DATA SPACES SUPPORT CENTRE

March 2026

Forward looking (research) agenda Data Spaces Blueprint

Publisher

Data Spaces Support Centre (DSSC)
c/o Fraunhofer-Gesellschaft zur Förderung
der angewandten Forschung e. V.
Hansastr. 27c
80686 Munich
Germany

Copyright

Consortium

Big Data Value Association
Capgemini Invent
Fraunhofer-Gesellschaft
Gaia-X
International Data Spaces Association
KU Leuven
MyData Global
SITRA
TNO
University of Galway
VTT

Contact

www.dssc.eu
contact@dssc.eu

Funded by
the European Union

The Data Spaces Support Center receives funding from the European Union Digital Europe Programme under grant agreement n° 101083412:

Authors

Matthijs Punter – TNO
Claire Stolwijk – TNO
Frank Drijfhout – TNO

Contributors

Table of Contents

1. Introduction

Europe's ambition to build a trustworthy, interoperable, and value-driven data economy is entering a decisive new phase. With the publication of the DSSC Blueprint version 3.0, a consolidated foundation now exists for the organisational, business, governance and technical capabilities required to develop and operate Common European Data Spaces. Yet, as data spaces move from experimentation toward large-scale deployment, the ecosystem faces new challenges and opportunities shaped by fast-evolving technologies, maturing business models, and an expanding regulatory landscape. This document provides a **forward looking research agenda** that builds on the insights of the existing DSSC Blueprint and identifies the areas where further innovation, harmonisation, and strategic development are required (See Figure 1 for the DSSC Blueprint[1]). Input for this agenda is collected via expert input, the Community of Practice and future research sections in former versions of the Blueprint.

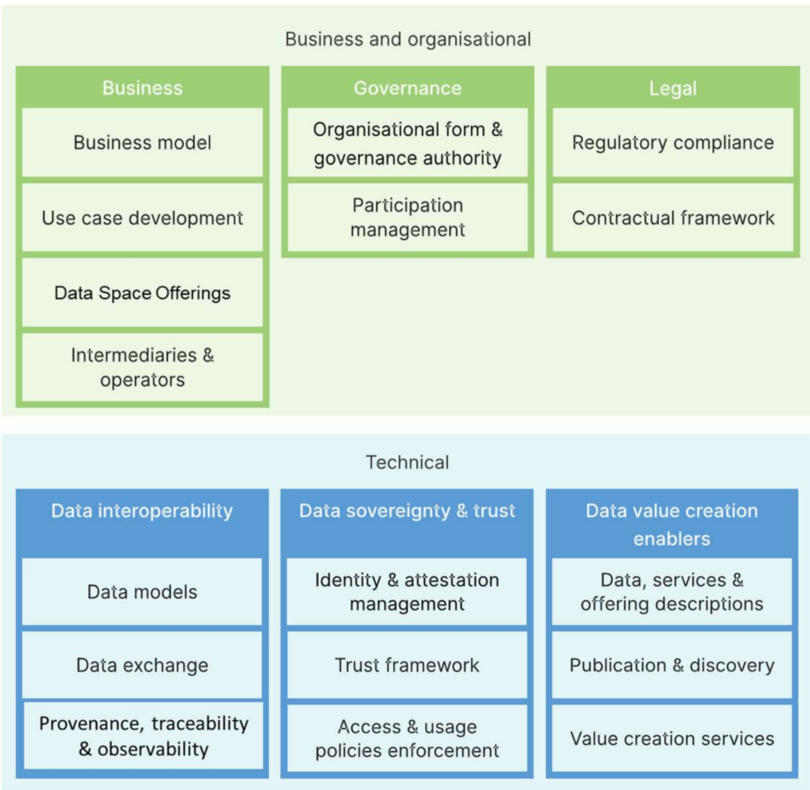

Figure 1 DSSC Blueprint

The objective of this agenda is to guide policymakers, governance authorities, intermediaries, technology providers, and domain communities in understanding **what needs to be explored next** to ensure that data spaces can scale sustainably, remain interoperable, and deliver meaningful economic, societal, and environmental value. While the Blueprint defines what a data space is and

[1] DSSC Blueprint: https://blueprint.dssc.eu/

which building blocks are required, this research agenda focuses on **how these building blocks must evolve** in the coming years.

Technological developments play a central role in this evolution. Core protocols such as DCAT, ODRL, DSP, and DCP/OID4VC are maturing and progressing toward international standardisation, significantly strengthening interoperability. Within Europe, harmonised standards are being developed to facilitate compliance with the Data Act. But there are evolutions as well: AI is reshaping semantics, metadata creation, and data exchange mediation, and it introduces new requirements for trust, provenance, and model governance. At the same time, machine interpretable rulebooks and trust frameworks will enable higher levels of automation and facilitate cross-dataspace collaboration. These developments require updates of architectural patterns, guidance, and robust governance practices in future versions of the blueprint.

On the business side, data spaces increasingly depend on clear and quantifiable value propositions. This is a key theme for 'season 2' of data spaces. Scaling requires more than technical compatibility: it requires viable business models for both data space operators and participants, new mechanisms for multiparty value creation, and the ability to replicate and expand proven use cases. The growing role of intermediaries and operators, the emergence of horizontal multi data space services, and the professionalisation of use case orchestration highlight the need for research into sustainable operating models, pricing strategies, incentive alignment, and ecosystem economics.

Legally, the landscape is evolving just as rapidly. The Data Act, Data Governance Act, sectoral regulations, and emerging implementing legislation introduce new obligations for data sharing, governance, and compliance. Through the omnibus it is expected that simplification will take place. Ensuring that data spaces remain aligned with these changing regulatory requirements demands continuous monitoring and updated contractual frameworks. Future research must examine how AI can support regulatory awareness, how machine-readable policies can streamline compliance, and how governance authorities can collaborate across sectors to build a pan European network of trust.

Together, these technological, business, and legal developments underline the need for a comprehensive and forward looking research agenda towards future versions of the DSSC Blueprint. This document addresses that need by outlining the priority questions, development directions, and structural innovations that will determine how data spaces evolve over the coming years. It aims to ensure that data spaces remain futureproof, interoperable, trustworthy, and economically sustainable forming the backbone of a connected European data ecosystem.

