30 May 2025

Department of Finance
Australian Government

By email: DATActReview@finance.gov.au

Submission to Statutory Review of the *Data Availability and Transparency Act 2022* (Cth) (DAT Act) – Issues Paper

This submission is prepared by Lyria Bennett Moses, relevantly a Professor in the School of Law, Society and Criminology in the Faculty of Law and Justice at UNSW and a researcher with the UNSW-UTS Trustworthy Digital Society Hub and Nicholas Hodgkinson, relevantly a Research Assistant with the UNSW-UTS Trustworthy Digital Society Hub. The UNSW-UTS Trustworthy Digital Society Hub has funded a seed project, in collaboration with the Australian Research Data Commons (**ARDC**), exploring the feasibility and implications of Australian "dataspaces".[1] We believe that some of the preliminary findings of that project, as well as ongoing work within that project, will be of interest to this statutory review. Our submission should thus be read alongside that of the ARDC. It represents the opinion of its authors as researchers and is not an institutional position.

Our submission is organised with reference to the five questions posed in the Issues Paper, with an additional sixth question on what else we believe is required to build the necessary infrastructure for an effective Australian data sharing ecosystem.

In summary, it is our opinion that the DAT Act and DATA Scheme have failed to deliver any significant improvements in mobilising Australia's public sector data for societal benefit. The DAT Act does not warrant continuation in its current form. It should be repealed and replaced with framework legislation, accompanied by a package of aligned law reforms and a new strategy to promote appropriate and trustworthy data sharing mechanisms across the economy.

1. Has the operation of the DAT Act advanced its objects?

Plainly, no. The objects of the DAT Act, set out in section 3, include promoting better availability of public sector data and establishing institutional arrangements for sharing public sector data that increase the integrity, confidence, and safeguards around that sharing. The evidence to date suggests the DAT Act has not advanced these objects to any significant degree. The Issues Paper itself notes that, as of March 2025, there have been only eight data sharing agreements under the DATA Scheme, all related to a single program—the National Disability Data Asset.[2] This limited uptake stands in contrast to the over 11,000 data sharing agreements identified outside the DATA Scheme in a June 2024 survey of just 19 Commonwealth entities.

---

[1] Otherwise referred to as "dataspaces" or "data-spaces".

[2] We note, as the ARDC does in its submission, that no Australian university has to date been a party to data sharing agreements executed under the DATA Scheme (despite being the only non-government entities eligible to participate): Australian Research Data Commons, Submission to Department of Finance, *Statutory Review of the Data Availability and Transparency Act 2022 (Cth)* (30 May 2025); 'Data Sharing Agreement Register', *Office of the National Data Commissioner* <https://www.datacommissioner.gov.au/data-sharing-agreement-register>.

This would indicate that the DAT Act has not yet become the primary enabler for "promoting better availability of public sector data", nor has it established "institutional arrangements" that are widely adopted for sharing.

Several general themes may have contributed to the DATA Scheme's limited uptake and its difficulties in achieving widespread cross-organisational data sharing to date:[3]

- A lack of technical and semantic interoperability between entities participating in the DATA Scheme.
- Persistent cultural and social challenges surrounding data sharing practices.
- The inherent risks associated with data sharing and the resulting caution exercised by organisations.
- An inability to effectively coordinate data ecosystems.
- A failure to adequately define what constitutes "success" for the DATA Scheme, or to establish a common vision, mission, or values for entities participating in the Scheme, or for the Scheme itself.

The practical relevance of the general themes identified above is further underscored by the findings of a working group established by the Office of the National Data Commissioner in April 2024 'to identify the key issues that impede uptake of the DATA Scheme … and identify potential solutions'.[4] This group, which included representatives from Commonwealth and state government agencies, identified several specific challenges:

- The fundamental role and value proposition of the DATA Scheme are unclear to potential users.
- Restrictions on direct participation for certain entities limit the Scheme's reach.
- The value of accreditation is not consistently recognised by stakeholders.
- The accreditation process is perceived as requiring significant time and effort, with an unclear basis for assessment.
- States and Territories lack equivalence with their Commonwealth counterparts in Scheme projects, which impedes two-way data sharing and parity in joint initiatives.
- The defined boundaries for data sharing projects under the Scheme can be limiting.
- Data Sharing Agreements are often found to be long and complex.
- There is a lack of clarity on managing the exit of output from the Scheme.
- Uncertainty persists regarding how the DAT Act's override provisions interact with other secrecy provisions and privacy legislation.
- The existence of established systems and processes for data sharing requests outside the Scheme contributes to the underutilisation of Dataplace.
- DAT Act terms and definitions do not align well with current data sharing practices or their use in other legislation.

