Australian Government
Department of Finance

November 2025

Statutory Review of the Data Availability and Transparency Act 2022 – Final Report

© Commonwealth of Australia 2025
ISBN: 978-1-925205-74-9 (online)
ISBN: 978-1-925205-73-2 (print)



Copyright Notice
The content of this document is licensed under a Creative Commons Attribution 4.0 International – CC BY 4.0 licence with the exception of:

- the Commonwealth Coat of Arms
- the Department of Finance logo
- images
- signature
- content supplied by third parties, as identified.

Third party copyright
Wherever a third party holds copyright in this material, the copyright remains with that party. Their permission may be required to use the material. Please contact them directly.

Use of the Coat of Arms
The terms under which the Coat of Arms can be used are detailed on Department of Prime Minister and Cabinet Website.

Attribution
© Commonwealth of Australia, Department of Finance, Statutory Review of the Data Availability and Transparency Act 2022 – Final Report, 2025.

Feedback, Enquiries and Other Uses
If you have feedback and enquiries about any aspect of the report or any questions about the CC licence or any other use of this document, please contact DATActReview@finance.gov.au.

Contents

Letter of Transmittal **5**

About the Review **6**

Objective 6

Reviewer 6

Terms of Reference 6

Conduct of the Review 6

Timing 7

Glossary/Abbreviations **8**

Executive Summary **10**

Key Issues 10

Recommendations 12

Implementation 13

Findings and Recommendations **14**

Background **17**

DAT Act history 17

Current state of public sector data sharing 19

Operation of the DAT Act 24

Effectiveness of the DAT Act and Commonwealth data sharing **31**

DAT Act objectives 31

Commonwealth data processes 35

DAT Act role 37

Settings and regulatory function **40**

Legislative complexity and inflexibility in a voluntary framework 40

The National Data Commissioner's functions and powers 53

Accreditation framework 60

The value of DAT Act accreditation 66

Participation and data sharing purposes **75**

Not-for-profit users of public sector data 75

Expansion of accreditation eligibility 77
The timing of participation expansion 82
Data sharing purposes 86
The spectrum of data sharing interests 92
The DAT Act does not empower First Nations people 92
Recognition of state and territory data custodianship 97
Broader systems and capability 102
Non-legislative barriers to data sharing 102
Non-legislative reform is required 107
Implementation 116
References 117
Appendices 126
Appendix A: Submissions, meetings and other engagements 126
Appendix B: DAT Bill amendments 129
Appendix C: Current state of public sector data sharing – additional background 131
Appendix D: Examples of legislative complexity and inflexibility in the DAT Act 150
Appendix E: Non-data accreditation frameworks in Australia 159
Appendix F: Digital identity accreditation frameworks 161
Appendix G: Public sector data sharing accreditation frameworks 163
Appendix references 165

Tables, Figures, and Textboxes

Tables

Table 1: Non-data and digital accreditation frameworks in Australia 61
Table 2: Digital identity accreditation frameworks in the UK, EU, Canada, and Australia 63
Table 3: Data sharing accreditation frameworks in the UK, EU, and Canada 64
Table 4: Proposed accreditation categories 73

Figures

Figure 1: Hierarchy of steps in principles-based legislative design 45

Textboxes

Box 1: GenV project 31

Box 2: The Sax Institute's 45 and Up Study 79

Box 3: The NSW Lumos Program 80

Box 4: Maranguka Justice Reinvestment Project 81

Letter of Transmittal

11 November 2025

Senator the Hon Katy Gallagher

Minister for Finance

Parliament House

CANBERRA ACT 2600

Dear Minister,

You appointed me as the Independent Reviewer for the Statutory Review of the *Data Availability and Transparency Act 2022* (DAT Act) to consider the DAT Act's effectiveness and whether its operation supports improvements in public data availability, sharing and transparency.

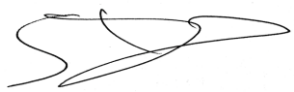
In accordance with the Terms of Reference and section 142 of the DAT Act, I am pleased to submit my Report of the Statutory Review of the DAT Act.

In conducting the Review, I have been particularly interested in the experience of the DAT Act accredited data custodians and data users, stakeholders and other interested parties on the impact of the Act in overcoming barriers to Commonwealth data sharing. To this end, I had excellent engagement by Commonwealth and state and territory government entities, universities, research institutes, private companies and individuals and I thank these participants for their time and contributions.

I would also like to thank the Secretariat provided by the Department of Finance and the Australian Bureau of Statistics. Taylor Black, James Borthwick, Wolfgang Hertel, Julia Minassian and Graeme Page provided me with exceptional support, analysis and management of the Review.

I am happy to assist with any matters in relation to our Report.

Yours sincerely,



Stephen King

About the Review

Objective

The Review considered the effectiveness of the *Data Availability and Transparency Act 2022* (Cth) (DAT Act) and whether its operation supports improvements in public data availability, sharing and transparency.

Reviewer

The Minister for Finance, Senator the Hon Katy Gallagher (the Minister), appointed Dr Stephen P King as the independent reviewer on 27 March 2025.

Terms of Reference

In accordance with its Terms of Reference, the Review considered the following:

- Does the Act support improved public sector data availability and transparency, including sharing public sector data in a controlled way?
- Has the operation of the Act advanced its objects?
- How does the operation of the Act compare and interact with other existing mechanisms for facilitating access to, sharing and use of public sector data?
- Stakeholder satisfaction with the operation of the Act as a tool for reducing barriers and enabling effective access to, sharing and re-use of public sector data.
- Should the Act remain in force past its current sunset date of 1 April 2027?
- Any other relevant matters.

Conduct of the Review

An Issues Paper was released on 30 April 2025 to inform the Review's consideration of its findings and recommendations. Public consultation on the Issues Paper ended on 30 May 2025.

The Review received 62 public submissions from Commonwealth and state and territory government entities, universities, research institutes, private companies and individuals. This initial consultation process also included 26 meetings with key stakeholders.

A Draft Findings and Recommendations paper was released on 18 July 2025. Public consultation on the Draft Findings and Recommendations paper ended on 8 August 2025.

The Review received 25 public submissions on the paper from Commonwealth and state and territory government entities, universities, research institutes, private companies and individuals.

A list of the public submissions and meetings is available at Appendix A and copies of the submissions will be made available on the Department of Finance's website when the Final Report is published.

In making the findings and recommendations in this Report, the Review considered all feedback received from stakeholders in response to the Issues Paper and Draft Findings and Recommendations paper. The Review also followed up some submissions with targeted questions to obtain further information.

Timing

Section 142 of the DAT Act requires periodic reviews of the DAT Act, and for an initial review to commence by 1 April 2025 and be completed by 1 April 2026 (the third and fourth anniversaries of the commencement of the Act).

The Review formally commenced on 27 March 2025, being the date that Dr King was appointed as the independent reviewer.

The Review is taken to be completed when the Minister responsible for the DAT Act is given a written report about the Review. A copy of the report must be provided to each House of the Parliament within 15 sitting days after the Minister receives it.

Glossary/Abbreviations

Abbreviation	Name
1975 Act	*Statistics Act 1975* (NZ)
AAMRI	Association of Australian Medical Research Institutes
ABS	Australian Bureau of Statistics
ACCOs	Aboriginal Community Controlled Organisations
ACNC	Australian Charities and Not-for-profits Commission
ACSC	Australian Cyber Security Centre
ADSP	Accredited Data Service Provider
AI	Artificial Intelligence
AIFS	Australian Institute of Family Studies
AIHW	Australian Institute of Health and Welfare
AIHW Act	*Australian Institute of Health and Welfare Act 1987* (Cth)
AISA	Approved Information Sharing Agreement
ALRC	Australian Law Reform Council
ANDII	Australian National Data Integration Infrastructure
APPs	Australian Privacy Principles
ATO	Australian Taxation Office
BLADE	Business Longitudinal Analysis Data Environment
CATSI Act	*Corporations (Aboriginal and Torres Strait Islander) Act 2006* (Cth)
CDO Group	Chief Data Officers Group
CLGs	Companies limited by guarantee
CSA	*Census and Statistics Act 1905* (Cth)
D&AWG	Data and Analytics Working Group
DAT Act	*Data Availability and Transparency Act 2022* (Cth)
DAT Bill	Data Availability and Transparency Bill 2020
DAT Bill 2022	Data Availability and Transparency Bill 2022
DAT Code	Data Availability and Transparency Code 2022 (Cth)
Data Maturity Report	2024 Australian Public Service Data Maturity Report
DDMM	Data and Digital Ministers Meeting
DDMM SOG	DDMM Senior Officials Group
DEA	*Digital Economy Act 2017* (UK)
DPA	*Data Protection Act 2018* (UK)
DSA	*Data and Statistics Act 2022* (NZ)
DSDG	Deputy Secretaries Data Group
FOI Act	*Freedom of Information Act 1982* (Cth)
GenV	Generation Victoria
Harper Review	Competition Policy Review
ICES	Institute for Clinical Evaluative Sciences
IGA	Intergovernmental Agreement on data sharing between Commonwealth and State and Territory governments
IPPs	Information Privacy Principles