2. Business and Organisational building blocks

2.1 General

Over the past years, data spaces have evolved from an emerging concept into a structured approach for enabling trusted, sovereign, and scalable data sharing across organisations, sectors, and borders. Early Data space Blueprints were primarily concerned with establishing the technical feasibility of data exchange while preserving control for data holders. Business and organisational aspects were present but became more explicit and expansive over time.

As data space initiatives progressed from conceptual designs to pilots and early deployments, it became increasingly clear that technology alone could not achieve data sharing at scale. The success of data spaces depends fundamentally on how organisations collaborate, how trust is governed, how responsibilities are allocated, and how value is created and shared. This realisation has driven a gradual but significant maturation of the business and organisational building blocks across the Data space Blueprint versions.

Later blueprints began to explicitly acknowledge data spaces as multi-party ecosystems rather than technical infrastructures. This marked an important shift: data spaces were increasingly understood as socio-technical systems that require clearly defined organisational structures, governance models, and shared rules. As a result, business and organisational building topics such as role definitions, participation models, onboarding processes, and governance bodies were introduced and refined.

2.2 Trends

Looking ahead, the next phase of data space development will focus on harmonisation, standardisation, automation and scaling of business and organisational elements of the data space.

First, there is a need for greater standardisation and harmonisation across data spaces, including common governance patterns, and contractual modules. This will allow organisations to participate in multiple data spaces with reduced complexity and overhead.

Second, automation will become more prominent thanks to AI. Governance rules, participation agreements, and data sharing contracts are expected to be increasingly generated and managed automatically, based on machine-readable policies and up-to-date legal requirements. This will support dynamic, large-scale data sharing while maintaining trust and compliance.

Third, data spaces are likely to transition from project-based initiatives to more institutionalised and sustainable organisational structures, with clear accountability, long-term financing models, and continuous maintenance of legal and organisational frameworks.

In summary, the evolution of data spaces reflects a shift from technology-centred experimentation towards mature ecosystems with scale and robust business and organisational foundations. The next steps will be decisive in embedding data spaces as a durable element of the data economy, capable of supporting innovation, compliance, and collaboration at scale.

These trends lead to new (research) questions, which will be discussed per business and organisational building block in the next sections. We also provide an approach for these questions. This is not an exhaustive list of questions, but some relevant questions that needs to be covered in the near future.

2.3 Impact on Business building blocks

2.3.1 Business Model

Key questions

The future of the dataspace business model will be shaped by a shift from experimentation to economically sustainable, ecosystem-based value creation. An important future goal of the business model building block is to move to measurable quantifications of the business model of the data space governance authority and the value propositions and data space participants. This quantification makes the value propositions more concrete, and will help data space candidates to participate and scale data spaces faster. There is an existing gap in the literature with regards to the quantification, for which the following questions needs to be answered:

- *What exactly should be quantified for a data space business model?*
- *Where to begin when quantifying the business model?*

A data space is not 'a firm' but an ecosystem with a governance structure. So its business model is based on the following principles:

- Value creation: What new value becomes possible through data sharing / interoperability?
- Value capture: Who captures what share of that value, through what mechanisms (fees, cost avoidance, productivity, risk reduction, innovation)?
- Value distribution & fairness: Are incentives aligned so participants continue to contribute?

That means that the quantification needs to take place with these principles in mind.

A data space is a multi-sided ecosystem in which value is created and captured across data providers, data users, and enabling service providers, under a governance authority. The DSSC Business Model building block indicates that data space business models are also multi-sided, requiring alignment of incentives, and emphasising that the model is operationalised via governance / rulebook and needs continuous monitoring.[2] The Business Model building block also Indicates that two business model

[2] DSSC Blueprint: https://blueprint.dssc.eu/

layers needs to be taken into account: the data space layer and the participant layer. This leads to two quantification layers:

1. Data space (ecosystem/platform) economics to quantify the value proposition on data space level.
2. Participant (firm-level) economics to quantify whether the participants have a clear value proposition, or formulated differently what is in it for them in terms of cost savings, risk reduction, quality improvement, increased efficiency etc.

Not all value propositions are easy to quantify such as improved customer satisfaction or better quality, but quantifying as far as possible can make the expected value propositions more concrete.

Approach

To quantify the business model at data space level and the value propositions at participant level, a clear distinction should be made between ecosystem-wide value creation and role-specific benefits.

- At data space level, quantification focuses on the aggregated measurable outcomes such as total economic value generated (e.g. revenues at data space level, shared infrastructure cost savings, reduced transaction and compliance costs, increased data reuse, and innovation enablement), balanced against the fixed and variable costs of governance, operation, and coordination to demonstrate overall sustainability.
- At participant level, value propositions are quantified by mapping each role (data provider, data consumer, intermediary, service provider) to concrete benefits—such as new revenues from data products, operational efficiency gains, risk and compliance cost reduction, or improved time-to-market and comparing these to participation and operational costs.

By aligning these two perspectives through transparent metrics and contribution models, data spaces can demonstrate both collective viability and individual return on participation.

2.3.2 Use Case Development

Key questions

Developing impactful use cases is central to the success and sustainability of any data space. Existing use cases show that use cases are the primary mechanism through which economic, societal, or environmental value is created.

Use case orchestrators and value coaches play an important role in making use cases successful. Use case orchestrators focus on how a specific use case is realized: they coordinate actors, align requirements, and guide the use case from idea to implementation within the data space. Value coaches help stakeholders identify, articulate, and validate the business, societal, or strategic value of data sharing.

Further stimulating the implementation and scaling of data spaces based on use cases requires the expansion of the role of the use case orchestrator and makes bottom up value coaching more important.[3] That brings up the following questions:

- *How does the expanded role for the use case orchestrator look like?*
- *What is the advantage of bottom up value coaching compared to a top down approach?*

Approach

These questions can be answered by observing the existing developments of data spaces and the roles of orchestrators and value coaches.