It would be prudent to seek feedback directly and proactively[5] not only from the few government entities who currently participate in the DATA Scheme, but also from those who might yet participate (government and non-government). Perhaps most importantly, insights should be gathered from those entities that are eligible to participate but actively choose not to do so. For example, one barrier to uptake is the fact that data that has been shared under the DATA Scheme cannot be accessed overseas, which may prevent its use in the context of

---

[3] See Olli Pitkänen, Marko Turpeinen & Viivi Lähteenoja (1001 Lakes Oy), Rulebook model for a fair data economy v 3.0 (6 February 2025).

[4] Office of the National Data Commissioner, 'DATA Scheme Working Group Findings and Actions' (November 2024) <https://www.datacommissioner.gov.au/sites/default/files/2024 11/DATA%20Scheme%20Working%20Group%20findings%20and%20actions.pdf>; see also Angeletta Leggio, Komathy Padmanabhan and Kristol Pyke, 'Decoding Research Data Governance at Monash University: The Journey of Operationalising the DATA Scheme' (eResearch Australasia, October 2024) <https://conference.eresearch.edu.au/wp-content/uploads/2024/11/Padmanabhan-Leggio-Pyke-Wednesday-1045-Angeletta-Leggio.pdf>.

[5] That is, actively, in addition to the formal written submissions received as part of this statutory review.

collaborative international research efforts (e.g., projects comparing health outcomes across different countries).[6]

Looking at the identified challenges holistically, there are two broader issues with the DATA Scheme:

- It assumes that legislation is sufficient and that the focus should be the sharing of Commonwealth public service data; there is no attempt to develop infrastructure to facilitate an ecosystem for data sharing.
- The legislation is itself complex, working on top of a complex legislative framework where rules for data are found not only in the DAT Act, but also in a wide variety of general laws (such as the Privacy Act) as well as diverse rules relating to different government functions such as customs, health, anti-money laundering, taxation, social security, etc (see, for example, the override provision in section 23).[7]

2. Does the DAT Act improve information flows between public sector bodies and accredited entities?

No. As alluded to above, the DAT Act in its current state has not demonstrably improved information flows between public sector bodies and accredited entities to the extent envisaged. The negligible number of data sharing agreements executed under the DATA Scheme indicate that the DAT Act is not yet the preferred mechanism facilitating such information flows.

In our opinion, the principal opportunity for the DAT Act to improve information flows, including nationwide public sector data sharing and the participation of States and Territories, lies in:

- Developing infrastructure to support a data sharing ecosystem, exploring possibilities along the lines of dataspaces in Europe;[8] and
- Replacing the DAT Act with framework legislation that simplifies the rules that apply to sharing Commonwealth data.

The Appendix to this submission provides a high-level background on dataspaces. We note the ARDC, the first Australian member of the International Data Spaces Association (**IDSA**), is actively exploring and contributing to the development of dataspace concepts for Australia.

3. How does the DAT Act add value in the wider data sharing context?

The DAT Act has delivered minimal (if any) discernible value to the wider data sharing context in Australia, largely because of its low adoption and perceived operational challenges.

The Issues Paper states that 34 entities are currently accredited, but the limited use of the DATA Scheme for data sharing, with sharing occurring through other mechanisms, demonstrates its ineffectiveness.

---

[6] We concur with the ARDC's concerns regarding the restrictive effect of the *Data Availability and Transparency (National Security Measures) Code 2022* (Cth) and s 16A(2) of the DAT Act on this point, see Australian Research Data Commons, Submission to Department of Finance, *Statutory Review of the Data Availability and Transparency Act 2022 (Cth)* (30 May 2025). As regards foreign researchers, see 'Foreign Individuals – DATA Scheme Requirements', *Office of the National Data Commissioner* <https://www.datacommissioner.gov.au/data-scheme-guidance/foreign-individuals-requirements>.