ISG	Information Sharing Guidelines for Promoting Safety and Wellbeing
Murray Inquiry	Financial System Inquiry
NDDA	National Disability Data Asset
NDIS	National Disability Insurance Scheme
NHDH	National Health Data Hub
NIAA	National Indigenous Australians Agency
OAIC	Office of the Australian Information Commissioner
ONDC	Office of the National Data Commissioner
OPC	Office of Parliamentary Council
PC Inquiry	Inquiry into Data Availability and Use
PHNs	Primary Health Networks
PHRN	Population Health Research Network
PLIDA	Person Level Integrated Data Asset
Privacy Act	*Privacy Act 1988* (Cth)
Privacy Act NZ	*Privacy Act 2020* (NZ)
Revised EM	Revised Explanatory Memorandum, DAT Bill 2022
SABRE	South Australian Business Research Environment
Scrutiny Committee	Senate Standing Committee for the Scrutiny of Bills
SDDC	Secretaries Digital and Data Committee
Singapore Statistics Act	*Statistics Act 1973* (Singapore)
Statistics Act	*Statistics and Registration Service Act 2007* (UK)
Stats NZ	Statistics New Zealand
Supplementary EM	Supplementary Explanatory Memorandum, DAT Bill 2022
TFN	Tax File Number
TRE	Trusted Research Environment
Trusted Entities	Data and Digital Ministers Meeting Work Program Four: 'Defining 'trusted entities' for the purposes of national data sharing'
UK GDPR	UK General Data Protection Regulation
VNDA	Vocational Education and Training National Data Asset

Executive Summary

The DAT Act was introduced in response to the recommendations of the 2017 Inquiry into Data Availability and Use (PC Inquiry), which identified substantial potential benefits flowing from greater data availability and use, including supporting economic and research opportunities, and enabling streamlined and efficient service delivery.

The DAT Act established new legislative and governance arrangements to enable better use of public sector data across the economy while ensuring appropriate safeguards were maintained to protect sensitive information. It also established a National Data Commissioner to oversee these arrangements.

Section 142 of the DAT Act requires periodic reviews of the Act, and for an initial review to commence by 1 April 2025 and be completed by 1 April 2026. Without legislative amendment, the DAT Act will cease to have effect (sunset) on 1 April 2027.

In the first three years of the DAT Act the Office of the National Data Commissioner (ONDC) has implemented an accreditation framework, made legislative instruments to support the operation of the DAT Act, published guidance to support DAT Act participants and adopted an explicitly facilitative posture to support data sharing under the DAT Act.

Key Issues

The Review considers the effectiveness of the DAT Act and the extent to which it has achieved its objects of improving public sector data availability and transparency. Findings and recommendations are presented under five themes:

- effectiveness of the DAT Act and Commonwealth data sharing
- settings and regulatory function
- participation and data sharing purposes
- the spectrum of data sharing interests, and
- broader systems and capability.

The Review finds that the DAT Act has not been effective in achieving its objectives. This is due, in a large part, to it being a complex and prescriptive framework that is voluntary for Commonwealth data custodians. Further, disincentives for custodians to use the DAT Act or share more data are likely to persist so long as they have unlimited discretion to refuse requests.

While the Review recommends changes that orientate data custodians to respond more favourably to data sharing requests, such changes can only be justified if the DAT Act is made more enabling and simpler to use.

Effectiveness of the DAT Act and Commonwealth data sharing

Fundamental flaws in the design of the DAT Act have prevented it from facilitating greater sharing of public sector data. The DAT Act's limited uptake is largely due to these design issues, many of which mirror broader, systemic challenges in Commonwealth data sharing.

As a result, the economic and social benefits anticipated by the PC Inquiry and the Government have not been realised.

Despite some improvements in data sharing outside the DAT Act (for example, in the continued improvement of data sharing assets and greater commitments to share and make non-sensitive data open by default), significant challenges of the kind identified by the PC persist. There is an aversion to risk, resource constraints, and limited incentives for data custodians to share data that impede timely and effective data sharing. There is also limited visibility of data holdings, inconsistent processes across agencies, and a lack of centralised registers or standardised data sharing pathways.

Stakeholders generally support the continuation of the DAT Act, but only if it is substantially reformed. While the objects of the Act remain relevant, its current complexity and lack of flexibility limit its utility and must be addressed. There is a strong demand for a clear, efficient, and consistent authorising pathway for data sharing, as well as for the DAT Act accreditation framework to be retained and improved to better support the needs of data sharing participants.

The Review recommends the DAT Act not sunset, subject to it being amended to provide a clear authorising pathway that enables greater and better sharing of Commonwealth data for approved purposes.

Settings and regulatory function

The DAT Act is hampered by legislative complexity and inflexibility, making it difficult and costly to use, with data custodians preferring their own frameworks. The Act's authorisation framework is overly prescriptive and voluntary for custodians, resulting in limited uptake for public sector data sharing. The inflexibility of the DAT Act further restricts the types of data sharing activities that can be authorised, while the absolute discretion given to data custodians to refuse requests, without meaningful oversight or review, undermines the Act's objectives.

The Review recommends shifting to a principles-based approach to reduce complexity and improve flexibility, embedding a default posture of agreeing to share data (with refusals only in limited, reviewable circumstances), and recalibrating the National Data Commissioner's functions to focus on assurance, oversight, and facilitation of data sharing decisions.

Participation and data sharing purposes

Participation in the DAT Act is currently too limited, as eligibility for accreditation is restricted to government bodies and universities, excluding not-for-profit research institutes. There is broad stakeholder support for expanding eligibility to unlock greater public benefit, improve service delivery, and better align with existing data sharing practices. Also, while the current DAT Act data sharing purposes are broadly appropriate, enhancements are needed to support data curation and the creation of linked assets.

The Review recommends that entities that can seek accreditation to request and use data under the DAT Act should be expanded to include Aboriginal Community Controlled Organisations (ACCOs), not-for-profit research institutes (including independent research organisations and medical research institutes), Primary Health Networks (PHNs), and not-for-profit service delivery organisations (including Approved Aged Care Providers). The

Review also recommends expanding the permitted purposes for data sharing under the DAT Act to include data curation and the creation of data assets, as well as some refinements to the service delivery purpose to ensure it can operate as intended.

These changes would enable more flexible, efficient, and inclusive data sharing, while maintaining appropriate safeguards, and would help address unmet demand for access to Commonwealth data in the public interest.

The spectrum of data sharing interests

The DAT Act does not adequately empower First Nations people, nor does it provide equivalence to state and territory data custodians, limiting its effectiveness in supporting national commitments such as the National Agreement on Closing the Gap and the Framework for the Governance of Indigenous Data. The DAT Act's current eligibility and governance settings restrict many First Nations organisations and communities from accessing or controlling data about themselves, and do not require data custodians to consider Indigenous data governance principles or co-design processes. Similarly, the Act does not grant states and territories equal standing with the Commonwealth in data sharing decisions, which impedes the creation of connected, cross-jurisdictional datasets and consistent national frameworks.

The Review recommends expanding accreditation to include ACCOs, embedding Indigenous data governance frameworks, and explicitly recognising the roles of states and territories, while also calling for the development of a nationally consistent data sharing framework to achieve full interoperability and standardised pathways for users to access public sector data across all levels of government.

Broader systems and capability

Non-legislative barriers continue to restrict effective data sharing across the Australian public sector, even as legislative reforms progress. These barriers include limited data discoverability, inconsistent data standards, fragmented and duplicative platforms, risk aversion, and insufficient capability and capacity.

The Review recommends that a new leadership function could provide strategic direction for the data sharing ecosystem, including the National Data Commissioner and the DAT Act, and drive structural changes to help 'unblock' Commonwealth government data sharing. A baseline dataset of data sharing across the Commonwealth is needed to inform policy and investment decisions for the entire ecosystem. It should be a mandatory requirement through amending legislation (for example, the Public Governance, Performance and Accountability Rule 2014 or the DAT Act) that data custodians provide information about all their data sharing activities across all their data sharing frameworks.

Recommendations

Despite its challenges, the Review considers that there is a role for the DAT Act and that it should not be allowed to sunset. However, significant amendments are required to ensure that it can provide a clear authorising pathway that enables greater and better sharing of Commonwealth data.

The Review offers 15 recommendations to improve the statutory framework, as well as non-legislative changes aimed at creating a clear, efficient, and consistent framework for public sector data sharing.

A list of the findings and individual recommendations on a thematic basis can be found in the following Findings and Recommendations section.

Implementation

Without legislative intervention, the DAT Act will sunset on 1 April 2027. If the Review's recommendations are adopted, it may be necessary to extend the operation of the DAT Act while amendments are progressed. Each of the recommendations are intended to improve the operation of the DAT Act, or data sharing more generally.

However, if only certain recommendations were to be prioritised, the Review considers Recommendations 1 to 3 to be essential.

