Submission: Statutory Review of the DAT Act - Issues Paper

Rosie Hicks, CEO ARDC

30/05/2025

The Australian Research Data Commons (ARDC) welcomes the opportunity to comment on the *Statutory Review of the Data Availability and Transparency (DAT) Act 2022 - Issues Paper*.[1]

The ARDC has been engaged with the processes surrounding the DAT Act since early 2016 which marks the beginning of the Productivity Commission's *Inquiry into Data Availability and Use* (PC Inquiry).[2] Since then, we have made eleven submissions to various bodies, had a Memorandum of Understanding with the Office of the National Data Commissioner (ONDC) that included seconding staff, and worked closely with both the ONDC and universities to progress implementation of the DATA Scheme.[3]

This level of effort reflects the importance Australia's researchers put on public sector data and its value to them. Any gains in improving its use directly affects the cost, quality, relevance and timeliness of outputs which in turn affects the impact the research can have nationally and globally.

As highlighted by the Issues Paper and from our many conversations with stakeholders, after nearly a decade of working towards the promises of the PC Inquiry, the DAT Act has not delivered meaningful improvements for researchers.

The policy has not lived up to its original promise primarily because the Act was constrained by a single, relatively rare edge case - the need to override legislation. Due to the perceived risks of that approach, the Act was made excessively prescriptive with the burden remaining on users.

Even if the Act were to address that rare edge case, it would not significantly increase the flow of data within the public sector or to the research and private sectors, which was a key intention of the reform. The DAT Act has not moved the dial on mobilising Commonwealth public sector data for societal good.

> *The need for an Act remains, but it must be substantively different from the current one.*

The recommended changes and the justifications for them are outlined below.

We would be happy to discuss these matters with you.

[1] Statutory Review of the Data Availability and Transparency Act 2022 | Department of Finance
[2] Data Availability and Use - Public inquiry - Productivity Commission
[3] Introducing the DATA Scheme

ARDC response to questions in the issue paper

Has the operation of the DAT Act advanced its objects?

No. The objects of the DAT Act have not been advanced because sharing under the DATA Scheme was limited; existing agreements would likely have occurred regardless. Notably, no Australian university was involved in the agreements made despite them being the only entities outside of government eligible to participate.[4] Of course, the long lead time to establish the Scheme account in some respect for the low numbers. Nevertheless the design of the Act, as discussed below, means that even with time it could not be successful in mobilising the large middle ground of public sector data.

In terms of providing answers specific to each object of the Act:

(a) serve the public interest by promoting better availability of public sector data

Australia is a wealthy country. Many Australians readily adopt digital technologies and there are very good levels of digitised government services. Collectively, Australia produces a lot of public sector data. It exists and therefore is, in theory, available.

Discoverability of data is essential before you can access data that is available - 'You can't use data if you don't know it exists'.[5] Unfortunately, in the course of establishing the Scheme, the Data Commissioner has had to repeat efforts trying to get agencies to make data discoverable. This should already be standard practice given data.gov.au has been in place for some 20 years.[6] [7]

Implementing the Australian Government Data Catalogue[8] has drawn too much effort away from the purpose of the initiative ('use') and undermined data.gov.au as the globally discoverable one-stop shop for all (meta)data federated from other domain catalogues across Australian government(s). It is not clear (or it exaggerates significantly) the data available only as a result of the provisions of the Act.

This object of the Act was not achieved because data custodians were neither legally required to make data discoverable nor properly resourced or incentivised to get data into the hands of policy analysts, researchers, and innovators.

(b) enable the sharing of public sector data consistently with the Privacy Act 1988 and appropriate security safeguards

The ARDC has made recommendations to various privacy reviews and so will not repeat those here.

[4] Data Sharing Agreement Register
[5] PC Inquiry, p.159.
[6] Australian Government Data
[7] The Global Data Barometer 2nd edition: A Shared Compass for Navigating the Data Landscape
[8] Australian Government Data Catalogue

The matter of 'appropriate security (and) safeguards' are addressed further below. We highlight the negative effect current approaches have on the conduct of research and on research collaborations.

