Geonovum Testbed 2
5.2 Research sub-topic: Data sharing under conditions

1. Executive Summary

This technical report analyzes the mechanisms, frameworks, and architectural components required to enable data sharing under conditions, a model that ensures data is exchanged securely, lawfully, and in full alignment with the provider's usage policies. It examines three foundational enablers of sovereign and policy-driven data exchange: Data Spaces, the iSHARE trust and authorization framework, and Federated Catalogue Services (FSC).

As data ecosystems expand in scale and complexity, organizations increasingly require structured, predictable, and enforceable methods to share data across domains. Conditional data sharing addresses this need by allowing data providers to specify and enforce constraints on access, purpose, usage duration, redistribution, and auditability throughout the data lifecycle.

This report synthesizes the functional, technical, governance, and legal requirements necessary to support such controlled data exchange. It also demonstrates how European-aligned frameworks collectively provide a scalable, interoperable, and trustworthy foundation for sovereign digital collaboration across sectors and domains.

2. Introduction

The transition toward a trusted and interoperable European data economy requires mechanisms that enable organizations to share data securely, predictably, and on their own terms. Traditional models of data exchange,often based on bilateral agreements, bespoke integrations, or centralized platforms,do not offer the sovereignty, scalability, or governance assurances needed for cross-sector collaboration at European scale. In response, the Data Spaces Support Centre (DSSC) has articulated a comprehensive framework for sovereign data sharing, emphasizing the ability of data providers to define, enforce, and audit the conditions under which their data may be accessed and used.

At the heart of this approach is the principle of *conditional data sharing*, whereby usage rights, restrictions, and obligations remain intrinsically linked to the data throughout its lifecycle. This principle requires a federated architecture in which identity, policy enforcement, discovery, and semantic alignment are implemented consistently across independent organizations. Data spaces,federated ecosystems built on shared governance, trust frameworks, and interoperable technical components,form the foundation for achieving this alignment.

Within these ecosystems, trust and authorization mechanisms such as iSHARE ensure that participants can authenticate one another and apply access conditions in a uniform, automated manner. Likewise, Federated Catalogue Services (FSC) provide the discovery layer that enables participants to find datasets and understand the terms under which they can be used, without compromising the sovereignty of individual providers. Together, these elements operationalize the DSSC vision by enabling scalable, policy-driven data exchange across domains, sectors, and national borders.

The following sections present the core concepts, frameworks, and challenges associated with sharing data “under conditions” in a DSSC-compliant environment. They offer a detailed overview of the legal, technical, and governance foundations needed to build and operate sovereign data spaces, culminating in recommendations to advance interoperability and trust across the European data ecosystem.

3.1 What “Under Conditions” Means

Sharing data under conditions refers to a model where the data provider retains full sovereignty over the data and determines the exact terms under which it may be accessed and used by others. These conditions are expressed through enforceable policies that accompany the data throughout its lifecycle within the dataspace. Providers may impose identity-based restrictions to ensure that only authenticated and trusted participants can request access. They can also require consumers to declare a specific purpose for use and limit data access to that purpose alone. Access may be constrained by time windows, frequency limits, or usage quotas, ensuring that consumers interact with the data only within an approved operational context. Additionally, providers may prohibit redistribution, prescribe how the data may be combined with other datasets, or mandate deletion after use. To ensure accountability, all interactions must be traceable, allowing both provider and dataspace governance bodies to verify compliance. Together, these elements create a controlled environment in which data is shared, accessed, and consumed in alignment with the provider’s rights, obligations, and expectations, reflecting the DSSC’s emphasis on sovereignty and enforceable, machine-readable usage policies.