These recommendations are critical to resolving the challenges experienced with the current DAT Act settings. They are focused on delivering on the expectations of the DAT Act's framework, and increased data sharing will not occur without them. If the recommendations are not accepted and implemented, the DAT Act's authorising framework will continue to be ineffective and underutilised, and should be allowed to sunset.

Findings and Recommendations

The following table summarises the findings and recommendations from the DAT Act Review.

Findings	Recommendations
Effectiveness of the DAT Act and Commonwealth data sharing	
1. The DAT Act has not achieved its objectives. 2. Commonwealth data processes continue to impede data sharing. 3. There is a role for the DAT Act, but substantial modifications are required.	1. The DAT Act should not sunset, subject to it being amended to provide a clear authorising pathway that enables greater and better sharing of Commonwealth data for approved purposes.
Settings and regulatory function	
4. The DAT Act's authorisation framework is difficult to use because it is too complex, including because it is overly prescriptive, and inflexible. Being both difficult to use, and entirely voluntary for data custodians, uptake of the DAT Act for public sector data sharing has been very limited.	2. The DAT Act's authorising framework should be amended to take a principles-based approach to ensure clarity and flexibility. 3. The DAT Act should embed a default posture of agreeing to share data, with data custodians able to refuse requests in appropriately limited circumstances, subject to oversight and review.
5. The National Data Commissioner's current functions and powers do not effectively enable them to support uptake of the DAT Act, or to drive improvements across the broader public sector data sharing system. The National Data Commissioner is therefore not empowered to successfully advance the objects of the DAT Act.	4. The National Data Commissioner's functions and powers should be recalibrated to focus on assurance, oversight and assistance in facilitating data sharing decisions.

Findings	Recommendations
6. DAT Act accreditation is a valuable framework which supports trust in the data system, however, its processes are perceived as burdensome, complex, and inflexible. The uniformity of accreditation standards, requirements for organisational-level accreditation, and strict authorised officer and eligible entity definitions act as barriers to participation under the DAT Act.	5. The DAT Act should establish a permissions-basis for accreditation which replaces the current strict 'user' and 'data service provider' accreditation designations. 6. Explicit accreditation categories should be introduced to more simply reflect the application of different accreditation standards and to facilitate alignment between accreditation and data sharing use-cases. 7. Transparency and other measures which promote greater regulatory flexibility in respect of DAT Act accreditation should be introduced and have consideration to broader developments in the data system.
Participation and data sharing purposes	
7. Expanding DAT Act accreditation to include ACCOs, not-for-profit research institutes, and not-for-profit service delivery organisations would enhance the value derived from public sector data sharing. Nevertheless, such expansion should be balanced with careful consideration of both the mechanisms available to support the participation of new entrants and preserving public trust and social license in the data system.	8. The entities that can seek accreditation to request and use data under the DAT Act should be expanded to include ACCOs, not-for-profit research institutes (including independent research organisations and medical research institutes), PHNs, and not-for-profit service delivery organisations (including Approved Aged Care Providers). 9. The DAT Act should include a power which allows the Minister to expand accreditation eligibility further, subject to advice from the National Data Commissioner (or other appropriate office or body with appropriate expertise).

Findings	Recommendations
8. The current DAT Act data sharing purposes are generally appropriate, however improvements are needed to enable sharing for the purposes of data curation. The use of data for government service delivery under the DAT Act is complex and requires a recalibration of settings which balance the need for more simplified data sharing processes with privacy protections.	10. Expand the data sharing purposes to include data curation and the creation of data assets. 11. Improve the operation of the service delivery purpose, and particularly the interaction with the prohibition on enforcement-related purposes.
The spectrum of data sharing interests	
9. The DAT Act is not well positioned to help Government achieve its commitment under the National Agreement on Closing the Gap or support data sharing consistent with the Framework for the Governance of Indigenous Data.	12. Embed Indigenous data governance frameworks into decision-making processes and expand the participation in the DAT Act so that First Nations peoples are better heard, recognised and empowered to contribute to positive outcomes for Indigenous communities.
10. The DAT Act does not provide equivalence to state and territory data custodians, which limits its capacity to enable two-way data sharing between jurisdictions.	13. The DAT Act should explicitly recognise the roles of states and territories in Commonwealth processes that involve jurisdictional data. 14. Longer term, there should be a nationally consistent data sharing framework that achieves full interoperability across jurisdictions and provides standardised pathways for users to access Australian public sector data held by any government.
Broader Systems and Capability	
11. The data ecosystem, in general, requires a capability uplift to enable better outcomes for participants.	15. Further investment in the data ecosystem is required to improve capability and enable better outcomes for participants.

Background

DAT Act history

Origins of the DAT Act

1. In 2014 the Financial System Inquiry (Murray Inquiry) (Department of the Treasury 2014) recommended the Commonwealth undertake an inquiry into the costs and benefits of increasing and improving access to and use of data. The Murray Inquiry noted that increasing access to data could enhance consumer outcomes, better inform decision making, and facilitate greater efficiency and innovation in the financial system and the broader economy.

2. In 2015 the Competition Policy Review (Harper Review) (Department of the Treasury 2015) recommended the Commonwealth work with industry, consumer groups and privacy experts to allow consumers to access and use their own data for their own purposes and enable new markets for personal information services.

3. Based on these recommendations, in 2017 the then Treasurer requested the Productivity Commission undertake an inquiry into data availability and use (PC Inquiry) that included both public and private sector data.

4. In the request, the Treasurer highlighted the benefits that could stem from improving data sharing. Specifically, the Treasurer stated that (Productivity Commission 2017: v):

> Effective use of data is increasingly integral to the efficient functioning of the economy. Improved availability of reliable data, combined with the tools to use it, is creating new economic opportunities. Increasing availability of data can facilitate development of new products and services, enhance consumer and business outcomes, better inform decision making and policy development, and facilitate greater efficiency and innovation in the economy.

5. The PC Inquiry states that data should be used to drive economic value and create a comparative advantage for Australia. Based on previous studies, the PC Inquiry estimated[1] the economy-wide impacts from the improved use of public sector data could be between $7 billion and $64 billion per year.[2] Following the PC Inquiry, other studies have considered the economic value of specific types of public sector data.[3]

6. The PC Inquiry identifies potential benefits flowing from greater government data availability and use, including supporting economic and research activities, and enabling

[1] In 2013 dollars.

[2] The Productivity Commission advised the breadth of this range reflected different measures of benefit or value, with estimates based on different types of data (some use spatial data only, while others use a broader range of public sector data), different assumptions about how data is used and the associated benefits, and considerable structural differences between the countries for which some estimates were initially made (prior to being converted into an estimate for Australia).

[3] For example, Lateral Economics (2017) estimated that for every $1 invested in the Australian Census, $6 of value was generated to the Australian economy. Deloitte Access Economics (2023) highlight that government geoscience data contributed approximately $76 billion in added value to the Australian economy including 80,000 full-time equivalent jobs in 2021-22.

streamlined and efficient service delivery. For example, the Productivity Commission notes that health data can help policy makers and researchers to:

- identify emerging health issues within communities
- identify factors that contribute to particular medical conditions
- assess the safety of pharmaceuticals and other treatment options on an ongoing basis, and
- evaluate the effectiveness and efficiency of health policy.

7. Separately, the Productivity Commission found when comparing Australia to many other similar countries (2017:73-75):

> Australia lags in opening up public sector data… Australia registers particularly low scores on measures of spending, legislation and health data… Along with the shortfalls in Australia's current implementation of open data policies, there appears to be little systematic sharing of data between public sector agencies, or between agencies and researchers.

8. In response to the PC Inquiry, and recognising that unlocking both public and private sector data could drive economic growth, the Australian Government agreed to establish (Department of the Prime Minister and Cabinet 2018):
   - a National Data Commissioner to implement and oversee a streamlined, more efficient government data sharing and release framework, with the National Data Commissioner to be the trusted overseer of the public data system, and
   - new legislative and governance arrangements to enable better use of data across the economy while ensuring appropriate safeguards to protect sensitive information.
9. The new legislative and governance arrangements intended to overcome three key barriers to public sector data sharing:
   - legal restrictions that prevented Australian Government entities providing others with access to data in its custody, even when the sharing would have been both reasonable and safe
   - lack of clarity as to who Australian Government agencies could trust to share data with, and
   - uncertainty about best practices and appropriate safeguards for sharing data safely.[4]

Legislative process

10. The Data Availability and Transparency Bill 2020 (DAT Bill) was introduced to the Parliament on 9 December 2020. The DAT Bill proposed a new data sharing scheme and regulatory framework for sharing Commonwealth Government public sector data (Explanatory Memorandum, DAT Bill 2020).
11. In introducing the DAT Bill, the responsible Minister highlighted the value of data-driven government services for Australians, consistent with the findings of the PC Inquiry, and stated that the DAT Bill laid the foundation to realise these benefits and establish

[4] Submission 38, National Data Commissioner.

world-class and connected government services (DAT Bill 2020 Second Reading. Robert, Stuart).