<u>1. Expanding the Orchestrator's role</u>

The orchestrator is as a data space participant accountable for a specific use case, responsible for establishing business rules, aligning participants, and ensuring operational viability. But the evolving data space ecosystem demands more. Three drivers in particular push the orchestrator into a broader, more strategic role:

- <u>Increasing complexity of multi-party value creation</u>: Use cases often contain multiple data products, value creation services, and sometimes entire service bundles. This increases the orchestration challenge: the orchestrator must guide participants not only on what data to share but also on how to work together to deploy meaningful value generating logic.
- <u>The need for consistent governance & viability</u>: Orchestrators support the governance authority by clarifying viability, value, and key design choices. Orchestrators can explore details with participants and evaluate which choices are feasible and aligned with the data space strategy.
- <u>Continuous Improvement as an ongoing responsibility:</u> Use case development is not a one off process. It follows a lifecycle of identification, refinement, implementation, and continuous improvement. Orchestrators increasingly lead this lifecycle, ensuring that operational use cases evolve with user feedback, data flows, and performance insights.

<u>2. Bottom up value coaching instead of top down planning</u>

Traditional top down use case selection, where central bodies predefine priorities, faces limitations in dynamic ecosystems. The starting point is understanding real user needs, which are often diverse and discovered through co-creation. A bottom up value coaching model focuses on empowering participants to diagnose their own challenges, opportunities, and data driven value levers. This bottom up approach brings several advantages:

- <u>Stronger alignment with real needs and requirements:</u> Instead of building for assumed requirements, data space participants co-create use case scenarios to fulfil a specific need such as lowering costs, increasing quality and stimulating efficiency within their value chain. This approach strongly aligns with the described first step in the blueprint of identifying and tracking use case scenarios.

---

[3] Based on expert input.

- Accelerating viable use case refinement: Bottom up approaches improve the refinement stage where purpose, participants, and data flows are fleshed out by making users active contributors rather than passive recipients. This increases viability and ownership.
- Enabling scalable adoption mechanisms: Once one supply chain or domain operationalises a use case, others can adapt it, creating a replicable pattern as use and replication is a core mechanism for scaling.
- Stimulating organic growth of the data space: Continuous monitoring of successful, emerging, or abandoned use cases helps shape the ecosystem without imposing rigid top down direction. Tracking performance and user feedback are very important for the stimulation of the growth of the data space.

2.3.3 Data space offerings

Key questions

Data spaces can become AI enablers making it feasible to build, train, evaluate, deploy and govern AI across organisations without centralising sensitive data. Some AI projects waste time on finding, understanding, and mapping data. Data space offerings can mitigate that by making data accessible and reusable.

Turning data into a data product means transforming and packaging it into something that is consumable and marketable. In this way data productisation for AI becomes possible and turns datasets into ' AI model-ready assets'. Advantages of data space offerings for AI are that they are:

- Reusable across teams and use cases
- Composable (combined with other data products)
- Versioned so models can be reproduced and compared
- Discoverable via catalogues and standardised descriptions

Although the data space offerings have the potential to enable AI this is often not happening yet. In most cases, data spaces are used first for data exchange, compliance, and interoperability, with AI as a secondary or future use case. This pattern is consistent across roadmaps and community surveys, which identify AI enablement as important but not yet dominant. Especially for model training and finetuning the use of data space is rare. Although data spaces are increasingly seen as infrastructure for AI data spaces often lack AI-ready data space offerings and data products. That leads to the following questions:

- *What makes a data space offerings AI-ready in terms of quality, metadata, lineage, licensing, evaluation?*
- *How can the use AI be stimulated by the use of data space offerings?*

Approach
If a data space offering (a dataset, data product, or data service published through a data space) is AI ready depends on the intended use. Related to the intended use a repeatable assessment is needed that checks:

1. Fitness for machine learning / generative AI use,
2. Machine-actionable metadata & policies,
3. Evidence that can be audited.

Data spaces stimulate AI use not by passively hosting data and data space offerings, but by actively shaping an environment where data products for AI are easy to find, safe to use, trusted, legally compliant, economically attractive, and continuously improvable. This requires coordinated action across technical, governance, economic, and community layers of the data space ecosystem.

See also section 3.5.1 and 3.5.2 on the technical perspective to data products and their publication in a data space.

2.3.4 Intermediaries and operators

Key question
The role of data space intermediaries and operators is shifting from that of perceived brokers or gatekeepers towards neutral enablers of trust, compliance, and scalability within data ecosystems. Rather than owning, aggregating, or monetising data themselves, European intermediaries and operators increasingly focus on reducing complexity for data space participants by providing enabling services such as identity, catalogues, policy enforcement, logging / clearing, onboarding, trust. As data spaces mature, intermediaries and operators become less visible in individual data transactions but more critical at ecosystem level, acting as stabilising infrastructure that enables decentralised data sharing to function reliably, legally compliant, and at scale without re-centralising control or value creation.

Successful intermediaries and operators design enabling services as horizontal, reusable services that are configured per data space. The service model of data space intermediaries is likely to evolve from being tied to a single ecosystem or sector towards a multi-data-space-oriented model that operates horizontally across domains and initiatives. This evolution leads to the following question:

- *How does the service offering for groups of data spaces looks like based on sector agnostic services to avoid high costs and slow scaling?*

Approach
Instead of delivering bespoke services tailored to one specific data space, intermediaries will increasingly offer standardised, interoperable services such as identity and trust services, automated contracting, consent and policy management, compliance support, and operational hosting, that can be used across multiple data spaces simultaneously. This shift allows intermediaries to achieve

economies of scale, reduce duplication, and support participants that operate in several data spaces at once, while maintaining neutrality and avoiding ecosystem lock-in. As a result, intermediaries and operators transition from project-based service providers to cross-data space infrastructure actors, enabling consistency, efficiency, and scalability in an increasingly interconnected data space landscape. That might require some shift In their service model by:

1. Starting from common data-space functions, not sectors or silo perspectives and keeping developments in mind such as cross-data space interoperability.
2. Bundling services into service packages: For practical adoption services are often bundled.
3. Aligning pricing with reuse: Reusable services should be priced as: subscriptions (per participant, per month), usage-based (per transaction etc).

See also paragraph 3.2.5 on the development of generic services, which might be offered by intermediaries or generic service providers.