3.2 Legal and Policy Context

The DSSC Specifications situate conditional data sharing within the broader landscape of European data regulation, emphasizing that legal compliance is a foundational requirement for dataspace participation. Several key EU frameworks shape what it means to share data under conditions. The General Data Protection Regulation (GDPR) sets strict rules for processing personal data, including requirements for consent, purpose limitation, data minimization, and protection of individual rights. The Data Governance Act (DGA) introduces governance mechanisms for data intermediaries, establishes rules for data altruism, and promotes trusted data-sharing environments across sectors. The Data Act further strengthens fairness and transparency in business-to-business (B2B) and business-to-government (B2G) data access, ensuring that contractual terms do not favor dominant players and that data holders provide access under reasonable, non-discriminatory conditions. Collectively, these regulations require data spaces to adopt robust technical and organizational measures for identity verification, access control, policy enforcement, and auditability. Within this regulatory framework, conditional data sharing is not optional but a mandated approach that ensures

lawful, ethical, and sovereign management of data throughout the dataspace ecosystem.

4. Data Spaces as Enablers of Sovereign Data Sharing

4.1 Definition of Data Spaces

A Data Space is a federated, interoperable ecosystem in which independent organizations can share data securely and confidently while maintaining full control and sovereignty over their own assets. Rather than functioning as a centralized platform or repository, a data space connects distributed data sources through shared building blocks such as common governance models, standardized technical interfaces, semantic vocabularies, and trust frameworks. This structure enables participants to discover, access, and use data under clearly defined conditions, ensuring that each organization retains authority over how its data is accessed, by whom, and for what purpose. In this sense, a data space is both a technical environment and a governance system designed to foster cross-organizational collaboration without sacrificing autonomy or legal compliance.

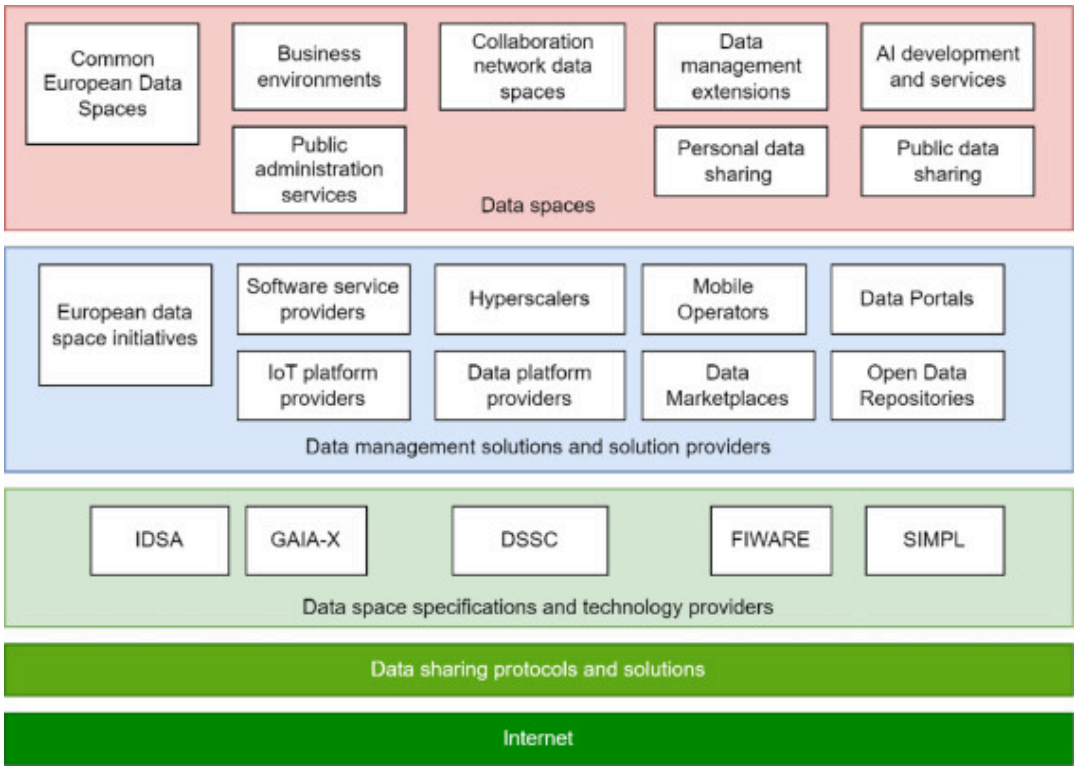

Figure 1: Background and evolution scenarios for data spaces based on the Internet and data sharing (Soininen 2025)