(c) enhance integrity and transparency in sharing public sector data

The ARDC supports the work done by the ONDC to establish registers in accordance with the DAT Act. These are essential for exposing various activities indicating the health of the data sharing system.

Given the value they provide, their use should be extended to capture more formally the other (over 11,000) data sharing agreements, requests for access that are denied, and satisfaction levels with the government's data request and provisioning services.[9]

The ARDC has also stated previously the Act should mandate use of 'federated trust services'. These are necessary to replace many of the prescriptive requirements of the Act. They are fundamental data infrastructure services for enabling trusted cross-organisational sharing at speed and at scale. An example of this is federating identity and authentication services across agencies and sectors. Another might be ensuring federated policy based access control services. A third would be a federated system of automated, immutable logging that captures conformance with the rules of sharing that were agreed.

(d) build confidence in the use of public sector data

Building confidence in the use of public sector data requires demonstrated successful outcomes. The absence of sharing with universities under the Scheme has not provided the case studies needed to build trust among data custodians, researchers, or the public. This represents a significant missed opportunity.

Given this situation, three issues are now active:

1. **Implementation Credibility.** Universities that invested in preparation for the Scheme have experienced justifiable frustration at the costs incurred for no outcomes. Researchers have had to continue developing workarounds and alternative channels. For both, the experience continues to undermine expectations they will ever use public sector data via DAT Act mechanisms.
2. **Regulatory Framework Perception.** The failure of the Scheme to facilitate any university sharing during its initial implementation period suggests deeper design or operational flaws. It raises questions about whether the custodian opt-in system and the permission-based framework is viable in practice. It creates a justifiable perception the legislative framework allowed continued underinvestment in provisioning data externally and prioritising control over enablement.
3. **Statutory Review Implications.** There are implications for this review and the interpretation of its findings and recommendations. Given the limited evidence base, evaluating the framework will

[9] Baseline Researcher Access to Public Sector Data | ARDC

now be over reliant on theoretical rather than empirical analysis. As the current approach did not work, anything short of a major redesign is likely to be viewed with scepticism.

(e) establish institutional arrangements for sharing public sector data

While the Act has established some institutional arrangements for public sector data sharing—including the Commissioner's role, accreditation frameworks and agreements processes—these have not translated into practical outcomes for the research community. There may have been some progress, but without corresponding data flows, these arrangements remain largely theoretical.

It is difficult to assess if the arrangements that have been implemented are fit for purpose. A key concern is that the PC Inquiry argued for developing 'trusted users' whose status persisted (as a 'program'). This was to avoid having bespoke requirements of trustworthiness for each data sharing 'project'.

Having been shaped by the Act and especially the inclusion of the Five Safes Framework, key institutional arrangements reflect a project rather than the suggested program approach. Additionally, accreditation criteria were not published publicly as rules, which is necessary to build trust in the credential, and the provisions in the Act relating to data sharing agreements were made overly-prescriptive.

The result is that each data user must re-prosecute all elements for every project, including on matters already covered by accreditation or else existing mechanisms for research (e.g., TEQSA requirements for universities, the public interest test for research grants or human research ethics approvals).

The approach taken under the DAT Act and embedded in institutional arrangements have replicated rather than reformed practices that are known to impede data sharing.

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

The role and performance of the DAT Act in enabling nationwide public sector data sharing and enabling better data flows.

The DAT Act has not enabled better flows of public sector data nationally. This matters to researchers because it defines whether they have to go to all governments or just one standardised scheme to get national data. If governments nationally could improve data flows between them, then researchers (and many others) would presumably also achieve much better access, use and impact.

In July 2021, Australian governments signed the *Intergovernmental Agreement on data sharing between Commonwealth and State and Territory governments* (IGA).[10] This is an excellent document. The ARDC would obviously like to see support of publicly funded research explicitly included in the objectives, but regardless, the Guiding Principles for the Agreement (Para.3) are valuable (rather than those in Schedule

[10] Intergovernmental Agreement on data sharing between Commonwealth and State and Territory governments

D). They are of the type that should have been included in the DAT Act for Commonwealth agencies. That is, they are high level commitments to behave in certain ways that, if followed sufficiently, would progress development of the sharing scheme as a national capability.