2.4 Impact on Governance building blocks

2.4.1 Organisational form and governance authority

Key question

Data spaces (health, mobility, energy, finance, research, etc.) are each governed by their own Data Space Governance Authority (DSGA), operating at different levels and domains. A DSGA is accountable for creating, maintaining, and enforcing the governance framework for a particular data space. In other words, DSGAs are the central governance nodes for each data space initiative. These authorities are often similar, but also differ from each other in mandate, data scope, and jurisdiction. To come to one European data union cooperation between different DSGAs becomes key. The effectiveness, trustworthiness, and scalability of data spaces therefore depends on the interrelations between these DSGAs. The related question that needs to be answered is:

- *How should the network of DSGAs be organised to ensure an effective multi-level governance structure?*

Approach

Based on empirical insights it becomes clear that DSGAs connect upward (to domain and cross-sector governance) and sideways (to other DSGAs for interoperability). Rather than one authority controlling all, DSGAs tend to form federations where they mutually recognise: each other's conformance, shared interoperability mechanisms, and shared trust requirements. A network of DSGAs usually looks like a federated, multi-layer structure. Not a single hierarchy. In practice it's a mesh of governance bodies connected by shared rulebooks, mutual recognition, and common trust / interoperability mechanisms. Each (sector) data space keeps its DSGA responsible for its own rulebook.

To stimulate networking between data space governance authorities, it is essential to create structured, recurring collaboration mechanisms that go beyond ad-hoc exchanges. This can be achieved by establishing regular cross-data space forums and communities of practice where governance authorities share experiences, align interpretations of regulatory and organisational principles, and discuss emerging challenges. Joint working groups on topics such as governance models, certification, contractual frameworks, and compliance can foster mutual learning and convergence, while shared documentation spaces and reference models help capture and reuse best practices. Complementing this with peer-to-peer exchanges, joint pilots, and coordinated representation in policy dialogues will strengthen trust, reduce fragmentation, and gradually build a coherent network of governance authorities capable of supporting interoperable and scalable data spaces. However, structural networking alone is not sufficient. For a federated governance ecosystem to function effectively, DSGAs also require practical implementation guidance that translates governance principles into operational structures. This includes structured implementation frameworks, model rulebooks, decision-right allocation templates, participation agreements, legal form options, and step-by-step methodologies for aligning the governance design with the technical architecture, regulatory requirements, and business models.

An outcome of these structured recurring collaboration mechanisms can be the interconnection of DSGAs through a so-called Federation Governance Layer that aligns rules, ensures interoperability, and provides shared governance implementation baselines. This body provides the common governance baseline that makes inter- data space federation possible.

Within sectors the networking between DSGAs is already happening for instance within the mobility and health data spaces. Networking of DSGAs between different sectors is more rare and needs to be stimulated based on the aforementioned approach. To support cross-sector scalability, common operational toolkits and reference governance artefacts should be developed and shared across DSGAs. Standardised rulebook templates, compliance frameworks, onboarding procedures, and governance-technical alignment models can significantly reduce fragmentation and increase legal certainty. Without such operational convergence, federated governance risks remaining a structural concept rather than an executable reality.

2.4.2 Participation management

Key question

Participation management governs the definition of roles and responsibilities within a data space as well as the onboarding, lifecycle management, and offboarding of participants. Participation Management spans two interdependent layers:

Operational Processes: Human-driven governance activities such as:

- Defining roles and responsibilities (data providers, recipients, data intermediaries, data rights holders).
- Onboarding and offboarding workflows, including eligibility checks and contractual acceptance.

- Decision-making on compliance, risk management, and participant obligations.
- Continuous review and adaptation of governance frameworks.

Technical Processes: Implemented via building blocks (BBs) and automated systems, such as:
- Registries**:** Maintaining authoritative participant lists and trust anchors.
- Identification and Attestation Systems**:** Credential issuance, verification, and lifecycle management.
- Onboarding Tooling**:** Digital acceptance of terms, automated compliance checks, and secure credential provisioning.
- Monitoring and Audit Services: Observability of transactions, anomaly detection, and traceability.

That means participation management can involve lengthy, resource-intensive workflows, particularly during onboarding and compliance verification. If designed independently for each data space, participation management risks becoming fragmented, duplicative, and inefficient, thereby limiting scalability at European level. So the related question is:

- *How can participation management be organised to ensure efficiency, scalability, and cross–data space interoperability while preserving governance integrity?*

Approach

AI can automate participation management in data spaces by acting as an intelligent orchestration layer that supports onboarding, verification, lifecycle management, and compliance monitoring of participants. By analysing organisational profiles, certifications, declared roles, and intended data uses, AI can automatically assess eligibility against the data space rulebook, recommend appropriate participation agreements, and trigger the required contractual and governance steps. During operation, AI can continuously monitor changes, such as new legal requirements, expired certifications, or shifts in participant behaviour and proactively update access rights, notify governance authorities, or initiate revalidation processes. This reduces manual effort, accelerates participation, and ensures that participation management remains consistent, scalable, and aligned with the evolving governance and trust requirements of the data space ecosystem.
Within a federated governance architecture, such intelligent participation management mechanisms could be shared or mutually recognised across DSGAs, thereby reducing duplication and strengthening cross-sector scalability.

2.5 Impact on Legal building blocks

2.5.1 Regulatory compliance

Key questions

The regulatory compliance building block ensures that the governance and operational design of a data space remains aligned with applicable legal frameworks at EU and Member State level. Specifically, it covers the identification, interpretation, and operationalisation of applicable EU and Member State law, including binding legislation, implementing measures, and relevant soft-law instruments. Given the constantly expanding and developing legislation the questions are:

- *How can data spaces establish continuous regulatory monitoring mechanisms in an environment of expanding and evolving legislation?*
- *How can regulatory awareness be systematically translated into enforceable compliance structures?*

To answer these questions the following approach is suggested.

Approach

Continuous regulatory alignment requires institutionalised monitoring processes, legal expertise, structured internal compliance workflows, and clearly defined accountability mechanisms. Within such a framework, AI-based systems can support regulatory monitoring by assisting with large-scale legal text analysis and change detection. AI should not replace the governance authority but function as a decision-support and orchestration mechanism under clearly defined accountability structures. AI systems can continuously scan large volumes of regulatory material, distinguish substantive from editorial changes, and flag developments likely to affect data space governance. AI-generated alerts and regulatory mappings must remain traceable and auditable to ensure transparency and accountability. Final legal interpretation, policy adaptation, and rulemaking authority must remain with the governance body.