12. The DAT Bill was subject to several inquiries[5] as well as discussions with the then Opposition that resulted in substantial amendments before it was passed by both Houses of Parliament. These amendments included increased privacy protections and a reduction in the types of entities eligible to participate (including the removal of foreign organisations and private entities). Accordingly, the DAT Bill 2022 was amended to include a requirement to undertake a review of the legislation three years after its commencement, and an automatic sunset provision five years from its commencement.

13. The DAT Act received Royal Assent on 30 March 2022 and came into effect the following day.

Current state of public sector data sharing

Commonwealth overview

Data sharing operating environment

14. Outside of the DAT Act, other frameworks are routinely used to authorise the sharing, collection and use of public sector data. Commonwealth data custodians share data for a range of purposes and with many users, some of which are outside the scope of the DAT Act. This sharing can be authorised under rules of general application, such as the *Privacy Act 1988* (Cth) (Privacy Act), or by agency specific legal frameworks that permit data to be shared under certain conditions.[6]

15. Most of these general and specific data sharing frameworks pre-date the DAT Act, providing a crowded environment where some agencies operate established data sharing schemes that have grown in relevance as demand and acceptance of sharing public sector data has increased. Unsurprisingly, agencies tend to prefer iterating on their established systems, due to their experience and familiarity with them.

16. Augmenting the legal frameworks is a series of Commonwealth strategies and standards. These set expectations and best practice for how Commonwealth agencies manage broad issues across the data ecosystem, such as the Data and Digital Government Strategy as well as for specific themes or areas of interest, such as the Framework for the Governance of Indigenous Data.[7]

17. Whole-of-government data governance groups promote the consistent and effective use of public sector data, of which data sharing is one element. These groups vary in focus and membership, ranging from strategic decision-making bodies comprising senior Commonwealth officers through to groups comprising data practitioners who share information, guidance and best practices at the operational level.[8]

18. A range of systems across the Commonwealth provide platforms to facilitate data sharing. These include platforms for data users to identify and request access to data,

[5] See Appendix B for more information on the parliamentary discussions.
[6] See Appendix C, Part 1 for summaries of the key legal frameworks used by Commonwealth agencies to share data.
[7] See Appendix C, Part 2 for summaries of the key strategies and standards that apply to Commonwealth data sharing.
[8] See Appendix C, Part 2 for summaries of key whole-of-government data governance groups.

platforms to access or explore the data itself, and platforms for agencies to create integrated data for data sharing in a secure, consistent and expedient manner.[9]

19. At the time of the PC Inquiry, many of today's data sharing frameworks, assets and systems did not exist or had not reached a mature state capable of delivering sustained data sharing outcomes (Productivity Commission 2017). Data assets such as the Business Longitudinal Analysis Data Environment (BLADE) created in 2014, Person Level Integrated Data Asset (PLIDA), created in 2015), and the National Health Data Hub (NHDH) analysis asset (created in 2021) are examples of significant progress over the last decade (Gruen 2020).[10] These assets are enabled using agency specific (non-DAT Act) legislation and are supported by strategies, standards, platforms and infrastructure to develop data assets that unlock greater insights from public sector data.
20. As of August 2024, the only data asset to have been created using the DAT Act is the National Disability Data Asset (NDDA).
21. Data sharing typically occurs through a range of agreements with different durations, purposes, and recipients. In June 2024, a survey of 19 Commonwealth Government agencies revealed there were over 11,000 data sharing agreements outside of the DAT Act (noting some of these may have been entered into before the DAT Act had commenced).[11] Some larger data custodians have established more standardised arrangements supported by enterprise data-sharing platforms, governance arrangements, delegations and instruments or agreements that enable data sharing. In contrast, some other custodians only share data on an ad hoc basis, or do not share at least parts of the data they hold at all, even with other Commonwealth agencies.

Data sharing capability and capacity

25. Commonwealth agencies' data sharing capability and capacity are essential to service user demand as the number of available datasets and data sharing agreements continue to grow.
26. Data sharing capability is a subset of broader organisational capability. This capability ensures that data custodians have the governance and skill to make data discoverable, understand and provide services to emerging fields of analysis, mitigate the risks of sharing data, and can make informed data sharing decisions.
27. Data sharing capability can differ from an agency's normal data capability or maturity. Data sharing requires organisations to create or support pathways for their data to be accessed by other parties for a wide range of potential uses. This action may have no direct bearing on an agency's normal functions or priorities and can expose that agency to new capability requirements that it has no knowledge or experience in.
28. For example:
    - A data custodian that routinely shares identifiable data directly to another agency for compliance purposes may have robust safeguards to establish a secure pipeline to transmit data, and craft contractual agreements to ensure that data will not be misused by the recipient. That same data custodian may not have the capability or

[9] See Appendix C, Part 3 for summaries of key platforms enabling Commonwealth.
[10] See Appendix C, Part 3 for summaries of these data assets, including growth metrics.
[11] The figure comes from an informal survey conducted by the ONDC, supported by the Department of Finance, and was not compulsory for agencies to complete.

confidence to share data in unfamiliar settings, such as the ability to apply privacy safeguards so that data can be published as a de-identified, open dataset without restriction.

- A data custodian may be unfamiliar with the analytical techniques and systems requirements that particular data users require to realise outcomes for their research project. This may require investment for the data custodian to investigate and mitigate any risks to their data if used in this manner, but that investment may not be a priority compared to the custodian's own internal priorities and data needs.

29. Data custodians with sufficient data sharing capability require adequate levels of capacity to support data sharing needs while also delivering on their core work programs and priorities. A data custodian's capacity can extend to a variety of actions, including resourcing data capability uplift, processing data sharing requests, and maintaining platforms or data assets for users to engage in data sharing. Timely and informed data sharing decisions can be impacted where demand for data outstrips an agency's capacity to receive, consider, approve and ultimately share data.

30. Many Commonwealth data custodians' enterprise strategies directly or indirectly reference improving data sharing as a goal but the comparative priority of this goal, when measured against other organisational priorities, is unclear.[12]

31. Policy proposals such as Data Integration Partnerships for Australia (DIPA) provide fixed-term, program-specific investments to improve whole of government data sharing uplift (Department of Finance 2024a). This includes investing in new assets, infrastructure and platforms to enable data sharing, and resources to support or undertake analysis. Other policy proposals can provide investment for certain components.

32. Aside from the abovementioned fixed-term funding measures, departmental appropriation[13] and charging users (on a cost-recovery basis) are the main sources used to resource agencies' data sharing capability or capacity (Department of Finance 2023a; Department of Finance 2023b).

National overview

Data sharing operating environment

33. All levels of government create public sector data as they deliver services, regulate activities and interact with people and businesses. Such data is typically created and held by individual agencies based on their role and interactions.

34. State and territory governments are active in connecting data from different agencies and jurisdictions to better understand the people they serve. Within jurisdictions connected information can improve the effectiveness of government services and improve how Australians access services, for example, using a single front door. Cross-jurisdictional data sharing helps governments at all levels understand their people as they interact with related or exclusive services provided by other jurisdictions. Connected

[12] Based on an assessment of select Commonwealth custodian's data-related enterprise strategies, including ABS (n.d.); AIHW (2022); DCCEEW (2024); DEWR (2024); Education (2023); Health (2022); DSS (2024).
[13] For ordinary operating costs.

datasets also provide a more complete picture of Australians' lives, which is valuable for broader research, policy design and evaluation by researchers outside of government.[14]

35. Signed by National Cabinet in July 2021, the Intergovernmental Agreement on data sharing between Commonwealth and State and Territory governments recognises public sector data as a shared national asset and aims to maximise the value of data to deliver outstanding policies and services for Australians. It commits all jurisdictions to share public sector data as a default position, where it can be done securely, safely, lawfully and ethically. A National Data Sharing Work Program focusses effort on specific priority data sharing areas (Department of Finance n.d.).

36. Commonwealth agencies mostly share data through a range of agency-specific laws that permit the collection and sharing of data in a manner consistent with the Privacy Act. These laws and authorisations have largely evolved to support agency functions, practices and information needs as they change over time. The result is a complex environment where timely data sharing can be significantly impeded by lack of consistent and interoperable frameworks.

State systems

37. State government-held public sector data often faces a similar challenge of siloed data holdings and agency-specific legislation. To address this, many states have implemented their own state-wide data sharing frameworks with a common goal to remove barriers to data sharing. Three examples highlight how data sharing can be enabled using legislative and non-legislative enablers:[15]

    - South Australia does not have legislation for general privacy but instead applies a Cabinet Administrative Instruction to set personal information handling requirements for government agencies (Government of South Australia 2020). Data sharing within South Australia pairs legislation (to enable data sharing for policy making, program management and service planning and delivery) and non-legislative guidelines (to enable data sharing that is required on an immediate-needs basis).
    - Queensland relies on the general provisions of its privacy legislation, and agency specific legislation, to authorise data sharing, but pairs this with a non-legislative framework to inform how its agencies should approach data sharing decisions and assess the risks against the benefits.
    - Western Australia has recently introduced data sharing legislation that integrates its data sharing enablers alongside its privacy requirements. Key data sharing components, such as requirements for data sharing agreements are prescribed in detail.