What may have come next is that each jurisdiction committed to establishing an equivalent to the DAT Act with some form of council of commissioners coordinating implementation and reporting progress to the Digital Ministers' Meeting. This would ideally be supported by a shared national strategy or else aligned jurisdictional strategies against which the signatories committed effort and funding.[11]

This seems not to have happened. There is little evidence the IGA has facilitated, in any substantive way, broad intergovernmental sharing and alignment of systems and processes as agreed. There is evidence that newer initiatives have ignored, not been aware of, or been unable to use the DAT Act for sharing.[12]

Opportunities to further facilitate State and Territory participation in the DATA Scheme, including embedding greater efficiency in the development of two-way data sharing arrangements.

We believe the more detailed and specialist work now required would benefit from adopting the concept of 'dataspaces' as the implementation approach.[13] Even if not adopted explicitly, dataspaces provide a valuable blueprint as well as open source assets against which a proposed approach could be evaluated.

The current form of dataspaces was developed from research originally sponsored by the German government. It was co-developed with industry as members of the not-for-profit *International Data Spaces Association* (IDSA).[14] The Europeans have since spent significant funds on further developing and implementing dataspaces, an investment Australia is well placed to leverage. [15] [16] Dataspaces are:

> A distributed system defined by a governance framework that enables secure and trustworthy data transactions between participants while supporting trust and data sovereignty. A dataspace is implemented by one or more infrastructures and enables one or more use cases.[17]

Dataspaces are the central approach for implementing the 2020 EU *Data Strategy*.[18] Their use underpins the *Data Governance Act 2022* that includes the objective of improved sharing of public sector data.[19]

---

[11] Making the most of the AI opportunity: productivity, regulation and data access - Commission Research Paper, p.16
[12] Nature Positive (Environment Information Australia) Bill 2024
[13] Manifesto of International Dataspaces
[14] International Data Spaces
[15] As of March 2025, the EU is reported to have provided €3,838 M of public funding for dataspaces.
[16] Agreement between the Government of Australia and the Government of the Federal Republic of Germany on Scientific and Technological Cooperation [1976] ATS 28. See also Australia and Germany strengthen ties on science and research.
[17] Core Concepts - Glossary - Data Spaces Support Centre
[18] A European strategy for data | Shaping Europe's digital future A new strategy is planned for release in Q3, 2025.
[19] Data Governance Act explained | Shaping Europe's digital future. It is of note this Act came into force the same year as the DAT Act. It may be instructive to compare approaches and outcomes to date.

Responsibility for coordinating the implementation of dataspaces sits with the EU's Data Spaces Support Centre (DSSC), a collaboration that includes the IDSA.[20] The DSSC works with EU members to implement dataspaces in the domains prioritised in their Data Strategy such as for Agriculture, Energy, Health, Manufacturing, Mobility, Public Administration, Research and Innovation, Skills and Tourism.[21]

Critically, these domain dataspaces are intended to be developed in such a way as to enable cross-dataspace interoperability, effectively forming a single European dataspace.

The ARDC was the first Australian member of the IDSA and we are trialling dataspaces here, including with industry.[22] We are contributing back, such as by helping in the development of international dataspace standards.[23] [24] As a member of the IDSA, we have the option of initiating a national hub to aid in coordinating knowledge sharing and adoption.[25] A national hub would obviously benefit from involvement by other sectors, such as the government and those under Australia's *Digital Economy Strategy*, thereby extending the utility of dataspaces beyond just public sector data.[26]

Dataspaces could support both the IGA on data sharing and the DAT Act for Commonwealth entities while simultaneously delivering international interoperability with a growing number of countries.

Of note, the Queensland Government has also stated recently that it is:

> …currently implementing a dataspace model, with the aim of overcoming barriers to cross-agency collaboration and data sharing whilst maintaining trust and control. This approach is more than a technological shift; it strategically enhances data reuse, maximises existing investments, and creates new value for the public. If implemented successfully, it could set a national example for trusted data sharing, not just across the public sector, but also external to the government.