A robust overview generated by AI typically includes different types of legislation, such as:

- Horizontal EU frameworks that affect most data spaces (regulatory frameworks for personal and non-personal data, Data Act, cybersecurity, and competition). The European Commission explicitly frames common European data spaces as needing to respect EU rules / values including personal data protection and competition law.
- Datas pace-enabling EU legislation (e.g., Data Governance Act, Data Act) that underpins trustworthy data sharing and common data spaces.
- Sector regulations (e.g., health) that create specific data space rules and institutions. EHDS is presented as the first sector-specific common EU data space regulation with a dedicated framework and phased implementation.

- Primary source legal texts & amendments (EUR-Lex) and Commission policy pages for implementation updates. The DGA's official legal act and timeline are published via EUR-Lex and Commission policy pages.
- Implementation instruments (implementing acts, guidance, board outputs), because regulations often become operational through additional acts and specifications (explicitly noted for EHDS).

The outcome should be a structured "Regulatory Perimeter Framework" that categorises:

- Mandatory EU-wide obligations
- Member State–specific requirements
- Sector-specific obligations
- Optional or strategic compliance extensions

Such a framework should include decision trees and role-based compliance mapping to ensure usability and enforceability, building on the work done to develop a first prototype of the Legal Compass. Regulatory awareness must ultimately be embedded in enforceable internal policies, contractual obligations, audit mechanisms, and, where necessary, sanctioning procedures within the data space governance framework.

2.5.2 Contractual framework

Key question

The Contractual Framework building block describes the legally enforceable agreements underlying the operation of a data space, as entered into by different parties in a relationship with the data space. Agreements are classified into the following three categories, based on the nature of their subject matter:

- Institutional agreements
- Data-sharing agreements
- Services agreements

The legislation underlying these agreements is under development and requires updates of these agreements. That leads to the following question:

- *How to ensure up-to-date contractual agreements for global data sharing by data spaces based on updated legislation?*

Approach

AI can help to keep data space contractual agreements across institutional agreements, data sharing agreements, and service agreements continuously up to date under changing legislation by enabling a "monitor → interpret → update → deploy → evidence" loop.

In practice, the data space governance authority maintains a modular contract architecture where legal requirements are in updateable annexes, and AI supports:

1. Legislative horizon scanning and alerting,

2. Impact analysis that maps changes to the affected clause modules (e.g., EU SCC transfer clauses, UK IDTA/Addendum for UK transfers, or adequacy pathways such as the EU-US Data Privacy Framework),
3. Automated redlining and versioning of the rulebook and templates, and
4. Smart contract assembly that generates the correct contractual bundle per data exchange based on context (origin/destination, roles, data categories), while maintaining an auditable trail of why a given version applies.

This approach is particularly effective because widely used transfer tools and frameworks are explicitly versioned and updated over time (e.g., the European Commission's modernised SCCs, the UK's IDTA/Addendum framework, and the EU-US DPF adequacy decision), allowing AI workflows to select the right mechanism and trigger re-papering only where needed. AI should function as a support tool, assisting legal experts and the governance authority in identifying and updating affected clauses. Final contractual decisions, validations, and rule interpretations remain under the responsibility of the governance authority, ensuring legal enforceability.

3. Technical building blocks

3.1 General

In the past few years there has been a process of ongoing technological convergence. In DSSC Blueprint version 3.0 there is now a clear list of technical capabilities needed in building blocks, associated with a clear overview of recommended technical protocols. In addition, a categorisation of services was provided.

Ultimately this can lead to a situation whereby discussions can shift from technology to business and the decision on technical capabilities will be primarily a sourcing decision and no longer a technical decision. With a growing number of (Common European) data spaces adopting the specifications set in the blueprint, this provides an increasingly attractive platform for service providers to offer generic services for use by data space governance authorities and individual participants of data spaces. The DSSC has provided an initial categorisation of these services, dividing between participant agents (focusing on individual participants), federation or facilitating services (focusing on the ecosystem as a whole) and value creation services. Federation or facilitating services can be offered by data intermediaries and may be subject to the provisions in the Data Governance Act (see also the legal compliance building block).

Moving forward there are a number areas which can be identified for further development and research. We will focus on several areas: standardisation, the role of Article 33 Data Act, trust frameworks, machine interpretable rulebooks, the role of AI and the impact on generic (technical) services to support the deployment of data spaces.

We will conclude with an overview of the impact and outlook per pillar of technical building blocks.

3.2 Trends

3.2.1 Standardisation

The blueprint has identified a set of common technical protocols which can be adopted by all data spaces. These are built up as followed:

Foundational technical standards: these include primarily the standards developed by W3C, including DCAT (Digital Catalogues) for specifying metadata, ODRL (Open Digital Rights Language) for specifying permissions, obligations and prohibitions and Verifiable Credentials (VC) for expressing claims. Together, they provide a powerful set of technical standards which can be used in distributed digital systems, such as data spaces.

Protocols: to support the interaction between participant agents and facilitating services, protocols are needed.

> *Dataspace Protocol (DSP)*
> DSP enables the exchange of data product metadata and the negotiation of data sharing contracts. DSP serves this purpose by combining DCAT entries (metadata) and ODRL (licensing data). Through ODRL, a data provider can specify the required permissions, obligations and prohibitions. Within a data sharing contract, data providers and data users can agree to their specifics (as is the case for specifics regarding other metadata).

> *Decentralized Claims Protocol (DCP) and OpenID for Verifiable Credentials (OID4VC)*
> To prove that an obligation is met, parties can exchange a claim with each other. Here, further protocols are needed - building on Verifiable Credentials - for validating and verifying claims. Validating a claim implies checking whether the issuer of the claim is actually conformant to the stated policy. This can be done by providing evidence to a trust service. Evidence can be yet another claim, or any kind of information requiring automatic or manual validation. Claims can be shared between parties. The receiving party needs to be able to verify that a claim is indeed correct. This is again done by consulting a trust service in the ecosystem. Several protocols are available for this process of validating, sharing and verifying claims, most notable: the Decentralised Claims Protocol (DCP) and OpenID for Verifiable Credentials. The former is mostly used in machine-to-machine communication, whereas the OpenID for Verifiable Credentials standard is mostly used in situations with manual sharing of claim (e.g. through an app). Both standards can be used next to each other.

It is expected that the standardisation of these protocols will continue. DCP and DSP have been submitted by the Eclipse Dataspace Working Group to ISO to become a PAS (Publicly Available Specification). Several others initiatives are driving the further standardisation of OpenID for Verifiable Credentials. These include the developers of the EU Identity Wallet, which has adopted this standard for identity claims.