38. These frameworks have enabled states and territories to develop their own data assets and contribute to the creation of national data assets and platforms (which are co-designed by Commonwealth, state and territory governments).[16]

39. A notable departure between Commonwealth and state-wide data sharing frameworks is the DAT Act's accreditation framework as a standard to proactively and independently assure custodians of a user's suitability to handle data. Jurisdictions do not administer

[14] See Appendix C, Part 3 and 4 for examples of connected datasets.
[15] See Appendix C, Part 4 for summaries of state-based data sharing frameworks.
[16] See Appendix C, Part 4 for summaries of state and national data assets.

their own accreditation framework (legislative or otherwise) to verify a user's fitness to access the data and rely on the decision maker to evaluate the risks.

National governance structures

40. The Commonwealth and state and territory governments have established several whole-of-government data governance groups to ensure consistent and effective data management across jurisdictions. Representatives on these groups can range from ministerial representatives for the Data and Digital Ministers Meeting to senior government officials in the Data and Analytics Working Group to support the National Data Sharing Work Program (Department of Finance 2024b; Department of Finance 2024c).

41. These groups focus on various aspects of data governance, including information sharing, best practices, and strategic guidance. Some groups will focus on a wide range of activity while others will support specific data sharing initiatives or themes.[17]

International comparisons

42. Other jurisdictions face similar challenges to Australia with sharing government-held data for public benefit. There is no clear overseas example of a completely effective legislative framework that operates like the DAT Act, although there has been success in implementing different models.

43. Overseas, countries employ different systems and platforms to enable data sharing and deliver improved Government service delivery or access to data for research or policy purposes. There is no clear overseas example of a successful platform or system that enables the sharing of data for both service delivery and research or policy-making purposes.[18]

Related initiatives/reviews

44. There are several initiatives and reviews that have been completed or are in progress that have a bearing on Commonwealth data sharing,[19] with key findings or recommendations including the following:

- The Productivity Commission 5-year Productivity Inquiry recommends private sector access to government data (PC 2023).
- The Productivity Commission Investing in cheaper, cleaner energy and the net zero transformation Inquiry includes an interim finding that gaps in environmental and cultural heritage data delay approval processes and increase costs, and the interim recommendations is for the Australian Government to share environmental data with appropriate protections for culturally and commercially sensitive information (PC 2025a).
- The Productivity Commission Harnessing data and digital technology Inquiry predominately focusses on improving private sector and consumer data flows, it also

[17] See Appendix C, Part 2 for summaries of national governance structures.
[18] See Appendix C, Part 5 for examples of legislative frameworks used by other countries.
[19] See Appendix C, Part 6 for summaries of related initiatives and reviews.

included themes and messages around the Australian Government's role in improving data sharing (PC 2025b).

- The Government response to the Privacy Act Review Report concludes that an overhaul of Australia's privacy laws is required to ensure they remain fit-for-purpose in the digital age (Australian Government 2023). This includes strengthening privacy laws to ensure the collection, use and disclosure of people's personal information is reasonable, reflects community expectations and is adequately protected from unauthorised access and misuse.
- The National Data Sharing Work Program includes a work program with increased focus on national guidance to enable best-practice family and domestic violence information sharing, establish the attributes of a 'trusted entity' to support national public sector data sharing and create foundational infrastructure for a national location spine to link together datasets (Department of Finance 2025).

Operation of the DAT Act

Overview of the DAT Act and legislative framework

45. The DAT Act's objects are to:
    - serve the public interest by promoting better availability of public sector data
    - enable the sharing of public sector data consistently with the Privacy Act and appropriate security safeguards
    - enhance integrity and transparency in sharing public sector data
    - build confidence in the use of public sector data, and
    - establish institutional arrangements for sharing public sector data.
46. The DAT Act establishes a data sharing scheme (the DATA Scheme) under which Commonwealth bodies are authorised to share public sector data with accredited users, and accredited users are authorised to receive and use the data, in a controlled way. The sharing, collection and use of data must be part of a project that is done for one or more of the permitted data sharing purposes and must be undertaken consistently with the specified data sharing principles.
47. For the purposes of the DAT Act, public sector data encompasses all data lawfully collected, created, or held by a Commonwealth body, or on its behalf. This includes data provided to a Commonwealth body by bodies outside of the Commonwealth such as from State or Territory Governments, or the private or non-profit sectors. Data includes facts, statistics, and other information capable of being communicated, analysed or processed via physical or electronic means.[20]
48. The DAT Act is supported by subordinate legislation, including:
    - the Data Availability and Transparency Regulations 2022 (Cth) which prescribe specific circumstances where data is barred from being shared under the DAT Act

[20] Data sharing is precluded if it is to be used for an enforcement related purpose or relates to, or prejudices, national security within the meaning of the *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth).

- the Data Availability and Transparency Code 2022 (Cth) (DAT Code) which provides further guidance and conditions relating to the operation of the DAT Act
- the Data Availability and Transparency (National Security Measures) Code 2022 (Cth) which provides further guidance and conditions relating to National Security issues.

Authorising framework

49. The DAT Act overcomes barriers to data sharing through an authorisation that overrides Commonwealth, State or Territory laws which would otherwise prohibit the sharing, collection and use of certain data, provided appropriate safeguards are in place. The DAT Act does not override the Privacy Act and the sharing, collection and use of data under the Act must be consistent with the Privacy Act.

50. Under the DAT Act, accredited users can request public sector data from Commonwealth data custodians for data sharing projects. An accredited data service provider (ADSP) can, and in some cases must, be used to provide data services to support data sharing projects.

51. To share data, entities must have a data sharing agreement in place which sets out the details of the data sharing project. A data sharing agreement must contain certain details, including a description of how entities will give effect to the data sharing principles and how the project serves the public interest. Data cannot be shared until the data sharing agreement has been registered.

52. There are three categories of participants in the DAT Act: data custodians, accredited users, and ADSPs (collectively called 'scheme entities').
    - Data custodians are Commonwealth entities that control data that can be shared.
    - Accredited users are Commonwealth, state and territory government bodies, and Australian universities, that are accredited to obtain and use Commonwealth data.
    - ADSPs are Commonwealth, state and territory government bodies, and Australian universities, that are accredited to provide one or a combination of data services including de-identification, secure access, and complex data integration.

53. Accreditation serves as a gateway to accessing data under the DAT Act and ensures users and ADSPs are capable of handling public sector data and minimising risk of unauthorised access or use. The Minister for Finance and the National Data Commissioner are the authorities for accrediting users and ADSPs and can impose conditions on accreditation if needed.

54. Commonwealth data can only be shared if it is for one of the three permitted purposes: government service delivery, informing government policies and programs, and research and development. Data cannot be shared for national security or enforcement-related purposes.

55. Government service delivery includes the provision of information (such as advice that the individual is eligible to receive a benefit), the provision of a service (such as assistance to a person to help restore their property after a flood), determining an eligibility for payment, or paying a payment.

56. The DAT Act is intended to work with the Privacy Act to protect personal information. It contains general privacy protections that minimise the sharing of personal information, prohibit the re-identification of data that has been de-identified, and prohibit the storage or access of personal information outside Australia. Express consent is always required to share biometric data. The DAT Act also contains purpose-specific privacy protections, depending on the data sharing purpose of the project.

57. Data custodians must consider and respond to all requests they receive from an accredited user within a reasonable period, but they have no obligation to share data and can refuse requests for any reason. If refusing a request, data custodians must provide their reasons in writing to the accredited user within 28 days after the refusal decision has been made.

Overview of data sharing projects

58. Data sharing projects must be consistent with five risk management principles (known as data sharing principles) set out in the DAT Act. These principles are otherwise known as the 'Five Safes' (Revised Explanatory Memorandum, DAT Bill 2022 (Revised EM)). The data sharing principles pose specific questions to help assess and describe each risk in a qualitative way and are designed to facilitate safe data release and prevent over-regulation. The five principles relate to:

    - project
    - people
    - setting
    - data
    - output.[21]

59. Participants must enter into a data sharing agreement which sets out the details of the data sharing project. A data sharing agreement must describe how the participants will give effect to the data sharing principles and how the project serves the public interest.

Regulatory machinery

60. The DAT Act establishes the National Data Commissioner as an independent statutory office holder responsible for overseeing the DAT Act. The National Data Commissioner is supported by the National Data Advisory Council.

61. The National Data Commissioner's responsibilities include accrediting eligible entities, handling complaints, providing education and support in relation to handling public sector data, and maintaining registers of accredited entities and data sharing agreements. The National Data Commissioner may only perform these functions in relation to data shared under the DAT Act.

62. The National Data Commissioner is also responsible for dealing with complaints from entities regulated by the DAT Act about other entities regulated by the Act, as well as complaints from any person or entity (including members of the public) about the administration and operation of the Act. The DAT Act confers a range of regulatory and

[21] For further information on the data sharing principles see 'Share Data' on the ONDC website: https://www.datacommissioner.gov.au/share-data.

investigative powers on the National Data Commissioner to support the management of complaints as well as general monitoring and assessment of the DAT Act. In the case of a privacy complaint, the National Data Commissioner may refer the complaint to the Office of the Australian Information Commissioner (OAIC).