4.2 Four Levels of Data Spaces

The DSSC describes data spaces as multi-layered systems with interconnected dimensions that work together to guarantee trust, interoperability, and sovereignty.

At the business level, participants articulate the value proposition of the data space, define relevant use cases, and identify the incentives that motivate organizations to participate.

The governance level establishes the rules of engagement, including roles and responsibilities, certification processes, legal agreements, and compliance mechanisms that ensure consistent and trustworthy behavior across the ecosystem.

The functional level describes the operational building blocks needed to enable sovereign data exchange, such as identity management, authorization and policy enforcement, brokering and discovery services, and clearing or transaction logging functions.

Finally, the technical level defines the architecture, API specifications, security mechanisms, interoperability protocols, semantic standards, and connectors that enable automated and secure data exchange across diverse systems. Together, these layers create a coherent structure that ensures a data space operates reliably and in alignment with the DSSC reference framework.

4.3 European Alignment

Data spaces must adhere to the wider European vision of a sovereign, interoperable, and fair data economy. Their design draws on and harmonizes the work of major European initiatives, including the International Data Spaces Association (IDSA) with its IDS Reference Architecture Model (IDS-RAM), and GAIA-X, which emphasizes federated cloud and data infrastructure combined with strict policy compliance. The DSSC integrates these contributions into a coherent framework of shared building blocks, governance structures, and interoperability guidelines that can be consistently applied across both sector-specific and cross-sectoral ecosystems. Consequently, data spaces developed in line with DSSC principles are naturally aligned with EU objectives for trusted, secure, and accountable data sharing

5.1 Overview

Within a data space, the iSHARE framework plays a critical role in ensuring trustworthy and secure interactions among participants by standardizing identification, authentication, and authorization processes across a decentralized ecosystem. It provides a uniform trust and access-control model that allows organizations to reliably verify one another's identities and rights without relying on centralized authorities or pre-existing bilateral agreements. By embedding these capabilities into the dataspace architecture, iSHARE supports the broader goal of enabling sovereign, condition-based data sharing.