3.2.3 Data Act article 33

Article 33 of the EU Data Act provides the legal framework for data providers in Common European Data Spaces. Effectively this has implications for other roles as well. Through the Trusted Data Framework, standardisation is ongoing at CEN/CENELEC and ETSI to provide technical specifications and harmonised European standards. Harmonised standards can be used to assume compliance with the Data Act, whereas technical specifications provider further guidance.

Key developments expected in the course of 2026 are:

The release of the **Trusted Data Transaction** standards. These provide the interoperability requirements for implementing article 33. Aspects include the provisioning of metadata on the description of a data product, the provisioning of metadata on the semantics of the data contained in the data product (data models, taxonomies, code lists, etc.), the provisioning of metadata on the technical accessibility of the data (API endpoints, security mechanisms, etc.) and the way in which data providers and data users can (automatically) come to data sharing contract and enforce this during operation use. The standards have been developed using material from the Data Spaces Support Centre, but take into account wider feedback through standardisation bodies.

A **framework for describing data catalogues**: building on DCAT and the work of SEMIC on DCAT-AP a data catalogue framework for data spaces will be made available by ETSI. This framework allows data spaces to specify a more specific set of semantics used for their (domain specific) catalogue of data products.

A **framework for internal data governance**, which can be used as a quality metric and aspects in the catalogue metadata of a data product.

Together, the standards will provide a generic framework which data spaces and their participants need to use. DSSC2 will likely be tasked to provide data spaces with guidance on the usage of these standards.

It is likely that the aforementioned technical protocols can be used to implement the requirements coming from the harmonised European standards. Where needed, further alignment and convergence can be foreseen. Also, it is possible to add further specifications (e.g. for data marketplaces) or add legacy standards, if circumstances in a particular data space require this. For example: when the business model of a data space requires a marketplace or when existing domain-specific standards continue to play an important role (e.g. AS/4-eDelivery in e-invoicing and public procurement).

3.2.4 Trust frameworks

Initiatives such as Gaia-X and iSHARE have made the concept of a ‘trust framework’ commonplace in many data spaces. However, until now there was no clear definition of what a trust framework exactly is and how it should be implemented in a data space. Both initiatives have linked legal and contractual elements (e.g. membership requirements or contracts to be signed), business models (e.g. what someone needs to pay for using the trust framework) and technology with each other. Technology includes both technical specifications and software. As of today for example, the adoption of the Gaia-X Trust framework requires the usage of Gaia-X Digital Clearing House software.

Moving forward, it is expected that standardisation will provide more clarity on the scope of trust frameworks. The draft contents of the Trusted Data Transaction standard provides some guidance (strongly influenced by the work of the Data Spaces Support Centre) and work items are being prepared both at CEN/CENELEC and ISO to further the work on formal standards on this topic.

It is expected that future standardisation will make a distinction between four elements:

1. The **core concept of trust frameworks**: what makes a trust framework
2. **Standards and specifications** for implementing trust frameworks: protocols such as DCP, OID4VC, etc.
3. **Software** for implementing these standards and protocols.
4. Specific **policies and rules**, forming the domain specific content of the trust framework: the policies, types of claims and mechanisms to provide proof of compliance.

As indicated, in current trust frameworks these are all intertwined.

We expect that ongoing standardisation efforts within both ISO and CEN/CENELEC will clarify this and will provide further clarity on the distinction between the four elements mentioned above. In particular for bullet (1), the core concepts, it is important to have a clear list of elements contained there-in.

It is expected, in line with the DSSC blueprint version 3.0, that a trust framework will contain:

- An overview of the policy/policies the framework serves.
- The type of claims the framework serves.
- The trust anchors (organisational entities) which – by contract, law or standing – can be considered to be authoritative for validating a claim.
- The semantics of these claims, their payload.
- The mechanisms to verify the integrity of a claim (e.g. electronic signature or hash code).

The proof which needs to be provided for validating the claim. These can either be other claims or information for further manual or automatic analysis (e.g. auditor's report, signed paper contracts).

The trust services which can be used for both validating and verifying the claim on behalf of one or more trust anchors.

This implies that there is a clear link between policies, which can be part of a data space rulebook or data sharing contract, the claims used to express compliance with these policies and the trust framework for validating and verifying these claims. It is likely that trust frameworks set-up in this way, can be expressed in a machine interpretable way, allowing for compliance to be highly automated.

If this proves to be possible there are several consequences:

- Generic trust frameworks can be set-up across multiple Common European Data Spaces. For example for elements such as identity management, infrastructure sovereignty, data management, assurance of data quality, etc. They can be used by multiple data spaces in their rulebooks and – in this way – facilitate cross-data space collaboration.
- Individual data spaces need to set-up either their own trust framework (e.g. for data space participation claims) and/or re-use generic trust frameworks (e.g. for legal identities). Trust

frameworks need to be linked to policies described in the respective rulebook and linked to types of claims. Similarly, a link can be established with the policies of individual participants (as fixed in data sharing contracts between parties).

- It becomes possible to develop generic trust services, which can be configured according to any specified trust framework. The trust service simply executes the machine interpretable specification and uses common technical protocols for interacting with participant agents and other facilitating services.
- For existing trust frameworks this allows for a decoupling of software/protocols and the actual contents of the trust framework. The value of the trust framework will be determined by the value of the policies expressed by the trust framework. In the case of Gaia-X this might for instance relate to labeling-system it suggests for infrastructure sovereignty. eIDAS might be considered a trust framework for identity. And new trust frameworks might emerge as well, e.g. for validating claims on being EU Trusted Data Intermediaries or even Common European Data Spaces.

3.2.5 Machine interpretable rulebooks

Similar to trust frameworks, also rulebooks can become more machine-interpretable in the future. Present-day rulebooks are often documents, maintained in a wiki or git-based environment or published as PDF-documents.

There is no fixed structure for a rulebook. Several initiatives, such as 1001Lakes and SITRA, have developed guidelines for data space rulebooks, which have been incorporated in the DSSC Toolbox. However, there is no formal fixed structure of elements which should be contained in every rulebook.

