- Collective guardrails: community conditions and social license boundaries are enforced, particularly for groups historically subject to harm or extraction.
- Group-aware privacy: re-identification and disclosure risks are assessed and mitigated at group level, not only overall.

TYPICAL ROLES AND RESPONSIBILITIES

- Governance leads and community representatives: define fairness objectives, review outcomes, and set remediation.
- Data stewards and platform operations: monitor parity, service levels, and dataset representativeness.
- Ethics and legal advisors: align fairness controls with legal protections and sector norms.
- Security, privacy, and analytics teams: assess group risks, audit models and policies, and implement mitigations.
- Auditors: verify evidence of monitoring, decisions, and remediation.

Method F1

Social License & Community Conditions Check

Objective

Assess whether proposed data uses comply with community-defined conditions for acceptable use ("social license"), and whether governance processes can resolve ambiguous or contested cases in ways that are fair, reasoned, timely, and enforceable.

Scope

Two or more realistic proposals involving affected communities:

- one clearly compliant; and
- one borderline, novel, or contested.

At least one proposal should involve datasets or use cases with heightened risk of harm, sensitivity, or unequal impact on specific groups.

Preconditions

- Documented community conditions or social license criteria, such as allowed and prohibited purposes, sensitivity thresholds, red lines, benefit-sharing requirements, or required safeguards.
- A defined escalation forum with representation from affected stakeholders and, where appropriate, independent members.
- Mechanisms to translate governance decisions into enforceable policies, contractual terms, or access rules.

Procedure

- Screen proposals against published conditions; decide clear cases.
- Escalate ambiguous cases; record deliberation, rationale, and outcome with fairness considerations explicit.
- Translate decisions into policy or access changes and deploy.
- Publish a summary to relevant participants; monitor adherence where required.
- Review any objections and decide on remediation or follow-up.

Indicators and suggested thresholds (streamlined)

- Timely screening and escalation with documented rationale.
- Enforcement fidelity: policy and access controls match the decision.
- Visibility: concise decision summaries accessible to stakeholders.
- Community satisfaction signal: absence of unresolved fairness objections after publication.

Evidence to retain

Proposal dossiers, screening notes, escalation records, policy updates, notifications, and any monitoring reports.

Common failure modes and remedies

- Vague conditions → add concrete examples, thresholds, and safeguards.
- Decisions not enforced → bind governance outcomes to technical tickets and verify deployment.
- Limited representation → broaden forum membership; include independent oversight.

Scoring rubric (0–5)

0–1 ad hoc approvals; 2 informal screening; 3 documented decisions; 4 enforceable outcomes with summaries; 5 mature cycle with monitoring and responsive adjustments.

Real-world Examples

- Responsible Data Re-use in Developing Countries: Social Licence through Public Engagement: https://www.afd.fr/en/ressources/responsible-data-re-use-developing-countries-social-licence-through-public-engagement
- CARE Principles for Indigenous Data Governance (community benefit, authority to control): https://www.gida-global.org/care
- Free, Prior and Informed Consent (FPIC) toolkits for community authorization: https://www.fao.org/indigenous-peoples/our-pillars/fpic/en/
- Citizens' Juries / Mini-publics (structured deliberation for contested data uses): https://www.jefferson-center.org/what-is-a-citizens-jury/
- Deliberative Polling (evidence + facilitated dialogue before decisions): https://cdd.stanford.edu/what-is-deliberative-polling/
- Social Impact Assessment (IAIA methodology) to assess distribution of benefits/harms: https://www.iaia.org/uploads/pdf/SIA_Guidance_Document_IAIA.pdf
- OECD Due Diligence for Responsible Business Conduct (stakeholder engagement + conditional approvals): https://mneguidelines.oecd.org/due-diligence-guidance-for-responsible-business-conduct.htm

Method F2

Algorithmic Value Alignment & Fairness Test

Objective

Assess whether automated or rule-based decision systems produce unjustified disparities across groups and respect declared individual or community preferences and constraints, and whether explanations, appeals, and corrective mechanisms function effectively in practice.

Scope

A representative set of cases where governance rules or policies are implemented algorithmically, such as ranking, recommendation, eligibility, prioritization, or access control. The scope should include:

- cases with group attributes relevant to fairness assessment, where lawful and appropriate; and
- edge cases that stress declared preferences, constraints, or social license conditions.