63. The DAT Act also establishes the National Data Advisory Council. The Council comprises the National Data Commissioner, the Australian Statistician, the Australian Information Commissioner, Australia's Chief Scientist and at least 5 and no more than 8 other members appointed by the National Data Commissioner (ONDC 2025a). Its role is to:

> advise the National Data Commissioner on data sharing including on ethics, balancing data availability with privacy protection, trust and transparency, technical best practice, as well as industry and international developments.

Transparency

64. The National Data Commissioner must maintain public registers of accredited users, ADSPs, and data sharing agreements. The National Data Commissioner must also prepare and give to the Minister for Finance, for presentation to Parliament, an annual report on the operation of the Act each financial year. The annual report must include:
    - details of any legislative instruments made that financial year
    - the scope of data sharing activities and regulatory actions which have occurred, including reasons for agreeing to or refusing data sharing requests, and
    - staffing and financial resources made available to the National Data Commissioner and how they were used.

ONDC implementation

65. The DAT Act came into effect on 1 April 2022 and establishes the National Data Commissioner as the independent regulator of the DAT Act. The ONDC has approximately 40 permanent staff, which are provided by the Department of Finance to support the National Data Commissioner, with a budget of $16.653 million for 2024–25 and $14.425 million for 2025–26 (Department of Finance 2025a; Department of Finance 2025b).

Ministerial Statement of Expectations and Statement of Intent

66. The Minister of Finance, as the Minister with portfolio responsibility for the DAT Act, wrote to the National Data Commissioner in December 2022 to convey their expectations to progress activities under the following themes:
    - continuous improvement and building trust
    - maintain a risk-based framework and promote a regulatory approach that facilitates voluntary compliance
    - collaboration and engagement with stakeholders (ONDC 2022a).

67. As requested by the Minister, the National Data Commissioner provided a response (a Statement of Intent) that outlined how the National Data Commissioner will meet these expectations (ONDC 2022b).

ONDC's Annual Priorities

68. In line with the Statement of Intent, the ONDC publishes its Annual Priorities. For the 2025-26 financial year the ONDC's priorities are to:
    - facilitate data sharing
    - continue to build the trusted data community
    - promote adherence to DAT Act requirements
    - educate and guide on best practice (ONDC 2025b).

Establishing accreditation

69. Part 5.2 of the DAT Act establishes the accreditation framework. From 1 June 2022, Commonwealth, state and territory government entities could apply for user accreditation, with Australian universities able to apply from 1 August 2022. All eligible entities could apply for accreditation as an ADSP from 1 August 2022.[22]

70. The framework for accrediting data service providers was established by an ONDC-led working group of expert advisors from the ABS, the AIHW, and the Australian Cyber Security Centre (ACSC). The working group considered the requirements of accreditation for integrating authorities in conjunction with security and privacy expectations.

71. ONDC developed standard operating procedures to assess applications and service level standards: two and three months for accreditation as a data user and data service provider, respectively. ONDC has consistently met these service level standards since they took effect from October 2023.

72. As of 30 September 2025, 40 entities are accredited to participate in the DAT Act (17 Commonwealth Government entities, 11 State and Territory government entities, and 12 universities) as a user or ADSP.

73. ONDC initiated two independent reviews of the accreditation framework, both completed in late 2024. Both reviews found that the accreditation framework is sound.

Legislation, advice, guidance and education

74. Following the commencement of the DAT Act, legislative instruments were developed to support its operation.

75. The Data Availability and Transparency Regulations 2022 prescribe specific data, data custodians, or circumstances when data sharing is barred under the DAT Act. They commenced in April 2022.

76. A Ministerial Rule with effect from September 2022, transitioned six Accredited Integrating Authorities (AIAs) – the ABS, the Australian Institute of Family Studies (AIFS), the AIHW, the Department of Social Services, Queensland Treasury and the Department of Health, Victoria – to be ADSPs. An additional entity, Queensland Health, was transitioned in November 2023 (Data Availability and Transparency (Consequential Amendments) Transitional Rules 2022).

---

[22] Submission 38, National Data Commissioner.

77. The National Data Commissioner made two data codes which commenced in December 2022:
    - the DAT Code to guide participants on applying the data sharing principles, including the public interest test and approaches to consent, privacy and ethics
    - the Data Availability and Transparency (National Security Measures) Code 2022 sets out additional measures to manage national security risks that may arise if foreign individuals, working within an accredited entity, are provided access to shared data.
78. In June 2025, the National Data Commissioner amended the DAT Code to include requirements for data sharing agreements to explicitly recognise the rights of states and territories over data for which they are custodians.
79. The National Data Commissioner's functions include providing advice to DAT Act participants on how the DAT Act applies in specific circumstances. Guidance notes are available on the ONDC's website to support DAT Act participants to share data safely. Topics include the role of an authorised officer, making and responding to data sharing requests, making and registering data sharing agreements, charging fees, data breach responsibilities, and reporting requirements under the DAT Act.

Regulatory approach

80. ONDC's early focus was on developing standard operating procedures to carry out the core regulatory functions including for accrediting eligible entities and handling complaints from DAT Act entities and others. Other early priorities were:
    - building ONDC and DAT Act participants' capability to minimise the risk of, and mitigate the harm from, a data breach, and
    - supporting DAT Act participants to meet their reporting obligations. Reporting obligations include the requirement for accredited entities to report events and changes in circumstances and for data custodians to report annually to the National Data Commissioner on data sharing requests, data sharing agreements and complaints.
81. As of 30 September 2025, ONDC has handled 22 complaints. The complaint function is a redress mechanism, and a means for the National Data Commissioner to identify potential cases of non-compliance and areas to improve or support implementation of the DAT Act. No complaints have been received in relation to sharing data under the DAT Act. However, there were six complaints regarding the operation or administration of the DAT Act. These included complaints about ONDC's responsiveness and about an entity being ineligible to become accredited and request data under the DAT Act. There were also 16 complaints unrelated to the DAT Act. These included complaints about the handling of data by a private sector organisation and about the fraudulent use of private information. These were referred to other regulators including the Australian Information Commissioner.

Feedback and advice

82. ONDC has taken several measures to seek and respond to feedback from DAT Act participants:

- In May 2024, a DAT Act working group was established to identify both the key issues that have impeded uptake of the DAT Act and potential solutions. The group presented its findings in November 2024 and recommended 22 actions (including 11 priority actions). As of 6 August 2025, ONDC reported that it had completed 7 of the priority actions (ONDC DATA Scheme Working Group update).
- In June 2024 the ONDC hosted its inaugural annual forum for DAT Act participants. The Forum provided participants with an opportunity to discuss the operation of the DAT Act. There were 24 entities from Commonwealth government agencies, State and Territory government agencies, and Australian universities in attendance.[23]
- In November 2024, the ONDC commissioned a series of executive interviews to gather feedback on its performance as a regulator. A sample of 26 executive leaders from 23 organisations participated. Many participants viewed the ONDC as playing an important leadership role in supporting data sharing. Participants were positive about ONDC's facilitative posture and universities remained optimistic about accessing data for research. Australian Government agencies that identified as less data mature highly valued the learnings from the DAT Act's accreditation process.[24]

[23] Submission 38, National Data Commissioner.
[24] Submission 38, National Data Commissioner.

Effectiveness of the DAT Act and Commonwealth data sharing

DAT Act objectives

Finding 1

The DAT Act has not achieved its objectives.

83. The DAT Act was introduced to overcome barriers to sharing Commonwealth data. It was envisaged the DAT Act would deliver substantial economic and social benefits through greater Commonwealth data availability and use, including supporting economic and research opportunities, and enabling streamlined and efficient service delivery (Productivity Commission 2017).

84. However, the DAT Act has not yet driven material additional sharing of Commonwealth data. This is unlikely to improve without significant changes to the DAT Act. Despite other pathways becoming more mature, there are still significant use cases where the sharing of data would provide benefits to Australia and these are not being exploited (Box 1 provides an example of such an instance).

Box 1: **GenV project**[25]

The GenV project led by the Murdoch Children's Research Institute (MCRI) is a longitudinal research initiative which currently tracks nearly 125,000 Victorian children born between 2021 and 2023 and their parents to improve health and wellbeing outcomes across Victoria. MCRI collects extensive data and biosamples to explore links between genetics, environment, and health, enabling faster, more inclusive research into conditions such as mental illness, obesity, allergies, and developmental challenges. GenV research cover topics such as congenital cytomegalovirus testing to reduce lifelong hearing and neurodevelopment impairment, and the role of medication use in pregnancy and lactation in later-life asthma of mothers and children.

GenV has obtained consent from nearly 125,000 Victorians to link their data, including explicit permission to access Medicare records and identifiers. Despite this consent there remains significant uncertainty about whether GenV will ultimately be granted access to the data. As MCRI is a medical research institute it is ineligible to obtain data under the DATA Scheme and consequently it must navigate existing Commonwealth data access systems, which are tailored for smaller, one-off research projects and do not guarantee access. MCRI is required to engage individually with data custodians through lengthy approval processes, often taking around six months per application resulting in significant administrative burden and delays.