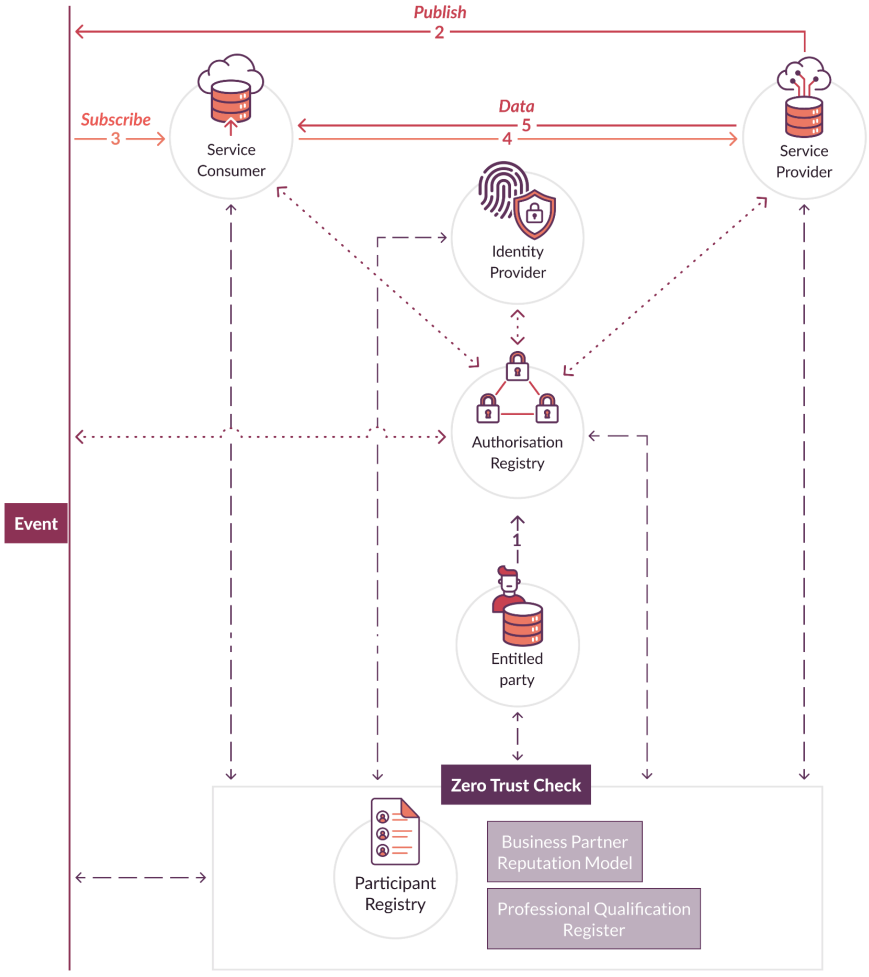

Figure 2: iSHARE Process Overview

5.2 Components

iSHARE achieves its functionality through a coordinated set of interoperable components. Identity Providers (IDPs) validate and issue trusted identities to participants, ensuring that every organization or service operating within the dataspace can be authenticated with confidence. Authorization Registries (ARs) maintain and distribute machine-readable access policies that define what each participant is allowed to do, enabling dynamic and scalable authorization management. Complementing these elements are policy enforcement mechanisms, which ensure that data is only accessed or used in accordance with the rights and restrictions defined by data providers. Together, these components create a consistent and enforceable trust infrastructure across the entire ecosystem.

5.3 Legal Framework

A foundational strength of iSHARE is its unified legal framework, which all participants must adopt as a condition of joining. This eliminates the need for complex bilateral contracting between every pair of organizations, replacing it with a shared set of rights, obligations, and compliance rules recognized throughout the dataspace. By standardizing legal terms, iSHARE significantly reduces onboarding friction, supports interoperability, and establishes clear accountability for all participants.

5.4 Impact

The combined technical and legal foundations of iSHARE enable data providers and consumers,many of whom have no prior relationship,to interact automatically and with mutual trust. Because identity, authorization, and compliance mechanisms are standardized, participants can rely on the dataspace infrastructure to validate who is requesting data and under what conditions. This trust-by-design approach not only improves operational efficiency but also accelerates the creation of scalable, cross-organizational data ecosystems. As a result, iSHARE becomes a key enabler for sovereign, secure, and policy-driven data exchange within DSSC-compliant data spaces.

6. Federated Catalogue Services (FSC)

6.1 Overview

Federated Catalogue Services (FSCs) are essential building blocks in DSSC-compliant data spaces, enabling participants to discover datasets, services, and related assets across a distributed ecosystem without centralizing metadata or compromising data sovereignty. Instead of aggregating information into a single platform, FSCs federate metadata queries across multiple catalogues operated by different participants. This approach ensures that organizations maintain control over their own metadata while still contributing to a unified discovery experience for data consumers, thereby supporting transparency, interoperability, and decentralization.

6.2 Role in Conditional Data Sharing

In a data space where data is shared under defined conditions, FSCs play a pivotal role in making those conditions visible and actionable. They allow data providers to expose metadata in a controlled manner, ensuring that only authorized or eligible

participants can view specific datasets or offers. FSCs also make usage policies discoverable by associating descriptive and machine-readable constraints,such as licensing terms, access rights, and purpose limitations,with individual data assets. Furthermore, they link metadata entries to technical endpoints, contractual references, or authorization mechanisms, enabling consumers to understand not only what data exists but how it can be legitimately accessed and used. Through these capabilities, FSCs serve as the entry point into a sovereign, policy-driven data-sharing workflow.