[7] Refer to the ARDC's comments on the operation of section 23, see Australian Research Data Commons, Submission to Department of Finance, *Statutory Review of the Data Availability and Transparency Act 2022 (Cth)* (30 May 2025). See also Pat Leslie and Keith Dowding, 'Rise of the Monster Acts: Growth in Legislative Complexity in Australia since the 1980s' (Australasian Study of Parliament Group (ACT Chapter), 13 March 2025) <https://www.aph.gov.au/About_Parliament/Parliamentary_departments/Parliamentary_Library/Research/Lectures?selectedVideo={61F487A1-73E9-4560-9693-CCE5E73F39D4}>.

[8] See, e.g., 'A European Strategy for Data | Shaping Europe's Digital Future', *European Commission* <https://digital-strategy.ec.europa.eu/en/policies/strategy-data>. Whether or not formally adopted by name, the underlying architecture of dataspaces provides a valuable benchmark for assessing any implemented data sharing strategy.

In our view, the DAT Act should be repealed and replaced with framework legislation that:

- Defines key terms (including "data", "data custodian" and "public sector data" or "government data");
- Establishes and clearly defines common attribute labels for data ("semantic labels"), with each label linked to distinct handling rules (e.g., personal data, sensitive data, Indigenous data, children's data, commercial data, data that has gone through a de-identification process, Protective Security Policy Framework-rated data, Consumer Data Right data), where multiple labels may apply to the same dataset.
- To further guide appropriate data handling, certain common attribute labels (as established above) could also be assigned quantitative risk levels.[9] For instance, data that has undergone a de-identification process may possess different quantifiable risk profiles concerning re-identification. The methodology for assessing and assigning these risk levels would be appropriately specified in regulations, rules, or standards, rather than within the principal framework legislation itself.
- Establishes the operational framework for data sharing, providing that differently labelled data are governed by distinct and proportionate rulesets for their access, use, and management.
- Establishes a register of entities with different kinds of accreditation relevant to accessing and handling differently labelled data (this could be designed to harmonise with or recognise accreditations from other relevant existing schemes (e.g., for Consumer Data Right (CDR) accredited data recipients) to streamline processes and avoid duplicative accreditation burdens);
- Provides a mechanism for the accreditation of dataspaces. Such accreditation could be granted subject to specific conditions or limitations (e.g., defining with whom data can be shared, or for what purpose(s) it may be used).
- Prescribes high-level rules applicable to all sharing of government data under the framework.

The high-level rules for government data sharing can either specify accreditation requirements or, ideally, can accredit entire dataspaces where the 'assurance layer' of those dataspaces (including the rulebook and standards) meets threshold requirements. This ecosystem-level accreditation, potentially complemented by a certification scheme for critical software components (e.g., connectors) and service providers operating within these spaces drawing inspiration from the IDSA Certification Scheme,[10] would provide a more holistic (and scalable) assurance to data custodians and participants. Assurance would stem from the certified design and ongoing oversight of the dataspace itself, rather than solely relying on individual entity accreditations for each interaction.

Other legislation, regulations and policy documentation that contain data-handling rules for different kinds of labelled data can then be amended to align with framework legislation. In some cases, as for PSPF-rated data and personal information, existing rules can be amended so that terminology and processes align. In others, new rules may be required. Either way, data would only be shared in accordance with all the relevant rules that apply to data with the relevant label(s). In some cases, there may be different rules for data discoverability (the circumstances in which an entity can be told that data exists at all) and data access (the circumstances in which an entity can get access to the data).[11]

This provides a much clearer system for government data custodians to determine what can and cannot be shared than the current system where different legislation (including the DAT Act) uses different terminology, concepts and processes. Current data discovery platforms can align with the rules for data discoverability of differently labelled datasets.

---

[9] See, e.g., 'Voluntary Data Classification Framework' <https://research.csiro.au/dataclassification/>.
[10] 'Certification', *International Data Spaces Association* <https://internationaldataspaces.org/offers/certification/>.
[11] Non-discoverable data is somewhat analogous to dark matter; its existence is understood (or can be inferred), yet it remains, by its very nature, "invisible". Conversely, data that is discoverable may still not be meaningfully accessible. For example, access might be restricted to metadata or summaries, rather than the underlying dataset.

The proposed framework legislation need not limit sharing to particular countries, sectors or contexts—that can occur within the specific rulesets that apply to differently labelled data where such restrictions are relevant. Thus, unlike the DAT Act, there is no need to *generally* exclude the private sector organisations or require data to remain in Australia. Instead, such restrictions may be placed on data with particular labels. Framework legislation might also provide governance mechanisms that would allow for private sector organisations to access more categories of data, for example, something analogous to a university ethics committee that would be funded by industry.