Regardless of whether the Australian Government adopts dataspaces formally, the ARDC will pursue this approach to ensure Australian researchers can continue to work closely with researchers in other countries who are increasingly using research and development dataspaces.[27] [28] [29]

[20] Data Spaces Support Centre
[21] Common European Data Spaces | Shaping Europe's digital future
[22] Australian Dataspaces Program | ARDC
[23] ISO/IEC CD 20151 - Information technology — Cloud computing and distributed platforms — Dataspace concepts and characteristics
[24] International standards
[25] Hubs & competence centers - International Data Spaces
[26] Digital Economy Strategy 2022 Update Released | PM&C
[27] European Open Science Cloud (EOSC)
[28] China aims for more than 100 'trusted data spaces' by 2028 under national action plan
[29] Promotion of Data Spaces | Enabling digital transformations in industries and a society | IPA, Japan

As part of the ARDC's *Australian Dataspaces Program* we are also collaborating with the UNSW-UTS *Trustworthy Digital Society Hub*.[30] [31] This includes a project exploring legal requirements for dataspaces in Australia. We would be happy to discuss this work.

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

The impact of excluding private and non-government sector entities on the value proposition of the DAT Act and DATA Scheme.

The ARDC and other stakeholders have previously noted the difficulties created by the DAT Act excluding private and non-government sector entities from using data shared via the DATA Scheme.

In addition to these limitations:

- Section 16A(2) of the Act requires that, 'If data that includes personal information is shared, the data sharing agreement that covers the sharing must prohibit any accredited entity…from… accessing, or providing access…outside Australia.' This presumably includes Australian researchers living or travelling overseas. These provisions apply when the data is obtained via the DATA Scheme, but the same or similar may not apply if the data is obtained via other channels.
- The *Data Availability and Transparency (National Security Measures) Code 2022* is an inappropriate approach to data security. It unnecessarily discourages or prevents all engagement with foreign researchers[32] and invites reciprocal measures by other countries when, in the vast majority of cases, there is no risk to security.

Various financial, policy, research and practical incentives mean it is essential for researchers to collaborate across sectors and internationally. Australia globally outperforms in research, not least because we collaborate so well internationally. It is not obvious how the current approach enables this while protecting data in a cost-effective, meaningful or productive way.

The immediate impact is that researchers avoid, and are advised not to use, the DATA Scheme. The wider impact of implementing these exclusions early on is it will now be very difficult to generalise the Act for a broader set of participants and use cases without substantive changes.

[30] Australian Dataspaces Program | ARDC
[31] Trustworthy Digital Society
[32] Foreign individuals – DATA Scheme requirements

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?

The ARDC suggests the following ten changes are required:

1. ***Remove the 'Authorisation to Override Other Laws'***

Inclusion of the override provision (s23) is regrettable. It had the opposite effect to the one intended, causing the Act as a whole to be made overly complex;[33] it simultaneously failed to bring 'clarity on how the DAT Act override interacts with other secrecy provisions and privacy legislation'.[34]

The provision should be removed. This will be the first and most important step in refocusing the Act on the access and use of Commonwealth public sector data. Rather than having an override provision, the government should intensify further its efforts to modernise legislation and address other factors.[35]

The focus should be on developing a coherent universal scheme to be used whenever sharing Commonwealth public sector data.

2. ***Mandate Public Sector Data Custodian Participation***

Currently, government organisations can choose whether to participate in the Scheme (opt-in) rather than being automatically included. This increases the number of steps and decisions before any sharing can occur. It does not reflect mandatory approaches (and the logic underpinning them) of other similarly important areas of government such as health and safety, protective security and financial accounting.

To achieve the intent of the Act, all custodians of Commonwealth public sector data, including commercial and other entities operating on behalf of the Commonwealth (e.g. service providers),[36] should be subject to its provisions. This includes participation in the DATA Scheme, its codes and rules. This would apply for any matters affecting the access and use of data external to the entity; matters relating only to the governance, management and use of data internally would remain unaffected.