6.3 Standards

To ensure interoperability and consistency across sectors and domains, FSCs rely on widely accepted metadata standards and semantic models. The DSSC Specifications highlight DCAT-AP as the primary metadata schema for dataset descriptions and catalogue interoperability within European data ecosystems. In domains requiring rich semantic modelling or real-time context data. FSCs also integrate seamlessly with trust frameworks such as iSHARE, ensuring that discovery processes respect identity verification, access constraints, and policy enforcement requirements. Together, these standards enable FSCs to function as a coherent and interoperable discovery layer within the broader dataspace architecture.

7. Technical and Semantic Interoperability

In a data space, interoperability is a foundational requirement that enables participants to exchange data securely, meaningfully, and in accordance with agreed conditions. Achieving this interoperability requires alignment across several dimensions. First, policy languages such as ODRL, XACML, and Rego are essential for expressing machine-readable usage constraints, obligations, and permissions that can be consistently interpreted and enforced across heterogeneous systems. Second, semantic standards like RDF and JSON-LD ensure that data from different providers can be understood and integrated by consumers, regardless of variations in internal data models. These semantic technologies enable shared meaning, support linked data principles, and promote cross-domain reuse. Finally, communication protocols,including RESTful APIs, OAuth2-based authorization flows, and the IDS Communication Protocol (IDS-CP),provide the secure technical channels through which data is requested, accessed, and exchanged. When implemented together, these standards create a robust interoperability layer that allows distributed systems to interact cohesively within a federated data ecosystem, ensuring that data sharing remains predictable, compliant, and technically seamless.

8. Challenges and Gaps

Although the DSSC Specifications provide a robust foundation for building federated, sovereign data spaces, several practical challenges and gaps still hinder widespread adoption and seamless operation. These challenges span technical, organizational, legal, and semantic dimensions, and they often manifest differently across sectors, making interoperability and trust difficult to achieve at scale.

From a technical perspective, one of the most persistent issues is the inconsistent implementation of policy enforcement mechanisms. While machine-readable usage conditions,such as those expressed in ODRL or XACML,form the cornerstone of sovereign data exchange, many organizations lack mature tooling to interpret and enforce these policies reliably. As a result, the same policy may be applied differently across connectors, platforms, or domains, undermining trust in cross-organizational data flows. Additionally, not all participants have equally advanced identity management or authorization systems, creating uneven security baselines and reducing predictability in the ecosystem.

On the organizational side, data spaces depend heavily on trust among participants, yet many organizations enter these ecosystems without any prior relationship or shared operational history. Establishing confidence in the behavior, reliability, and compliance of unfamiliar actors requires rigorous onboarding procedures, accreditation processes, and continuous monitoring,capabilities that are still emerging in many sectors. Fragmentation in governance maturity also causes friction, as some domains lack the institutional structures needed to enforce shared rules or resolve disputes efficiently.

The legal challenges are equally significant. Even though European regulations such as GDPR, the Data Governance Act, and the Data Act aim to harmonize data rights and obligations, their interpretation varies across member states and industries. Organizations often differ in how they understand concepts such as lawful basis for processing, usage rights, liability boundaries, and contractual obligations in cross-border contexts. This uncertainty can discourage organizations from sharing data or lead to overly restrictive agreements that limit interoperability and reuse. Moreover, aligning contractual frameworks with automated policy enforcement remains a complex and evolving task.

Finally, semantic gaps continue to impede effective data discovery, integration, and reuse. Data providers frequently describe their datasets using different metadata schemas, vocabularies, taxonomies, or domain ontologies. Without semantic alignment, data consumers cannot easily assess dataset relevance, understand variable meanings, or merge data from multiple providers. Even when standards like DCAT-AP are adopted, their extensions and domain-specific profiles may differ, resulting in inconsistencies that require manual mapping or transformation.