4. What changes could be made to the DAT Act or the DATA Scheme to make it more effective in facilitating access to, sharing and use of public sector data?

As previously outlined, our primary recommendation is the repeal of the DAT Act and its replacement with new framework legislation, accompanied by comprehensive data rule reforms. We highlight that, given the limited availability of useful operational evidence obtained since the DAT Act took effect—a consequence of its low utilisation to date—any comparative evaluations of the efficacy of prospective changes are necessarily speculative rather than empirical.

As a second-best alternative, dataspaces could also be facilitated through revising the DAT Act. We would require more time to perform a thorough review and itemise all necessary amendments, but such revisions would likely include the following:

Part 1.2, section 9—Definitions:

- Accredited Australian Dataspace could mean a dataspace operating under a Rulebook.
- Rulebook could mean the rules (e.g., governance, operational, technical, and ethical) specific to an Accredited Australian Dataspace, approved by the regulator (the National Data Commissioner).
- Participant could mean a member of an Accredited Australian Dataspace operating under its Rulebook.

Part 2.2, sections 13–13C—Authorisations:

- Data sharing and use within an Accredited Australian Dataspace by its Participants, in accordance with its approved Rulebook, would be deemed authorised under the DAT Act. (This would complement, rather than replace, the existing scheme of project-based authorisations.)

Part 2.3, sections 15, 16—Data sharing purposes and principles:

- Rulebooks must demonstrate how the relevant dataspace, its operations, and projects conducted within it will uphold these DAT Act purposes and principles. Delegated legislation created under the DAT Act might require Rulebooks to detail specific processes for assessing projects against these requirements.

Part 2.4, sections 16A–16F—Privacy protections:

- Rulebooks must mandate how consent, data minimisation, restrictions on biometric data, re-identification prohibitions, and limitations on overseas data storage are implemented and enforced within the dataspace, potentially through specified technical standards. Those standards would ideally be developed through established mechanisms for international cooperation (for example, the International Standards Organisation).

Section 42—Functions of Commissioner

The Commissioner's functions would need expanding to include:

- Developing criteria for, assessing, and accrediting dataspaces.
- Reviewing and approving Rulebooks as a condition of dataspace accreditation.
- Developing, endorsing, and potentially mandating technical and operational standards for Accredited Australian Dataspaces and their Participants (e.g., for APIs, data formats, security protocols, auditable logging).
- Establishing and overseeing any certification schemes for key technical components (e.g., "connectors") or specialised service providers operating within Accredited Australian Dataspaces.
- Authorising and overseeing pilot programs for new dataspaces.

Section 126 (Data codes) and 127 (Guidelines):

- Empower the Commissioner to use data codes and guidelines to elaborate on requirements for dataspaces and Rulebooks (including, for example, technical standards and certification processes).

Part 5.2, section 74 (Accreditation framework):

- The Commissioner may accredit a Rulebook (designating the relevant dataspace an "Accredited Australian Dataspace"). The sole purpose of such accreditation would be the ability for Commonwealth data to be shared within that dataspace. Dataspaces would not require accreditation to operate more broadly (for example, as mechanisms for sharing data held by universities and/or industry).

Section 77 (Criteria for accreditation):

- Establish new, specific criteria for accrediting a dataspace. (This accreditation of the dataspace itself, with its embedded rules and approved Rulebook, would ensure Participants operate within a compliant framework, potentially streamlining existing DAT Act accreditation requirements for users and ADSPs when acting as Participants within that accredited dataspace.)

Sections 77B, 78 (Conditions of accreditation):

- Conditions may be applied to the accreditation of a dataspace.

Sections 81-83 (Suspension and cancellation):

- Amend to apply to the accreditation of dataspaces.

Part 5.5 (Regulatory powers and enforcement):

- Amend these powers to apply to Accredited Australian Dataspaces and their Participants.

5. Should the DAT Act be allowed to sunset?

Yes. It is our primary recommendation that the DAT Act be repealed and replaced with framework legislation, accompanied by a package of aligned law reforms, as detailed previously in this submission. Should a full repeal and replacement not be feasible, we have, as an alternative, proposed specific amendments to the DAT Act. These amendments are designed to enhance its capacity to facilitate the Commonwealth government's effective participation in dataspaces. If this latter approach is pursued, an extension to the DAT Act's current sunset provision would be warranted to provide the necessary timeframe for the development, implementation, and evaluation of these reforms.