The DSSC Blueprint does give an overview of required capabilities and design choices for each of the building blocks (both business & organisational and technical building blocks). Using the co-creation method these design choices can be fixed into agreements going into the data space rulebook. Under the definition of a data space, every participant adheres to those agreements. This in turn provides a platform to potentially lower the barrier for data sharing: by knowing another party adheres to an agreed set of rules, the number of rules to be set by individual parties can be limited. Through a trust framework the only thing to be verified is whether the other party is actually adhering to the rulebook. As an example: if I know that another person works for my company – and can prove this – I can more easily share and exchange data with that person. My company provides the necessary mechanisms (directories, badges, etc.) and underlying procedures (HR, hiring, department management) allowing me to verify this.

We expect rulebooks to increasingly adopt a standardised structure. This has the benefit of:

- Making rulebooks more comparable
- Improving interoperability (e.g. between rulebooks)

- Facilitating automation

Automation will be possible by expressing rulebooks in a machine readable format. Particularly for technical building blocks this is feasible, as many elements are already contained in a machine readable format, for example:

- Metadata on data products (Data, services & offerings descriptions)
- Semantic models (Data models)
- API-specifications (Data Exchange)
- Types of claims (linking to a trust framework, see above)

3.2.5 AI for data spaces

AI is increasingly an important factor for setting-up and using data spaces. For example to collect training data or by using a data space to share smart algorithms as data products in the ecosystem. Data spaces can be used as a means to manage policies for data and algorithms usage throughout the ecosystem and implement necessary requirements for provenance and observability.

In addition, AI can serve as a tool to optimize the functioning of the data space itself as well. Typical areas can include:

- Semantic annotation and reasoning on data, limiting the need for pre-defined semantic models and mapping by using AI-algorithms to discover patterns and do semantic reasoning.
- Defining and managing APIs and technical interfaces, where AI can be used to generate code and system integrations within a participant agent.
- Reasoning on claims and supporting proofs: where-as currently many organisations fully base their trust decision on a single data space membership claim, in the future AI algorithms might support reasoning on complex claims situations and policy evaluations for automated compliance.
- Automating the negotiation of data sharing contracts between AI-enabled participant agents

Overall, this can reduce the integration efforts and manage the complexity with a growing number of participants in a data space and an increased number of data products being shared (and viceversa: it can enable this growth).

3.2.5 Advancing the development of technical services

The DSSC has identified three main categories of services (1) participant agent services, (2) federation / facilitating services and (3) value creation services. It is likely that – given the availability of common standards – the first two categories can be highly standardised. The current DSSC Toolbox, together with SIMPL, already provides many available open source building block.

The challenge lies in turning this into a viable market offering with (sovereign) cloud service providers and managed service providers. Further fine-tuning of specifications might be necessary, but the key challenge lies in developing the market offering. There can be a market pull from Common European Data Spaces, but also a market push by vendors – which can offer these services either directly through the market or through domain-specific service providers (e.g. healthcare software in the health data space, operated by a generic participant agent).

3.3 Impact on Data Interoperability building blocks

3.3.1 Data Models: AI driven data annotation and structuring

The evolution of data modeling within Common European Data Spaces is progressing into a new phase, fueled by advancements in AI-driven data annotation and structuring. As AI systems increasingly interpret, categorize, and enrich datasets autonomously, reliance on rigid, predefined data models is diminishing. Rather than commencing with fixed schemas, data spaces are likely to transition toward adaptive, machine-supported semantic structures.

This shift indicates a movement from schema-first design to flexible, context-aware semantic layering, where AI continually contributes to metadata generation, ontology alignment, and cross-domain interpretation.

Future DSSC Blueprint iterations should update specifications to reflect collaborative human-AI modeling best practices, ensure traceability of AI-generated metadata, and define governance frameworks for evolving semantic structures. The blueprint must offer guidance on interoperability safeguards when adaptive semantics intersect with cross-organizational data sharing requirements.

3.3.2 Data Exchange: AI-Enabled Interoperability

Data exchange protocols have traditionally relied on predefined domain or application-specific conventions. However, the increasing maturity of AI systems capable of interpreting and harmonizing diverse technical interfaces presents a transformative opportunity. AI models can facilitate mediation between heterogeneous APIs, message formats, and communication protocols, enabling adaptable interoperability driven by contextual needs rather than solely rigid standards.

Such capabilities permit automatic translation layers that support participant interaction without requiring pre-alignment of all technical interfaces. Therefore data spaces can allow varied participants to connect with reduced integration effort and enhanced resilience to technological change.

For upcoming DSSC Blueprint releases, this necessitates reviewing existing interoperability design patterns. Recommendations should include architectural options for AI-assisted protocol negotiation, validation mechanisms to ensure accuracy of AI-generated translations, and fallback strategies for handling ambiguities in automated mediation. Furthermore, the blueprint should address new assurance approaches, verification pipelines, and compliance procedures for AI-enabled exchanges. Embracing these advances will allow data spaces to scale rapidly, integrate flexibly, and maintain robust interoperability amid evolving technologies.

3.3.3 Provenance, Traceability & Observability: End-to-End Lineage and Transparency

As data spaces grow across sectors and regions, the need for reliable, transparent data flows is paramount. Provenance, traceability, and observability have become essential prerequisites for auditability, accountability, and regulatory adherence. Frameworks such as PROV-O and PAV provide foundational elements for lineage representation, but achieving true interoperability demands standardization, infrastructure investment, and federated governance.

The emphasis on transparency addresses users' desire to understand data origins, transformations, and usage conditions – including tracking production, algorithmic processing, and decision-making logic in AI-driven workflows. Observability further contributes operational insight, enabling real-time monitoring of distributed components within data spaces.

Future DSSC Blueprint updates should specify conceptual standards and actionable implementation patterns for federated provenance systems, including guidance on distributed registries, tamper-evident evidence stores, secure cross-domain lineage queries, and integration with policy enforcement mechanisms. Enhancing this building block supports verifiable trust and facilitates compliance with stringent European data governance mandates.

3.4 Impact on Data Sovereignty & Trust building blocks

3.4.1 Identity & Attestation Management: Expanding Claim-Based Participation Models

Identity management within Data Spaces is advancing from simple authentication to multifaceted attestation. With the development of the European Digital Identity Wallet and Business Wallet (EUID + EUBW) and broader decentralized identity ecosystems, data spaces can leverage verifiable claims encompassing participation rights, certifications, policy compliance, and governance roles.