3. ***Require Data Discovery***

On the OECD's 2023 *OURdata Index*, which combines measures of data availability, accessibility and commitment to open data by governments, Australia ranks 28th down from 4th in 2014.[37] [38]

[33] Leslie, P., & Dowding, K. (2025). *Rise of the monster acts: Growth in legislative complexity in Australia since the 1980s* (SSRN Scholarly Paper No. 4970966). Social Science Research Network. https://doi.org/10.2139/ssrn.4970966
[34] ONDC. (2024, November). *DATA Scheme Working Group findings and actions*. DAT Act Discussion ONDC Working Group
[35] Trusted and secure | Data and Digital.
[36] Making the most of the AI opportunity: productivity, regulation and data access - Commission Research Paper, p.15.
[37] 2023 OECD Open, Useful and Re-usable data (OURdata) Index, Figure 1, p.12.
[38] Government at a Glance 2015 | OECD, Figure 1.7, p.33.

It is clear that decades of policy 'encouragement' alone has failed to achieve the intended outcomes.[39] Significant resources and other approaches are needed to arrest this slide.

The OECD's *2023 Digital Government Index* noted the top ten performing countries 'all enacted legislation mandating public sector institutions to make data available'. Australia has not yet properly legislated or resourced availability; it is ranked 21st on that index.[40]

To activate data supply, the Act must first require public sector data custodians to make discoverable publicly the metadata of data they control[41] as well as (if the data is not Open) the policies under which sharing would be considered ('offer'). This does not mean they have to share the content.

Custodians may seek a partial or full exemption (as per rules) from exposing metadata publicly or even beyond select agencies or systems. That is, they enable graduated access for discoverability. A decision to exempt entities from publishing metadata publicly should be registered and available for review.

4. ***Ensure Presumptive Sharing***

When comparing countries that excel in balancing privacy, public sector data sharing and research outcomes, presumptive access is critical. Top performing countries have a 'presumption of sharing'.[42]

As an example of presumptive sharing, a custodian makes (meta)data discoverable and (if the data is not Open), publishes an 'offer' that describes the conditions under which sharing can occur.[43] Any entity that agrees to the policies of the offer could enter into negotiations with the custodian that may result in a data usage contract (or agreement) between the parties. Entities know immediately if they do not meet usage conditions and either do not seek access or else take actions to uplift their ability to meet them.

Changes to the DAT Act should support this shift from permission to presumption. The Act should contain provisions that establish a rebuttable presumption that public sector data should be discoverable and usable unless specific exceptions apply.

[39] Data and Digital Government Strategy v1.0.pdf, p.16.
[40] 2023 OECD Digital Government Index, Refer Dimension 4, pp.19-20. This Index is often quoted to demonstrate how well Australia is doing regarding digital services - and it is doing well - but the data dimension indicates a long running issue. The divergence between dimensions may represent a 'natural experiment', perhaps revealing some insight useful for its remedy.
[41] Current definitions of 'public sector data' are problematic. They make sense in terms of archives or accountability regarding 'who knew what, when', but they also make the Commonwealth acquisitive of all data 'in its possession', broadly defined. It can make the Commonwealth ill-suited to brokering or facilitating sharing nationally as they can 'own' all data that is shared.
[42] For example, refer to the Nordic countries, Estonia, the UK and NZ for comparison.
[43] There should be nothing preventing custodians from publishing different metadata or offers for the same data. One offer might support sharing with other government agencies as allowed by legislation, another offer may support use for research.

5. ***Allow Currently Excluded Entities***

Exclusion of various entities is a significant barrier to improving the access and use of public sector data. There should, in effect, be no excluded entities if custodians remain as 'opinionated' providers with whom the decision to share, based on legal and other considerations, ultimately resides.[44]

Amendments to the DAT Act should allow participation by any entity that meets accreditation and is willing to enter into the necessary agreements. Then, if an offer can be met, sharing may occur.

The approach of negotiating in relation to offers does not conflict with the advice regarding 'trusted users' and 'programs not projects', because the bulk of attributes of users, the assurance measures of the scheme, and the conditions to be met for each dataset, persist across entities and proposals.

Where there are precluded purposes, such as for law enforcement, defence or national security, these only relate to functions[45] or activities (e.g., investigations versus advice) relevant to the data rather than applying to entire entities. This enables a hybrid approach - with custodians responsible for using any combination of legislation, function, activity and risk to determine each publish and offer decision.

This approach future proofs the Act, making it more flexible and targeted. It makes non-precluded data of currently excluded entities available; it protects precluded data of entities currently permitted.