6. What other changes are necessary?

As we stated at the outset of this submission, the issue is not only one of legislation but rather of infrastructure. We recommend developing a strategy for an Australian data sharing ecosystem that includes but goes beyond the sharing of Commonwealth data. Such an ecosystem would operate across sectors and be anchored by industry. We believe that dataspaces can provide a platform for such an ecosystem. Through strategy, government can partner with other organisations, including Standards Australia, to develop the assurance layer for the ecosystem. This will include, at a high level and allowing for specific implementations for different dataspaces, technical and semantic interoperability protocols, standard contracts, technical standards, certifiers and identity providers, as well as evaluation and audit functions. Some of this already exists, while others will need to be developed with government support. Within the strategy would lie a project for related law reform: the proposed framework legislation described above, related law reform aligning the rules that apply to processing differently labelled data with that framework legislation, and additional law reform projects as required.

As such, we envision that, the responsibility for developing detailed, operational standards for specific dataspaces would rest with industry itself. There would not be direct regulation of the internal standards of every individual dataspace by a regulator. Some dataspaces, particularly those not interacting with Commonwealth data under the proposed framework legislation, might operate outside the ambit of any accreditation requirements or the rules associated with sharing Commonwealth data.

To ensure a basic level of interoperability across the broader ecosystem, a new or existing regulator could be empowered to prescribe a set of high-level, general rules or standards.[12] This "general part" might include common data format standards; common language standards (i.e., semantic interoperability, using vocabularies or ontologies to ensure data is consistently understood across different systems or dataspaces); and overarching principles or protocols for data exchange. Industry, specific sectors, or individual dataspaces would then be free to develop more detailed, domain-specific standards tailored to their particular needs and use cases, building upon these general rules where applicable.

For dataspaces that are intended to be governed by or interact with the new "framework legislation" (especially those involving government data or seeking accreditation under it), a key mechanism would be the use of "semantic labels" attached to data. These labels would trigger the application of specific rulesets or direct the data and related activities to the relevant legislative pathway. This is fundamentally a “sorting exercise” where the data's label determines which rules or parts of the framework (or other relevant Acts) apply, allowing for differentiated handling based on data sensitivity, type, or context.

Note that the interaction between the strategy and the proposed framework legislation is limited to the use of Commonwealth data. There is no reason why the more onerous restrictions imposed on some Commonwealth data sharing including under the DAT Act should, by default, apply to all categories of Commonwealth data, let alone to other entities sharing other types of data. The data sharing rules binding differently labelled Commonwealth data would limit the dataspaces within which such data was shared and the circumstances within which it was shared within a dataspace. But it is also possible for dataspaces to support a wide variety of use cases, including sharing among private sector organisations.

---

[12] Under the proposed framework legislation, the primary responsibility of the central data sharing regulator would be to ensure compliance with general, high-level rules. Enforcement related to specific sectoral Acts or other existing laws—identified and made applicable through the data labelling process previously described—would remain the purview of the regulatory body already holding jurisdiction under those respective Acts. For dataspaces operating outside the framework, disputes would be resolved directly between the involved parties (e.g., for breach of contract).

Ongoing work

Our collaboration with the ARDC is still in its early stages and we will continue to develop our thoughts on dataspaces and how they could be used in Australia to promote responsible and efficient data sharing. We would be very interested in further conversations and collaborations to explore further the ideas in this submission.

Yours sincerely,

Lyria Bennett Moses
Professor and Head of the School of Law, Society and Criminology
[redacted]

Nicholas Hodgkinson
Research Assistant
[redacted]

Appendix: What are dataspaces?

Introduction

No single formal or legal definition for a "dataspace" exists; its meaning varies with context. The Data Spaces Support Centre (**DSSC**) defines a dataspace[13] as "an infrastructure that enables data transactions between different data ecosystem parties based on the governance framework of that data space," and as being "generic enough to support the implementation of multiple use cases".[14] Dataspaces are also understood as providing "a decentralised, neutral framework of protocols and frameworks that empowers participants to engage in trusted data sharing",[15] using common principles and standards.

Dataspaces differ from the predominantly bilateral arrangements contemplated by the DAT Act. The DATA Scheme authorises sharing on a project-by-project basis via specific data sharing agreements between a Commonwealth data custodian and an accredited user (or ADSP). While the DATA Scheme provides for accreditation and National Data Commissioner oversight, its core mechanism facilitates discrete, authorised exchanges for defined purposes. This is not conducive to a persistent, multi-directional data ecosystem under unified governance.