Preconditions

- Declared fairness objectives and relevant group definitions aligned with legal and ethical norms.
- Documented individual or community preferences and constraints, with a clear mapping to policy logic or model behavior.
- Test cases with expected outcomes, including parity checks and preference-alignment expectations.
- Mechanisms for explanation, appeal, and controlled updates to rules or models.

Procedure

- Define expected behavior based on stated fairness objectives, preferences, and constraints.
- Run test cases and representative real-world samples through the decision system; capture outcomes and explanations.
- Measure disparity metrics across groups and compare outcomes to declared preferences or constraints.
- Investigate mismatches or disparities and attribute causes to data, rules, model behavior, or implementation gaps.
- File appeals on representative mismatches and observe response quality, correction paths, and timelines.
- Apply mitigations such as policy refinements, threshold adjustments, constraints, or retraining, and re-test critical cases.

Indicators and suggested thresholds (streamlined)

- Outcome parity: disparities minimized or justified by legitimate, documented factors.
- Preference alignment: outcomes largely consistent with declared preferences or constraints.
- Explanation clarity: short, understandable reasons identifying key drivers of outcomes.
- Appeal effectiveness: timely, reasoned responses with corrective action where appropriate.
- Correction impact: measurable reduction in disparities or mismatches in re-tests within a defined window.

Evidence to retain

Parity and alignment metrics, test case definitions and results, explanations, appeal records, change logs, and post-mitigation evaluations.

Common failure modes and remedies

- Unclear fairness or preference objectives → adopt explicit parity targets or constraint formulations.
- Opaque logic → standardize explanations and surface salient factors.
- Preferences not machine-readable → encode conditions in referenceable policy or rule formats.
- One-off fixes → establish continuous testing and scheduled re-assessment tied to governance review cycles.

Scoring rubric (0–5)

0–1 undocumented or untested logic; 2 partial testing without appeals; 3 regular testing with basic explanations and appeals; 4 effective appeals and mitigations with documented updates; 5 continuous monitoring with governed updates and sustained parity and alignment.

Real-world Examples

- NIST AI Risk Management Framework (testing/monitoring/governance of impacts): https://www.nist.gov/itl/ai-risk-management-framework
- Fairlearn (parity metrics, post-processing constraints): https://fairlearn.org/
- IBM AIF360 (disparate impact tests and mitigation algorithms): https://aif360.res.ibm.com/
- Equalized Odds / Equality of Opportunity (post-processing to reduce group disparities): https://arxiv.org/abs/1610.02413
- Counterfactual Fairness (causal test for unjustified differences): https://arxiv.org/abs/1703.06856
- Calibration within groups (fairness-consistent probability calibration): https://proceedings.mlr.press/v70/pleiss17a.html

- Model Cards and Datasheets (documentation methods to encode constraints and expectations): https://modelcards.withgoogle.com/about and https://dl.acm.org/doi/10.1145/3287560.3287596
- Policy-as-Code test harnesses (OPA/Rego unit tests for governance rules): https://www.openpolicyagent.org/docs/latest/policy-testing/

Method F3

Onboarding & Authorization Parity Drill

Objective

Ensure enrollment, verification, and authorization processes do not systematically disadvantage specific groups or under-resourced organizations, and that errors are not disproportionately distributed.

Scope

A surge onboarding period covering diverse applicant types (for example, small NGOs, local clinics, academic teams, large institutions) across multiple organizations.

Preconditions

- Standard evidence requirements and role definitions.
- Metrics for time-to-onboard, error types, and manual review rates by applicant category.
- Escalation paths for applicants experiencing delays.

Procedure

- Run a controlled onboarding surge with diverse applicants.
- Measure time-to-onboard, false denials/approvals, and manual review rates by category.
- Identify bottlenecks that affect particular groups (documentation burden, assurance hurdles).
- Apply targeted mitigations (assisted onboarding, adjusted evidence pathways, clearer guidance).
- Re-test to confirm reduction in disparities.

Indicators and suggested thresholds (streamlined)

- Parity in time-to-onboard across applicant categories, within reasonable variance.
- Low and non-disparate error rates; fast remediation where errors occur.
- Accessible escalation routes with timely responses.
- Demonstrable reduction in disparities after mitigation.

Evidence to retain

Per-category onboarding metrics, error analyses, remediation records, and re-test results.