Meanwhile, decisions not to share must remain transparent and contestable with appropriately qualified bodies available to review them, in camera if required.

6. ***Remove the Five Safes Framework***

The DAT Act includes the Five Safes Framework as guiding principles, which would theoretically support a principles-based approach. However, the disconnect is how these are operationalised.

The Five Safes principles establish a restrictive framework for evaluation, the practical implementation requires specific authorisations against all five safes for every agreement rather than operating under broad authorisations with exceptions.

The principles, and its associated provisions such as those having to be included in data sharing agreements, should be removed from the Act. They may be used in subordinate instruments.

If it is necessary to have principles in the Act, those currently in the body of the IGA on data sharing would be most appropriate, particularly if framed as to be adopted by custodians.[46]

7. ***Adopt a Hybrid Outcomes-Principles Framework***

The DATA Scheme aspires to be principles-based but has been made to be permissions-based. It requires multiple explicit decisions and agreements, places the burden of justification on those seeking access,

[44] The scheme must support both contractual and technical controls over allowed re-use or on-sharing of data.
[45] Australian Governments' Interactive Functions Thesaurus (AGIFT) | naa.gov.au
[46] Intergovernmental Agreement on data sharing between Commonwealth and State and Territory governments, Para.3.

creates administrative processes that can delay or prevent sharing, and establishes a default position of non-sharing until requirements are satisfied. This is in stark contrast to the recommendations of the PC Inquiry accepted by the government and meant to be the basis of this Act.

Outcome-based sharing specifies desired results rather than methods or guiding principles. Instead of simply demonstrating policies are in place, entities must demonstrate achievement of mandated outcomes. Assessment is focused on measurable results tested periodically rather than process adherence.

The ARDC recommends that rather than completely replacing the principles-based approach, a hybrid outcomes-principles framework would be optimal.

A hybrid approach would address the current implementation challenges by focusing attention on measurable results while allowing the valuable ethical and conceptual frameworks established by principles-based elements. The principle frameworks that are chosen should support presumptive sharing - 'making data as open as possible and only as closed as necessary'.

8. ***Revise the Objects***

We note the objects of the Act vary from the original guidance and framing by the PC Inquiry ('Access and Use' to 'Availability and Transparency').[47] The objects should be revised to enhance their relevance:

- **Refocus on Use and Impact**: Retire the acronym (DATA) and refocus on improving and increasing use and impact of public sector data, with 'improved use' inclusive of safe, secure and proper.
- **Emphasise timeliness and efficiency**: The objects should explicitly recognise that data value can diminish with time, and streamlined, efficient processes are essential for researcher productivity.
- **Acknowledge cross-jurisdictional dimension**: The objects should more explicitly address the need for coordinated approaches across all levels of government, as many research challenges require integration of Commonwealth, state and territory public sector data.
- **Recognise international context**: Australia's research competitiveness requires alignment with international data sharing frameworks and standards. This would be similar for other sectors.
- **Address reciprocity**: The objects should recognise that data sharing should ideally benefit all participants, including data users, data providers and data subjects.
- **Incorporate the concept of proportionality**: The objects should explicitly recognise the level of control should be proportionate to the sensitivity and risk associated with different data.[48]

[47] Refer Ch 8.1, pp.308-315.

[48] This suggestion highlights that 'data minimisation' (s13 & s16B) should not be included in an Act intended to increase data sharing. Data minimisation is not in the Privacy Act; use of the word minimisation instead refers to the impact or effect. This is not to argue against the data minimisation principle, but that while it might be in guidance, it should not be in the Act.

9. ***Adopt a Tiered Accreditation Framework***

Use of accreditation sets explicit expectations for participants. It provides an important assurance mechanism for validating and then asserting to others that the entity has appropriate data governance and data handling capabilities. It means accredited participants are 'trusted users' and should not be re-evaluated on those same criteria for each proposal.[49]

To achieve the necessary levels of trust, all entities sharing data that is not Open should be accredited prior to any participation in sharing. This is because: data providers need to trust users will handle data appropriately; requesters need to trust that providers will supply data as offered; and all participants need to trust enabling services on which they rely (e.g., authentication). Ideally, accreditation should be conducted by independent standards certified testing authorities.[50]

The Act should specify the need for an accreditation scheme to apply to all participants and that it should be a tiered, risk-proportionate approach with each entity requiring the tier appropriate to the sensitivity category of data it handles and the corresponding control requirements.[51] [52] Beyond this, all other matters of accreditation should be made by the Commissioner and be publicly available.