Dataspaces, conversely, are federated data ecosystems with common governance or a federation of such ecosystems (that is, a 'network of networks'). They support ongoing, many-to-many data transactions within a trusted environment, defined by a common rulebook and shared standards or infrastructure.[16] Such a dataspace framework typically includes:

- Governance elements, such as legal agreements and common standards for managing security, privacy, and assurance; and
- Soft technical infrastructure, for example, common data standards and standardised Application Programming Interfaces (**APIs**).

Dataspaces comprise "participants" (or data sources) and the defined relationships between them. This ecosystem can encompass data sources within or across organisations—irrespective of their format, location, or underlying data model—representing a unified interface for data querying and integration.

While most dataspace models are European and thus align with EU policies and instruments,[17] they provide valuable conceptual foundations for how the Australian government might think more holistically about creating the infrastructure to support a thriving ecosystem for data sharing that builds in governance and assurance. To this end, a key aspect of my project with the ARDC is to explore how dataspaces can be adapted for Australia. This requires a broader strategy in addition to law reform.

Dataspaces in the context of European legal frameworks

In the European Union (EU), the Data Governance Act (DGA) and the Data Act (DA) provide foundational legislation for public sector data use and the operation of dataspaces. Other relevant EU instruments include:

---

[13] We use the single word formulation here, but it varies.

[14] A use case is a specific scenario describing how data sharing achieves a particular goal. 'Starter Kit for Data Space Designers | Version 1.0 | March 2023', *Data Spaces Support Centre* (31 July 2023) <https://dssc.eu/space/SK/29523973/Starter+Kit+for+Data+Space+Designers+|+Version+1.0+|+March+2023>.

[15] International Data Spaces Association, *The Data Space Manifesto v 1.0* (April 2025) <https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/The-Data-Space-Manifesto-Version-1.0-April-2025.pdf>.

[16] See Olli Pitkänen, Marko Turpeinen & Viivi Lähteenoja (1001 Lakes Oy), *Rulebook model for a fair data economy v 3.0* (6 February 2025).

[17] For example, European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions* (February 2020) <https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf>. See also: Lars Nagel and Douwe Lycklama, *Design Principles for Data Spaces v 1.0* (Position Paper, 2021) 34 <http://doi.org/10.5281/zenodo.5105744>.

- The General Data Protection Regulation (GDPR);
- The EU's overarching Data Strategy;
- The Free Flow of Non-Personal Data Regulation;
- The Open Data Directive;
- The Database Directive; and
- The Platform to Business Regulation.

National laws of EU member states will also be relevant where those states are participants in dataspaces.

As the DSSC states, the relationship between legal-regulatory compliance and dataspaces is twofold: first, data, privacy, and other legislation create the legal-regulatory framework within which dataspaces exist; and second, dataspaces act as a tool for legal-regulatory compliance by contributing to the development of products and services through the provision of policies, tools, and resources.

Our project is to develop a legal framework that would support Australia's participation in dataspaces. This ideally includes framework legislation that supports the simplification of rules for sharing Commonwealth government data. Alternatively, it will consider changes that might be made to the DAT Act. But it will also consider strategies and additional legal mechanisms to ignite and support a well-governed data sharing ecosystem for Australia.

Rulebooks
Dataspaces operate under "rulebooks" or governance frameworks. These rules can be tailored for specific sectors, or use-case categories. They would establish common operational, technical, and legal rules of engagement—thereby reducing ambiguity and the need for bespoke negotiations before each instance of data sharing, thus accelerating information flows.

Standards
Dataspaces operate within technical and semantic standards. These can be different for different dataspaces or they can align. What they facilitate is the "technical and semantic interoperability" that the DATA scheme currently lacks, enabling smoother and more reliable data exchange between participating parties. These standards should align with the legal and governance infrastructure (relevant legal requirements, contracts, data governance policies) so that compliance is "by design". They should also incorporate security, including through the use of privacy-enhancing technologies (**PETs**) and robust consent management mechanisms.

Data transactions within dataspaces should be automatically logged with cryptographical security. This provides a verifiable and tamper-evident audit trail essential for accountability, dispute resolution, and ensuring the overall integrity of the data sharing scheme (like, for example, the concepts of "Clearing House" or "Data Exchange Logging Service" functionalities described in the dataspace literature).