Common failure modes and remedies

- One-size-fits-all assurance → introduce tiered options with equivalent assurance outcomes.
- Documentation bias → provide assisted evidence collection and template attestations.
- Manual review choke points → expand automation for routine checks; reserve manual steps for high-risk cases

Scoring rubric (0–5)

0–1 unmeasured disparities; 2 observed but not mitigated; 3 basic parity in normal load; 4 parity sustained during surge; 5 parity with continuous monitoring and adaptive pathways.

Real-world Examples

- NIST SP 800-63A (identity proofing) with usability & equity considerations: https://pages.nist.gov/800-63-3/sp800-63a.html
- FATF risk-based approach (proportionate KYC that avoids undue exclusion): https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html
- eIDAS Levels of Assurance mapping for cross-border parity: https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation
- Accessible onboarding and documentation design (WCAG 2.2): https://www.w3.org/TR/WCAG22/
- Verifiable Credentials for portable attestations (reduce repeated burdens): https://www.w3.org/TR/vc-data-model-2.0/
- Assisted onboarding pathways (pattern libraries for inclusive service design): https://www.gov.uk/service-manual/helping-people-to-use-your-service/assisted-digital

Method F4

Privacy Re-identification Probe (Group Risk Lens)

Objective

Assess whether de-identification and disclosure controls protect small or vulnerable groups from disproportionate re-identification risk, while maintaining acceptable utility.

Scope

Datasets with identifiable small cohorts or sensitive attributes; at least one scenario with plausible external linkage

Preconditions

- Declared risk thresholds and group-aware assessment criteria.
- Access to controlled auxiliary data and utility measures relevant to intended analyses.
- Processes for targeted protections (aggregation, suppression, noise, or formal privacy techniques).

Procedure

- Identify subgroups with heightened risk (for example, small geographic or condition-based cohorts).
- Attempt linkage or inference attacks focusing on those groups, within ethical/legal bounds.
- Quantify group-specific risk and compare to thresholds; measure utility trade-offs.
- Apply targeted protections and re-test, ensuring representation is not erased.
- Document release conditions and monitoring plans.

Indicators and suggested thresholds (streamlined)

- Group-level re-identification risk at or below approved thresholds.
- Utility preserved for intended analyses; trade-offs documented.
- Protections applied consistently to affected groups.
- Ongoing monitoring for drift in risk due to new linkable data.

Evidence to retain

Risk estimates by group, attack descriptions, utility measures, protection parameters, and approved release profiles

Common failure modes and remedies

- Uniform protections that miss small-group risks → adopt targeted, group-aware methods.
- Over-suppression erasing representation → balance protection with minimum viable representation and transparency about limitations.
- Static assessments → schedule periodic re-assessment as external data landscapes change.

Scoring rubric (0–5)

0–1 overall risk only; 2 ad hoc group checks; 3 structured group risk assessment; 4 targeted protections with utility evaluations; 5 continuous group risk monitoring with stable release profiles

Real-world Examples

- k-anonymity / l-diversity / t-closeness (group-level disclosure control): https://epic.org/wp-content/uploads/privacy/reidentification/Sweeney_2015_Article_SimpleDemographicsOftenIdent.pdf , https://dl.acm.org/doi/10.1145/1217299.1217302 , https://dl.acm.org/doi/10.1145/1217299.1217301
- Differential Privacy (including group privacy considerations for aggregates): https://privacytools.seas.harvard.edu/differential-privacy
- ISO/IEC 20889 (de-identification terminology and techniques): https://www.iso.org/standard/69373.html
- UK ONS disclosure control guidance for microdata (cell suppression, thresholds): https://uksa.statisticsauthority.gov.uk/publication/the-ons-guidance-for-secure-access-to-microdata/
- ARX anonymization tool (risk estimation, transformations, utility analysis): https://arx.deidentifier.org/
- sdcMicro (statistical disclosure control for microdata): https://cran.r-project.org/package=sdcMicro

Endnotes

1 Verhulst, S. G. (2023). Operationalizing digital self-determination. *Data & Policy*, *5*, e14. https://doi.org/10.1017/dap.2023.11.