10. ***Include a Tiered Agreements Framework***

The DAT Act lacks an agreements framework that enables efficient, modernised data sharing. Without this, data sharing proposals face higher transaction costs, reduced legal interoperability, unclear rights and responsibilities, and limitations on control by custodians after data has been shared.

A modern, robust agreements framework has multiple tiers.[53] [54] For example:

- **Data scheme agreements**: Support multiple data sharing initiatives (dataspaces). The binding rules of the scheme ensure all dataspaces within the scheme remain interoperable regarding key governance and technology decisions - it supports 'cross-dataspace interoperability', collectively operating as the (potentially future national) 'public administration dataspace'.[55]
- **Dataspace agreements**: Bind all participants of each dataspace to the governance framework for that dataspace. Participants might join multiple dataspaces across the scheme for minimal additional uplift costs due to the coherence across the scheme. Emerging practice at this level is to use the *Rulebook Model for a Fair Data Economy* originally developed with funding from the Finnish Sovereign Fund (SITRA).[56] The 'rulebook' model consists of two parts: a general part

[49] Non-accredited users should be able to use Open data or else low risk data made available as a result of the Act under other licences and safeguards as defined in scheme rules.
[50] Levels of Assurance for Data Trustworthiness
[51] Voluntary Data Classification Framework
[52] AI Data Security | Cyber.gov.au
[53] Contractual framework - Blueprint v1.0 - Data Spaces Support Centre
[54] Governance Framework for Data Space Operations | Catena-X - Library
[55] Goals and scope of the iSHARE Trust Framework | iSHARE Trust Framework
[56] Rulebook model for a fair data economy (version 3.0) - Sitra

reflecting the rules of the scheme and a second part reflecting the rules agreed by participants of the specific dataspace (e.g., for the funding or operating model).

- **Data transaction contracts**:[57] Govern specific data exchanges between two parties. These rely on, rather than repeat, policy clauses or accreditation criteria in higher level agreements. Once the agreement is made, 'the data itself is shared on separate peer-to-peer channels, which are independent of the dataspace itself. Those peer-to-peer channels enable a diverse set of technologies and are fully customisable to the needs of the two sharing parties.'[58]

This tiered approach enables:[59]

- **Standardised governance**: Dataspace agreements implement governance frameworks, establish common elements like standardised clauses and licenses (if required in addition to scheme provided ones), and reduce transaction costs while increasing legal interoperability.
- **Flexible transactions**: Data transaction contracts or agreements reflect data control principles, allowing providers to set specific terms while operating within broader governance frameworks.

Modern data sharing increasingly relies on automated smart contracts and governance mechanisms (such as for supporting infrastructure for use by artificial intelligence). This requires legislative recognition of machine-executable contracts alongside traditional agreements. The DAT Act should:

- Recognise automated contractual enforcement
- Integrate with technical building blocks for compliance monitoring
- Use mandatory versus non-mandatory contractual clauses that respect regulatory requirements while allowing operational flexibility

Reforming the agreement framework provisions would transform the Act from a permission-based system to an enabling infrastructure that supports scalable, trustworthy data sharing while maintaining appropriate governance and accountability mechanisms.

[57] These would be agreements between organisations of the same government and contracts between separate legal entities, but they would be otherwise identical.
[58] Manifesto of International Dataspaces
[59] The Commonwealth previously developed a tiered agreements framework - the National Collaboration Framework. The IGA could, for example, represent the top tier of this framework. Unfortunately, a similarly tiered approach was not enabled by the DAT Act - it repeated the systemic propensity for 'unnecessarily complicated and time consuming' data sharing agreements as warned against by PM&C (2015), the PC Inquiry (2017) and many others since.

Should the DAT Act be allowed to sunset?

The DAT Act should be amended significantly. If it is not amended, the Act should sunset. Regardless of the mechanism, the ARDC would prefer to see a substantively different Act as soon as possible.