Also, the current structure requires that data sit in multiple secure environments rather than being brought together in one place. This fragmentation prevents the consolidation of datasets, increasing costs, limiting the reuse of data assets and delaying the impact of the research.

[25] Submission 4, AAMRI.

85. To promote greater sharing of Commonwealth data that delivers value for individuals and society, the DAT Act aims to establish robust safeguards that protect privacy and data security, while also enhancing integrity and transparency to build public trust.

86. As previously mentioned, the first 3 years of the DAT Act has seen the ONDC[26] implement the accreditation framework, make legislative instruments to support the operation of the DAT Act, publish guidance to support DAT Act participants, and adopt an explicitly facilitative posture to support data sharing under the DAT Act.

87. Fundamental flaws with the DAT Act have prevented it from driving additional sharing of public sector data. The DAT Act's limited uptake is the result of issues with its design, many of which reflect or are symptomatic of broader challenges in Commonwealth data sharing. Consequently, the economic gains and social benefits envisaged by the PC Inquiry and the Government have not materialised.

88. The following issues are emblematic of the limitations that have been raised with the Review. These issues are also covered in further detail in later sections.

Inability to access data

89. Being an accredited DAT Act data user does not guarantee access to data, as data custodians can refuse requests for any reason (section 25). Further, where a dataset has multiple custodians, access to a data requestor can only be granted if all data custodians agree, meaning each data custodian effectively has a veto right over requests.

90. Although 8 data sharing agreements have been registered under the DAT Act, all have been between Australian Government entities for the purposes of building the NDDA. To date, no other requests for data under the DAT Act have been agreed to.

91. Further, the Commonwealth agencies involved in the NDDA project have reported that the DAT Act will no longer be used to support the NDDA in the future, due to difficulties with using the DAT Act. While some issues likely relate to the inherently challenging scope of the NDDA project itself, others are attributable to the complexity and design of the DAT Act.[27]

DAT Act is complex and prescriptive

92. The DAT Act is complex and prescriptive which creates a high barrier to its use. Stakeholders report that the DAT Act is difficult to interpret, relies on administratively burdensome processes, and does not sufficiently recognise existing institutional governance frameworks and other legislation.[28]

---

[26] Submission 38, National Data Commissioner.

[27] Submission 9, ABS; Submission 18, Department of Health, Disability and Ageing; Submission 21, Department of Social Services; Submission 53, Services Australia.

[28] Submission 1, ACT Government; Department of Health; Submission 18, Disability and Ageing; Submission 60, University of Sydney.

Intended role of the DAT Act is unclear

93. Some stakeholders firmly believe the DAT Act should only be used as an authorising pathway of 'last resort'. The ABS in its submission highlighted this point: [29]

> In its current form, the DAT Act is predominantly useful for supporting a narrow range of data sharing, particularly the sharing of a Commonwealth dataset with an Accredited User, where this sharing requires an override of secrecy provisions.

94. However, others view the DAT Act as potentially providing the comprehensive system for all Commonwealth data sharing within its scope.[30] This view is supported by its expansive objects and the legislated role of the National Data Commissioner.

95. The lack of a clear purpose for the DAT Act's existence has led to confusion between data requestors and data custodians. Data requestors are more likely to use the DAT Act to request all data, which can be more efficient for them when they otherwise need to navigate multiple systems. Whereas data custodians with established systems are more likely to view the DAT Act as a pathway of last resort and direct data requestors to their own established pathways. For data requestors, this may result in delays and frustration if the data is provided through a different framework. For example, Monash University states: [31]

> After three months of waiting time on a few requests via the Scheme, the researchers have been asked to reapply with the agency, that is, start over again adding an additional three month delay to an already lengthy process.

96. Some data custodians with established enabling legislation and processes see limited need for the DAT Act and find it easier and simpler to use their established frameworks. For example:

- AIHW already has enabling legislation and a well-established approach to receiving and sharing data and see limited need for the DAT Act to facilitate their data sharing functions.[32]
- Department of Health, Disability and Ageing states that established data sharing mechanisms, developed over decades, continue to be more efficient than the newer, more complex DAT Act.[33]
- Services Australia holds personal, sensitive, and protected information on almost every Australian. In some circumstances, due to the complexity of legal, ethical, and consent considerations and accreditation processes, Public Interest Certificates are used to facilitate data sharing instead of the DAT Act.[34]

97. There are clear incentives for data custodians to continue to use established and bespoke data sharing arrangements. However, the lack of consistency between processes imposes costs on data requestors, including uncertainty on data access, the scope of access, and procedures to escalate requests with specific data custodians.

---

[29] Submission 9, ABS, page 3.
[30] Submission 36, Monash University.
[31] Submission 36, Monash University, page 3.
[32] Submission 12, AIHW.
[33] Submission 18, Department of Health, Disability and Ageing.
[34] Submission 53, Services Australia.

Inconsistent requirements

98. The discretion available to data custodians when considering requests under (and outside of) the DAT Act has meant that requestors of public sector data continue to experience inconsistent practices. This is despite the objects of the DAT Act being to enable consistent and robust institutional arrangements for data sharing.

99. Monash University highlights that Australian Government entities refused to use the university's secure environment (accredited by ONDC) and were instead directed to use a different Trusted Research Environment (TRE).[35] There are several TREs (such as the ABS DataLab) with the particular TRE used being at the discretion of the data custodian when establishing a data sharing agreement. Requiring researchers to use multiple TREs for separate instances of data sharing has significant cost impacts and is administratively burdensome.[36] Furthermore, the duplication of data held among TREs, for the purposes of making data access more efficient for requestors comes with the increased risk of, for example, data breaches.

100. Although the accreditation process assesses an equivalent level of capability for all entities, data custodians are perceived as treating non-Commonwealth ADSPs differently from their Commonwealth counterparts. Additionally, some data custodians have required separate security assessments, despite such settings being comprehensively assessed through the accreditation process.[37] For example, the University of Melbourne advised: [38]

> This issue is further amplified when data custodians operate their processes outside of the DATA Scheme. Without the standardised frameworks and safeguards provided by the Scheme, the lack of trust and transparency is exacerbated, leading to even greater inconsistency, inefficiency, and delays in data access. Researchers are left navigating a fragmented and unpredictable system, which directly undermines the goals of the DATA Scheme and the DAT Act.

101. The Review finds that Commonwealth data custodians frequently decline data requests, including those for de-identified datasets, without providing clear justification or engaging with the requesting party. Although the DAT Act requires data custodians to notify accredited users of refusal reasons, the explanation need not be informative, and users have no right of redress.[39] This has led to inconsistent outcomes and uncertainty for accredited users.

102. The DAT Act does not impose a timeframe for responding to data requests.[40] The lack of an enforceable deadline may contribute to lengthy delays in data requestors receiving or being denied data. For example, while the average time taken to assess data requests under the DAT Act is 39 days (as of May 2025), two Australian Government entities have taken an average of 79 and 111 days.[41] Further, the

---

[35] A TRE is a secure, controlled computing environment that allows authorised people to safely access, store and analyse sensitive data.
[36] Submission 36, Monash University.
[37] Submission 55, South Australian Department for Health and Wellbeing.
[38] Submission 58, University of Melbourne, page 8.
[39] Submission 58, University of Melbourne.
[40] While there are no specific legislative timeframes for considering a request, Section 25 of the DAT Act requires the data custodian to consider the request within a reasonable period. However, what is considered 'reasonable' is not defined.
[41] Internal ONDC document.

Universities Australia submission states '[d]ata sharing requests can take up to two years to process, which significantly delays time-sensitive research and policy projects.[42]

Commonwealth data processes

Finding 2

Commonwealth data processes continue to impede data sharing.

103. Since the PC Inquiry, the broader environment supporting data availability and use has improved substantially. This is due to both increased use of existing legislation outside the DAT Act (for example, in the continued improvement of enduring assets like BLADE, PLIDA and the NHDH), and greater commitments to share and make non-sensitive data open by default (for example, through the IGA and the Data and Digital Government Strategy (Digital Transformation Agency, Data and Digital Government Strategy).

104. While there have been improvements in Commonwealth data sharing using other (non-DAT Act) mechanisms, challenges persist.

Limited visibility of data

105. Despite improvements, there is limited visibility of data being shared, and data requestors continue to face challenges sourcing data held across Australian Government entities. For example, there is no central register of data sharing arrangements and Australian Government entities use a range of IT systems to track and administer their sharing to various degrees, including informal or ad hoc systems such as Microsoft Excel or Word. This creates difficulties in identifying what data is available, and how it can be accessed.