2 What are data spaces and what do they do? (2024, November 26). The ODI. https://theodi.org/news-and-events/blog/what-are-data-spaces-and-what-do-they-do/

3 Among others, see: *2. Core Concepts*. (2026). Data Spaces Support Center–Dssc.eu. https://archive.dssc.eu/space/Glossary/176554052/2.+Core+Concepts

4 United Nations. (1966, December 16). *International Covenant on Civil and Political Rights*. OHCHR; United Nations. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

5 Pajuste, T. (Ed.). (2025). Adapting Human Rights to a Digital World. In *Human Rights in the Digital Domain. Chapter 2*, Cambridge: Cambridge University Press.

6 Verhulst, S. (2026, January 10). The Case for Strategic Data Stewardship: Re-imagining Data Governance to Make Responsible Data Re-use Possible. arXiv preprint. https://arxiv.org/abs/2601.06687

7 Solove, D. J. (2024). Murky consent: An approach to the fictions of consent in privacy law. Boston University Law Review, 104, 593–639 https://www.bu.edu/bulawreview/files/2024/04/SOLOVE.pdf?utm_source=chatgpt.com

8 Marcucci, S., & Verhulst, S. (2025). Advancing Agency: Digital Self-Determination as a Framework for AI Governance. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5343658.

9 See note 1.

10 Véliz, C., & Hossein, C. (2024). *It's not personal, it's strictly business: Behavioural insurance and non-personal data impacts*. Computer Law & Security Review, 52, 105905. https://doi.org/10.1016/j.clsr.2024.106096.

11 Wachter, S., & Mittelstadt, B. (2019). A right to reasonable inferences: Re-thinking data protection law in the age of big data and AI. *Columbia Business Law Review*, 2019(2). https://ssrn.com/abstract=3248829

12 European Parliament, & Council of the European Union. (2025, February 11). Regulation (EU) 2025/327 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847. *Official Journal of the European Union*, L 2025/327. https://eur-lex.europa.eu/eli/reg/2025/327/oj/eng

13 EHDS governance is largely institutional: it creates an EU-level Board and a Stakeholder Forum including patient/consumer organizations, but the forum's function is consultative (information exchange and implementation input) rather than co-decisional.

14 Data Spaces Support Centre (DSSC). (2024). DSSC: Data Spaces Support Centre [Project factsheet]. European Commission, Digital Europe Programme. https://manufacturingdataspace-csa.eu/wp-content/uploads/2024/05/DSSC-Data-Spaces-Support-Center.pdf

15 Data Spaces Support Centre (DSSC). (2025, September 10). Data spaces blueprint v2.0—Home. https://dataspacessupportcentre.atlassian.net/wiki/spaces/BVE2/pages/1071251457/Data%2BSpaces%2BBlueprint%2Bv2.0%2B-%2BHome

16 Gaia-X European Association for Data and Cloud AISBL. (n.d.). What is Gaia-X? https://gaia-x.eu/what-is-gaia-x

17 Data Society Alliance (DSA). (n.d.). https://en.data-society-alliance.org/

18 Data Society Alliance (DSA). (n.d.). What "DATA-EX". https://en.data-society-alliance.org/data-ex/

19 Information-technology Promotion Agency, Japan (IPA). (2024, January 30). Promotion of data spaces. https://www.ipa.go.jp/en/digital/data/data-spaces.html

20 Information-technology Promotion Agency, Japan (IPA), Data Society Alliance, Robot Revolution & Industrial IoT Initiative, & The University of Tokyo. (2025, October 15). Agreement to jointly promote the dataspace technical concept as

"Open Data Spaces" [Press release]. https://www.ipa.go.jp/en/pressrelease/press20251015.html

21 Robot Revolution and Industrial IoT Initiative (RRI). (2025, November 11). Announcing the Japan Data Space Alliance (JDSA): A new collaboration accelerating data space advancement. https://www.jmfrri.gr.jp/english/8623/

22 Commonwealth of Australia. (n.d.). Delivering for all people and business. https://www.dataanddigital.gov.au/strategy/missions/delivering-for-all-people-and-business

23 Agency for Clinical Innovation (ACI), Critical Intelligence Unit. (2024, December 4). Evidence brief: Social licence for health data [Evidence brief]. https://aci.health.nsw.gov.au/__data/assets/pdf_file/0003/973470/Evidence-Brief-Social-licence-for-health-data.pdf

24 Scheibner, J., Hardin, T., Keech, W., & Richards, B. (2025). Public data sharing legislation, privacy and sharing of health and social welfare data in Australia: A legal and policy document analysis. *Data & Policy*, 7, e72. https://doi.org/10.1017/dap.2025.10038