This progression enables automated trust negotiation, wherein participants present cryptographically verifiable credentials for dynamic authorization. As data spaces mature, identity serves as a mechanism for sovereignty: participants control which claims they disclose and under what circumstances, utilizing trusted issuers and robust verification protocols.

Future DSSC Blueprint versions should integrate comprehensive guidance on claim ontologies, wallet compatibility, issuer governance, assurance levels, and audit requirements. Additionally, recommended patterns must address incorporation of identity data into authorization flows, compliance checks, and cross-space interoperability. By adopting richer claim-based ecosystems, data spaces can enhance trust, reduce onboarding complexity, and foster scalable, decentralized governance.

3.4.2 Trust Framework: Machine-Readable Trust as a Foundation for Cross-Space Federation

Traditionally, trust frameworks provided policy definitions, certification schemes, and governance rules; their function is now expanding to include direct integration into data space rulebooks and support for multi-space interoperability. Within growing federations, trust frameworks are evolving toward machine-readable formats facilitating automated verification, decision-making, and compliance oversight.

A robust framework must detail not only policies but also evaluation mechanisms for trust across diverse domains, including shared semantics, automated conformance checks, standardized trust registries, and interoperable cryptographic attestation. Machine-readable rulebooks empower tools to automatically interpret obligations, rights, and constraints, ensuring consistent enforcement.

Future blueprint iterations should define data models, governance processes, and interoperability standards for trust frameworks. This includes specifying the publication, discovery, verification, and consumption of trust artifacts by participant agents and value-added services. These developments enable seamless federation, supporting a cohesive European data ecosystem.

3.4.3 Access & Usage Policies Enforcement: Automated Policy Enforcement Through Claims and Extended ODRL

Automating access and usage policy enforcement is essential for scalable data spaces while ensuring compliance with legal and contractual requirements. Integrating verifiable claims into enforcement logic allows participants to programmatically demonstrate eligibility or authorization. Automation reduces operational overhead and ensures uniform interpretation of rights and duties.

This trend imposes new requirements on policy languages, such as ODRL, which may need enhancements or tailored profiles to express Data Space-specific contexts and constraints. Automated verification systems can assess policy compliance, monitor permitted operations, and generate auditable records.

Future blueprints should outline standard profiles for policy expression, enforcement workflows, and interoperability interfaces for automated decision engines. Guidance should include mappings among identity claims, contractual terms, and machine-readable rules. By facilitating robust automation, Data Spaces achieve trustworthy, transparent, and scalable policy management.

3.5 Impact on Data Value Creation Enablers building blocks

3.5.1 Data, Services & Offerings Descriptions: Metadata for Algorithmic Assets and AI-Driven Services

With AI increasingly integral to data spaces, there is an imperative to describe not just datasets and services, but also the underlying AI algorithms. Metadata should represent algorithmic attributes such as purpose, functionality, model lineage, evaluation criteria, training data features, performance guarantees, and risk assessments.

This approach aligns with EU AI Act requirements emphasizing transparency, accountability, and lifecycle monitoring for AI systems. Accordingly, Data Spaces should implement comprehensive metadata frameworks to ensure algorithmic assets are trustworthy, discoverable, and governed effectively.

Subsequent blueprint revisions must incorporate AI-focused metadata schemas, validation procedures, and governance protocols. Standardized descriptors will promote cross-data-space interoperability and support responsible, compliant deployment of AI solutions across industries.

3.5.2 Publication & Discovery: Federated Catalogs for Scalable, Distributed Discovery

Publication and discovery solutions are diversifying to meet sectoral and cross-sectoral needs. Some adopt centralized catalogs, while others favor federated or decentralized designs to address sovereignty concerns, organizational autonomy, and regulatory compliance.

Federated discovery enables participants to retain control yet ensures discoverability of datasets, services, and policies throughout an extensive ecosystem. This requires new architectural considerations, including metadata synchronization, catalog interoperability, and cross-catalog search protocols.

The DSSC Blueprint should be updated to reflect these developments, offering specifications for federated indexing, catalog compatibility, service registration, and governance of distributed discovery. Such updates will allow Data Spaces to scale efficiently without compromising autonomy, performance, or interoperability.

3.5.3 Value Creation Services: Convergence Between Participant Services and Value-Added Capabilities

Initially, Data Spaces distinguished core services from value creation services. With ecosystem maturation, this separation is fading as value creation services increasingly mirror advanced participant-agent offerings that extend core capabilities—such as analytics, transformation, algorithm execution, and decision support.

This convergence democratizes service provision, allowing both central operators and individual participants to develop and supply sophisticated functionalities. Consequently, the blueprint should articulate models for integrating these services with governance, interoperability, trust, and compliance mechanisms.

Future updates must define modular capability structures, service certification standards, and integration pathways enabling participant agents to embed value-added features seamlessly. Recognizing evolving value creation services ensures a flexible, innovative, and competitive data space environment.

4. Concluding remark

The evolution of data spaces in Europe is entering a phase where coordinated innovation, scaled deployment, and cross sector alignment become essential. Building on the foundations laid by the Data Spaces Support Centre, this forward looking research agenda highlights the strategic developments required to ensure that data spaces mature into an interoperable, trustworthy, and economically sustainable European infrastructure. As standardisation progresses, Article 33 of the Data Act becomes operationalised, and trust frameworks and rulebooks move toward machine interpretability, DSSC2 will play an increasingly pivotal role in guiding data spaces toward harmonised architectures and reusable technical and governance patterns.

To succeed, the next generation of data spaces must move beyond experimentation toward operational excellence—supported by quantifiable business models, automated participation management, robust governance cooperation between DSGAs, and AI ready data space offerings that stimulate value creation. DSSC and DSSC2 together form the backbone of this transition. Through shared specifications, coordinated support, and a commitment to federated interoperability, they will enable data spaces to collectively scale, innovate responsibly, and contribute to a cohesive European data ecosystem.

This agenda therefore serves not as a final roadmap, but as a living framework—one that anticipates continuous technological, regulatory, and organisational change. By embracing collaboration across sectors and leveraging the foundations laid by DSSC and its successor, Europe can build data spaces capable of supporting economic growth, societal wellbeing, and sovereign digital transformation for years to come.