In terms of subsequent actions required, as universities have been unable to access and use data, any legacy issues as a result of the Act ceasing should be minimal. They are best addressed directly with the universities accredited as well as any researchers with requests for data still pending.

Should you wish to discuss these or other matters, please contact Dr Adrian Burton, Deputy Chief Executive Officer [redacted] *or Mr Shannon Callaghan, Senior Data Policy Adviser* [redacted].

Summary of Recommendations

The need for an Act remains, but it must be substantively different from the current one.

The ARDC recommends that the following ten changes are required:

1. **Remove the Legislative Override Provisions**

Eliminate the authorisation to override other laws, which caused the Act to be made overly complex and have the opposite effect to that which was required. The focus should be on developing a coherent universal scheme to be used whenever Commonwealth public sector data is to be shared.

2. **Mandate Participation**

Change the current opt-in system to **mandatory participation** by all custodians holding Commonwealth public sector data - an approach similar to other equally important issues such as health and safety, security policy, and financial accounting. Extend the current data sharing related registers beyond the DATA Scheme so as to capture all sharing of Commonwealth public sector data.

3. **Mandate Data Discovery**

Legally require all Australian Government entities, and those acting on behalf of the Commonwealth, to **publish metadata** publicly for datasets they control, with exemption and review processes available. This will help address Australia's decline from 4th to 28th place on the OECD's *OURdata Index* since 2014.

4. **Establish Presumptive Access**

Shift permission-based frameworks to **presumptive access**, where custodians publish data availability and access policies (‘offers’), enabling entitled entities to access automatically or initiate negotiations.

5. **Remove Entity Exclusions**

Allow participation by any entity that meets accreditation criteria and enters the necessary agreements, rather than excluding entire entities. Apply restrictions based on specific functions or activities rather than blanket exclusions of government, private, foreign and non-government entities.

6. **Replace the Five Safes Framework**

Remove the restrictive *Five Safes Framework* from the Act, which requires specific authorisation against all five safes for every agreement. Replace with the principles from the *Intergovernmental Agreement on data sharing* to describe the behaviours needed to build a national scheme trusted to share data safely.

7. **Adopt a Hybrid Outcomes-Principles Approach**

Implement outcome-focused legislation emphasising measurable impacts of better data use, rather than process adherence. Use ethics and principles to guide implementation efforts and scheme operation.

8. **Revise the Objects of the Act**
    - Refocus on **use and impact** rather than just availability and transparency
    - Emphasise **timeliness and efficiency** recognising that data value diminishes over time
    - Address **cross-jurisdictional coordination** and **international alignment**
    - Incorporate **reciprocity and proportionality**

9. **Implement Tiered Assurance**
    - **Tiered Accreditation**: Risk-proportionate accreditation processes aligned with data sensitivity categories, establishing 'trusted users' who do not require re-evaluation for each proposal
    - **Tiered Agreements**: Multi-level framework from scheme agreements through to automated data usage contracts, enabling scalable and efficient sharing

10. **Extend Use of Federated Trust Services**

Mandate use across organisations and sectors of 'federated trust services' that automate authentication, contract negotiation and enforcement, policy based access control, and compliance logging .

Implementation Pathway

The ARDC recommends exploring **dataspaces** as an implementation approach, leveraging European Union investment and experience.

Conclusion

The current DAT Act prioritises control over enablement. Fundamental restructuring is required to create an enabling infrastructure that supports Australia's research competitiveness and Commonwealth public sector data utilisation. The minimal data sharing achieved under the current DAT Act means legacy issues are manageable at present, primarily requiring direct engagement with accredited universities and researchers with pending requests.

About ARDC

The ARDC drives the development of national digital research infrastructure that provides Australian researchers with a competitive advantage through data.

The ARDC accelerates research and innovation by driving excellence in the creation, analysis and retention of high-quality data assets. We facilitate access to national digital research infrastructure, platforms, skills, data sets and tools from academia, industry and government for all Australian researchers.

The ARDC is funded through the Australian Government's National Collaborative Research Infrastructure Strategy (NCRIS) to support national digital research infrastructure for Australian researchers.