25 Statistics New Zealand. (2019, July). Stats NZ's social licence for data stewardship [Report]. (Produced by Nielsen). https://www.stats.govt.nz/assets/Uploads/Corporate/Stats-NZs-social-licence-for-data-stewardship/Stats-NZs-social-licence-for-data-stewardship.pdf

26 Song, Z. (2023, January). Overcoming preconceptions: How big data can gain a social licence in New Zealand (NZIER Insight 105-2023) [Report]. New Zealand Institute of Economic Research (NZIER). https://www.nzier.org.nz/hubfs/Public%20Publications/Insights/NZIER%20Insight%20105%20Overcoming%20preconceptions.pdf

27 Health Data Research Network Canada (HDRN Canada). (n.d.). Social licence report. https://www.hdrn.ca/en/public/public-resources/reports/download/

28 Verhulst, S., Zahuranec, A. J., & Zable, A. (2025). Participatory approaches to responsible data reuse and establishing a social license. In S. P. Sebastião & A.-M. Cotton (Eds.), *Global public goods communication: Mapping actors, policies, and narratives* (pp. 157–172). Springer Cham. https://doi.org/10.1007/978-3-031-90667-1_10

29 Federal Office of Topography swisstopo. (2025, November 26). Federal Council adopts report on Switzerland's digital sovereignty [Press release]. https://www.swisstopo.admin.ch/en/newnsb/2VPWG78YrVs4eAVeiklQx

30 Madiega, T. (2020, July). Digital sovereignty for Europe [Briefing; EPRS Ideas Paper]. European Parliamentary Research Service (EPRS), European Parliament (PE 651.992). https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI%282020%29651992_EN.pdf. Within the Union itself, this turn found its most consequential expression in the European Commission's Technological Sovereignty Package, presented on June 3, 2026, which pairs regulatory authority with industrial investment across semiconductors, cloud and AI capacity, open source, and energy. https://digital-strategy.ec.europa.eu/en/policies/eu-tech-sovereignty.

31 Fleming, S. (2025, January 10). What is digital sovereignty and how are countries approaching it? World Economic Forum. https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/

32 Verhulst, S., Otero, B. (2026, June 8). The Triad of Tech Sovereignty: Dependency, Openness and Agency. https://sverhulst.medium.com/the-triad-of-tech-sovereignty-dependency-openness-and-agency-acc3f990b332

33 Federal Department of the Environment, Transport, Energy and Communications (DETEC), & Federal Department of Foreign Affairs (FDFA). (2022, March 30). Creating trustworthy data spaces based on digital self-determination: Report from the DETEC and FDFA to the Federal Council [Report], pp. 12-13. https://digitale-selbstbestimmung.swiss/wp-content/uploads/2022/05/Beilage-01-Bericht_EN-zu-BRA-UVEK-EDA.pdf

34 Federal Department of the Environment, Transport, Energy and Communications (DETEC), & Federal Department of Foreign Affairs (FDFA), 2022, p. 16, https://digitale-selbstbestimmung.swiss/wp-content/uploads/2022/05/Beilage-01-Bericht_EN-zu-BRA-UVEK-EDA.pdf.

35 Young, A., Verhulst, S. G., Safonova, N., & Zahuranec, A. J. (2020, November). The Data Assembly: Responsible data re-use framework [Report]. The GovLab. https://thedataassembly.org/files/nyc-data-assembly-report.pdf

36 Macaulay, E. (2025, July 21). Data and AI public engagement community of practice meeting notes [Meeting notes]. Connected by Data. https://docs.google.com/document/d/1aNg-uLH1R6QpYQIcrjqfE4n4c0-0yzNDpzialswnqVQ/edit?tab=t=0

37 Language Data Commons of Australia (LDaCA). (n.d.). https://www.ldaca.edu.au/

38 Liverpool City Region Civic Data Cooperative. (n.d.). https://civicdatacooperative.com/

39 Ada Lovelace Institute. (2021, September 7). Participatory data stewardship: A framework for involving people in the use of data. https://www.adalovelaceinstitute.org/report/participatory-data-stewardship/

40 OECD. (2022, September 24). *OECD Guidelines for Citizen Participation Processes* [Report]. https://www.oecd.org/en/publications/2022/09/oecd-guidelines-for-citizen-participation-processes_63b34541.html