Addressing these challenges is essential for scaling data spaces across Europe. Achieving true interoperability will require not only continued technological innovation but also stronger governance models, clearer legal guidance, and concerted efforts to harmonize semantic standards. Only through coordinated progress across all four dimensions can data spaces deliver on their promise of a trusted, sovereign, and efficient European data economy.

9. Recommendations

In line with the DSSC Specifications, several recommendations can support the effective development, deployment, and governance of sovereign data spaces. For implementers, the most critical first step is to begin with small, well-defined use cases that demonstrate clear value and can be scaled incrementally. Early success builds confidence among participants and allows technical and governance models to mature in controlled environments. Implementers should also adopt established trust frameworks such as iSHARE, which provide standardized mechanisms for identity verification, authentication, authorization, and legal alignment. Leveraging Federated Catalogue Services (FSC) is equally important, as they enable sovereign metadata distribution and controlled discovery of datasets without centralizing information.

For policymakers, fostering participation in data spaces requires both regulatory clarity and strategic incentives. Policymakers should promote consistent interpretation of data usage rights, licensing terms, and obligations across sectors and member states, reducing uncertainty for organizations that must comply with complex legal frameworks such as the GDPR, the Data Governance Act, and the Data Act. Incentive schemes,such as funding programs, public-sector participation, or aligned procurement practices,can further accelerate adoption and encourage organizations to embrace interoperable data-sharing mechanisms.

For standards bodies, the focus should be on harmonizing the technical and semantic foundations that enable interoperability across data spaces. This includes aligning metadata schemas, vocabularies, ontologies, and policy expression languages to reduce fragmentation between domains. Standards bodies should also support robust certification frameworks and interoperability testbeds, which provide implementers with the tools to validate compliance, test cross-system compatibility, and ensure that technical components behave consistently across federated ecosystems. Through these combined efforts, the European data space landscape can evolve into a cohesive, trusted, and scalable environment for sovereign data exchange.

10. Conclusion

Conditional data sharing, as envisioned in the DSSC Specifications, requires coordinated alignment across legal, technical, functional, and governance dimensions. Organizations must operate within a shared framework of trust, interoperability, and sovereignty, ensuring that data can be accessed and used only under clearly defined conditions. Data Spaces provide the overarching federated architecture that enables this alignment by combining common governance rules with distributed technical infrastructure. Within this framework, iSHARE plays a critical role by standardizing identity, authentication, authorization, and legal agreements, enabling participants to trust one another even without prior relationships. Federated Catalogue Services (FSC) further support this ecosystem by making datasets discoverable in a controlled, sovereign manner and exposing the policies and terms under which they can be accessed. Together, these components form a cohesive foundation for a secure, scalable, and interoperable European data economy,one in which organizations can collaborate effectively while preserving full control over their data assets. As data spaces continue to mature across sectors, this integrated approach will be essential for realizing the full potential of trustworthy, cross-organizational data exchange in Europe.

Building on these established foundations, the future success of conditional data sharing relies heavily on integrating emerging technologies and refining policy execution. Specifically, advancements in decentralized identity solutions (DIDs) and verifiable credentials (VCs) promise to enhance the granularity and sovereignty of access control within data spaces, allowing individuals and organizations to manage their authorization credentials with greater autonomy. Furthermore, the

development of sophisticated Policy Decision Points (PDPs) and Policy Information Points (PIPs) that can operate across federated, multi-cloud environments will be crucial for guaranteeing real-time, non-repudiable policy enforcement, thereby closing the gap between legally binding agreements and automated technical controls. Addressing these technical refinements while maintaining focus on semantic alignment and simplified legal compliance will ensure that Data Spaces remain the trusted, scalable platform for Europe's data economy.