41 U.S. Environmental Protection Agency. (2025, July 2). Public participation guide: Introduction to the guide. https://www.epa.gov/international-cooperation/public-participation-guide-introduction-guide

42 Indiana University. (n.d.). Ostrom Workshop. https://ostromworkshop.indiana.edu/

43 International Association for Public Participation (IAP2). (n.d.). Resources. https://www.iap2.org/page/resources

44 Federal Chancellery. (2025, January 1). Data space building blocks: Swiss data ecosystem (Version 1.1). Federal Chancellery. https://www.bk.admin.ch/dam/bk/en/dokumente/dti/Datenkosystem/Grundlagen/Data%20space%20building%20blocks_Swiss%20data%20ecosystem_V1.1.pdf.download.pdf/Data%20space%20building%20blocks_Swiss%20data%20ecosystem_V1.1.pdf

45 Contracts for Data Collaboration (C4DC), "Our Framework" (Contractual Wheel of Data Collaboration). https://contractsfordatacollaboration.org/our-framework/ ; Ancelle, J. (2024, February 29). Explanatory report: Technical data sharing—Template agreements [Report]. id est avocats Sàrl (prepared for the Swiss Federal Institute of Intellectual Property [IPI]).

46 Swiss Federal Institute of Intellectual Property. (n.d.). Model agreements. https://www.ige.ch/en/intellectual-property/ip-and-society/access-to-non-personal-data-in-the-private-sector/model-agreements

47 OECD. (2022). Building Trust to Reinforce Democracy: Main Findings from the 2021 OECD Survey on Drivers of Trust in Public Institutions. https://doi.org/10.1787/b407f99c-en.

48 Federal Office of Communications (OFCOM). (2025, January 15). Code of conduct for operating trustworthy data spaces. https://www.bakom.admin.ch/en/code-of-conduct-for-operating-trustworthy-data-spaces

49 Gille, F., Daniore, P., Maaß, L., & Zavattaro, F. (2025). Trust Performance Indicators and Trust Stress Tests: A Conceptual Proposition for Trustworthy Health Data Spaces. International Journal of Public Health, 70, 1608708. https://doi.org/10.3389/ijph.2025.1608708

50 Scottish Government. (2023, February 6). *Freedom of Information release: Citizens' Assembly of Scotland costs and Ministerial papers*. https://www.gov.scot/publications/foi-202200334314/

51 Involve. (n.d.). *How much does a citizens' assembly cost?* https://www.involve.org.uk/resources/knowledge-base/how-much-do-participatory-processes-cost/how-much-does-citizens-assembly

52 Swiss Federal Chancellery. (n.d.). *Data space «SwissHDS»*. https://www.bk.admin.ch/bk/en/home/digitale-transformation-ikt-lenkung/datenoekosystem_schweiz/monitoring-datenraume/swisshds.html

53 Williamson, O. E. (1979). Transaction-cost economics: The governance of contractual relations. *Journal of Law and Economics, 22*(2), 233–261. https://doi.org/10.1086/466942

54 Zhao, K. (2014). Forming interoperability through interorganizational information systems standards. *Journal of Management Information Systems, 30*(4), 139–172.

55 Black, J. (2008). Constructing and contesting legitimacy and accountability in polycentric regulatory regimes. *Regulation & Governance, 2*(2), 137–164. https://doi.org/10.1111/j.1748-5991.2008.00034.x

56 OECD. (2022, September 24). OECD guidelines for citizen participation processes [Report]. https://www.oecd.org/en/publications/2022/09/oecd-guidelines-for-citizen-participation-processes_63b34541.html; U.S. Environmental Protection Agency. (2025, July 2). Public participation guide: Introduction to the guide. https://www.epa.gov/international-cooperation/public-participation-guide-introduction-guide

57 U.S. Environmental Protection Agency. (2026, January 6). Public participation guide: Printed information. https://www.epa.gov/international-cooperation/public-participation-guide-printed-information

58 Research Institute for Sustainability (RIFS). (2022, August 9). Deliberative mini-publics. https://www.rifs-potsdam.de/en/

output/dossiers/mini-publics

59 Beyond Civic AG. (2025, March 28). Data Space Playbook: Governance guideline (Version v0.9) [PDF]. https://www.bk.admin.ch/dam/bk/de/dokumente/dti/DatenoekosystemSchweiz/Prototypen/Triregio/Playbook/bc_governance%20guideline_v0.95.pdf.download.pdf/bc_governance%20guideline_v0.95.pdf

60 Broadband Commission for Sustainable Development. (2025, July). Data governance toolkit: Navigating data in the digital age [Working group report]. https://www.broadbandcommission.org/wp-content/uploads/2025/07/Data-Governance-Toolkit.pdf

61 Data Spaces Support Centre (DSSC). (2025, April 4). Introduction – Key concepts of data spaces (Section 2.4: Rulebooks and data space governance frameworks). https://dssc.eu/space/BVE2/1071251613/Introduction%2B-%2BKey%2BConcepts%2Bof%2BData%2BSpaces#2.4-Rulebooks-and-data-space-governance-frameworks

62 Beyond Civic AG. (2025, March 25). Data space blueprint: Functional requirements (Version v0.9) [PDF]. https://www.bk.admin.ch/dam/bk/de/dokumente/dti/DatenoekosystemSchweiz/Prototypen/Triregio/Blueprint/bc_functional_requirements_v0.95.pdf.download.pdf/bc_functional_requirements_v0.95.pdf

63 Data Spaces Support Centre (DSSC). (2025, March 14). Contractual framework – Blueprint. https://dssc.eu/space/BVE2/1071254557/

64 Beyond Civic AG. (2025, March 28). Data space playbook: Governance guideline (Version v0.9) [PDF]. https://www.bk.admin.ch/dam/bk/de/dokumente/dti/DatenoekosystemSchweiz/Prototypen/Triregio/Playbook/bc_governance%20guideline_v0.95.pdf.download.pdf/bc_governance%20guideline_v0.95.pdf

65 Beyond Civic AG. (2025, March 28). Data space playbook: Governance guideline (Version v0.95) [PDF]. https://www.bk.admin.ch/dam/bk/de/dokumente/dti/DatenoekosystemSchweiz/Prototypen/Triregio/Playbook/bc_governance%20guideline_v0.95.pdf.download.pdf/bc_governance%20guideline_v0.95.pdf

66 Zahuranec, A. J., Chafetz, H., & Verhulst, S. (2023, November). Moving from idea to practice: Three resources for harnessing the power of data sharing agreements [Report]. Open Data Policy Lab. https://static1.squarespace.com/static/654501be298ff414eb84fa65/t/654517b98b7aad6b4aa8da57/1699026908451/A+Guide+to+Data+Sharing+Agreements.pdf

67 Data Spaces Support Centre (DSSC). (n.d.). Contractual framework. https://dssc.eu/space/BVE2/1071254557/Contractual+Framework

68 Ancelle, J. (2024, February 29). Explanatory report: Technical data sharing—Template agreements [Report]. id est avocats Sàrl (prepared for the Swiss Federal Institute of Intellectual Property [IPI]). https://www.ige.ch/fileadmin/user_upload/recht/gesellschaft/e/EN_IPI_-_Rapport_explicatif_-_id_est_avocats_fevrier_2024.pdf

69 Broadband Commission for Sustainable Development. (2025, July). Data governance toolkit: Navigating data in the digital age [Report]. https://www.broadbandcommission.org/wp-content/uploads/2025/07/Data-Governance-Toolkit.pdf

70 Federal Office of Communications (OFCOM). (2025, January 15). Code of conduct for operating trustworthy data spaces. https://www.bakom.admin.ch/en/code-of-conduct-for-operating-trustworthy-data-spaces

71 Federal Chancellery – Digital Transformation and ICT Steering. (2025, January 1). Data space building blocks: Swiss data ecosystem (Version 1.1) [PDF]. https://www.bk.admin.ch/dam/bk/en/dokumente/dti/Datenkosystem/Grundlagen/Data%20space%20building%20blocks_Swiss%20data%20ecosystem_V1.1.pdf.download.pdf/Data%20space%20building%20blocks_Swiss%20data%20ecosystem_V1.1.pdf

72 DigiSanté. (n.d.). Die Architekturvision (Die Vision von SwissHDS). https://www.digisante.admin.ch/de/architekturvision#Die-Vision-von-SwissHDS

73 DigiSanté. (n.d.). Die Architekturvision (Die Vision von SwissHDS). https://www.digisante.admin.ch/de/architekturvision#Die-Vision-von-SwissHDS

A ROADMAP FOR

DIGITAL SELF-DETERMINATION IN DATA SPACES