106. Most Australian Government entities have limited visibility of their own data holdings. Although the ONDC created Dataplace with the ability to manage any type of data sharing request (including ones made outside of the DAT Act), its use to-date has been limited. Since the launch of Dataplace in June 2022, only 62 data requests have been made (as of 30 September 2025). Of these, 37 were made by accredited entities under the DAT Act, while the other 25 requests were general requests (those that use another legal pathway to authorise data sharing, as well as those made by entities not eligible to participate in the DAT Act).[43]

107. Data discovery and the quality of metadata across the Commonwealth also lacks maturity with agencies and prospective requestors deploying significant resources to navigate, assess, and curate individual data sharing requests on an ad-hoc basis.

108. The 2024 Australian Public Service Data Maturity Report (Data Maturity Report) presents findings from the Australian Public Service Data Maturity Assessment

[42] Submission 56, Universities Australia, page 2.
[43] Submission 38, National Data Commissioner.

(Department of Finance 2024).[44] Of note, the maturity of Australian Government entities Data Quality, Reference and Metadata standards was rated (averaged over entities) as the lowest scoring indicator with an 'Initial/Ad hoc' rating. This rating reflects an entity's ability to manage and utilise data assets including the standards and processes in place to measure and monitor data quality standards, manage data assets and sources, and ensure metadata quality, consistency, currency, and security.

Incentives to share

109. There continues to be substantial caution, and at times a reluctance on the part of data custodians, to share data. This reluctance may be due to an increase in risk aversion and a lack of resourcing in place to support data sharing.

110. Risk aversion is more heightened now than at the time of the PC Inquiry due to the occurrence of large-scale data breaches and the release of findings from Royal Commissions such as the Royal Commission into the Robodebt Scheme. The significant costs and complexity associated with establishing the legality of what can be shared can result in data custodians simply choosing not to share. These issues impact all prospective users of data, Commonwealth, state and territory agencies and the research sector.

111. Risk aversion in data sharing is often intensified by the imbalance between the risks and rewards involved. While the benefits typically accrue to the data requestor and the broader public, data custodians are left to shoulder both the resource burden of sharing and the potential fallout if issues arise. This asymmetry in risk and return creates weak incentives for data custodians to engage in data sharing.

112. The benefits of data sharing will only be realised if this incentive and resource problem is addressed. Competing priorities for Australian Government entities limit the resources allocated to support the consideration of data sharing requests, with data sharing by agencies often viewed as either 'risky' or secondary to their core priorities.

Little consistency in processes

113. Data requestors are experiencing greater costs, inconsistency, inefficiency, and delays in data access as Australian Government entities processes and expectations of data sharing bona fides and systems not only differ from the DAT Act but also between Australian Government entities.

114. Although the ongoing preference of data custodians to utilise existing agency-specific processes is generally understandable at an agency level, it is inefficient at a whole-of-government level. It has prevented greater systemic efficiency which imposes additional costs on accredited users.

115. Outside the DAT Act, data requestors generally have no or limited redress when requests are rejected or are not responded to in a timely manner. Data custodians generally have no obligation to provide reasons for refusals or to decide requests within defined timeframes. The costs, delays and limitations that exist in the range of alternative

[44] The Australian Public Service Data Maturity Assessment aims to consistently measure and track Australian Public Service data maturity. All Australian Government agencies except national intelligence agencies can be assessed.

data sharing arrangements limit the ability for governments and researchers to access and use data in a timely manner to improve service delivery and public policy. While these costs are not borne by data custodians, the delays and poorer service that results is a real cost to government and to the broader public.

DAT Act role

Finding 3

There is a role for the DAT Act, but substantial modifications are required.

116. While non-DAT Act data sharing has improved since the PC Inquiry, there remains significant obstacles that the DAT Act can assist in overcoming. In particular, there is utility for the existence of a generally available authorising pathway, consistent processes and expectations for requestors and data custodians, and an accreditation framework.

117. Engagements and submissions from stakeholders (including data custodians that have their own preferred data sharing mechanisms) have demonstrated almost universal support for the objects of the DAT Act and its continuation, albeit with substantial amendments due to issues with its complexity and prescriptive approach. For example, the ABS submission states:[45]

> It is possible that the DAT Act may hold the potential to contribute meaningfully to Australia's data sharing landscape. However, achieving its original vision will require substantial reform. The legislative framework underpinning the DATA Scheme needs to evolve to meet the needs of a modern, collaborative data ecosystem.

118. There is also demand for the expansion of accreditation eligibility to include, for example, not-for-profit research institutes,[46] First Nations community-controlled organisations,[47] and the private sector[48]. The proposed expansion of accreditation eligibility identifies an unmet demand for public sector data and highlights the potential for improved outcomes through broadened access.

119. For example, the Association of Australian Medical Research Institutes (AAMRI) submission advises that medical research institutes contribute to the development of government policies and programs by advancing more effective and efficient treatments, fostering economic growth, and enhancing quality of life. Enabling medical research institutes to become accredited and request access to data under the DAT Act would remove much of the repetition and burden of existing processes.[49]

120. Stakeholders have expressed broad support for greater transparency and consistency in data sharing practices including for the development of standardised

[45] Submission 9, ABS, page 5.
[46] Submission 5, AAMRI; Submission 51 Research Australia; Submission 54, Social Research Centre.
[47] Submission 52, Seer Data and Analytics, Greater Shepparton Lighthouse Project and Maranguka Community Hub.
[48] Submission 47, Prospection; Submission 48, Psithur.
[49] Submission 5, AAMRI.

protocols and dispute resolution mechanisms which address inconsistent practices and improve trust between data users and data custodians.[50]

121. There is broad support for the accreditation process as an assurance mechanism, and for its role in uplifting the data maturity of entities seeking accreditation. Stakeholder feedback from both data users[51] and data custodians[52] mentions that DAT Act accreditation has uplifted organisational data governance and maturity, and streamlined data sharing by providing assurance to data custodians that data users can safely manage and share data.[53]

Reforming the DAT Act

122. The ongoing limitations and obstacles inhibiting access to public sector data are more likely to be overcome by substantially reforming the DAT Act than by allowing it to sunset. These reforms are necessary to justify the Act's continued operation and should be directed towards developing a simpler and more flexible DAT Act which provides a clear authorising pathway for sharing data for approved purposes. If this objective cannot be achieved, then the DAT Act should be allowed to sunset. However, it should be noted that simply allowing the DAT Act to sunset will not remove the underlying problems that the DAT Act was designed to address.

123. To be effective, the authorising pathway in the DAT Act should complement other pathways for data sharing (including where there is no safe, secure pathway) and be simple enough so that it can be used as a viable alternative to existing pathways, where appropriate. This means that the DAT Act pathway should both enable safe, secure and timely data sharing, and be clear and simple.

124. While other frameworks may be capable of securing additional data sharing and improvements to practices at an individual agency level, none of these operate at a system level.

Recommendation 1

The DAT Act should not sunset, subject to it being amended to provide a clear authorising pathway that enables greater and better sharing of Commonwealth data for approved purposes.

125. The DAT Act pathway is still required. It should be utilised to authorise sharing when no other pathway exists, and where the DAT Act provides a more efficient pathway compared to other options. The DAT Act should also be capable of operating alongside other data sharing pathways. If an alternative pathway achieves the desired outcomes for both the data user and data custodian there is no need for the DAT Act to be utilised.

---

[50] Submission 36, Monash University; Submission 55, South Australian Department of Health and Wellbeing; Submission 58, University of Melbourne.
[51] Submission 30 James Cook University; Submission 61, University of Tasmania.
[52] Submission 18, Department of Health, Disability and Ageing; Submission 37, National Archives of Australia.
[53] Submission 17, Department of Employment and Workplace Relations; Submission 20, Department of Industry, Science and Resources.

126. Substantial amendments to the DAT Act and non-legislative process changes are needed to encourage more data sharing. These changes should encourage more data sharing than would otherwise occur if the DAT Act did not exist.

127. While participants will continue to determine which authorising pathway is the most appropriate to meet their needs, the amendments recommended by the Review would improve the utility of the DAT Act to ensure it can provide an efficient, unambiguous, consistent and safe framework. This will enable the DAT Act to be used where:

- there is uncertainty about whether an entity is authorised to share the data under another framework, or
- the DAT Act is simpler and/or safer to use than another framework, or a combination of frameworks.

128. While the DAT Act is intended to complement existing sharing arrangements, it is envisaged that, over time, it could be the preferred option where it can drive greater system benefits (e.g. greater consistency, simpler and/or safer).

129. Amending the DAT Act would maintain existing momentum, provide a degree of certainty about the existing framework, and would be more efficient than sunsetting the DAT Act and starting again. However, if an amended DAT Act cannot provide an efficient, unambiguous, consistent and safe framework that increases data sharing then it should be allowed to sunset.

Settings and regulatory function

Legislative complexity and inflexibility in a voluntary framework

Finding 4

The DAT Act's authorisation framework is difficult to use because it is too complex, including because it is overly prescriptive, and inflexible. Being both difficult to use, and entirely voluntary for data custodians, uptake of the DAT Act for public sector data sharing has been very limited.

130. The Review received consistent feedback that the DAT Act is difficult and costly to use, that data custodians prefer to use their own authorising frameworks, and that prospective users face significant challenges requesting data under the DAT Act.

131. The Review has found that the DAT Act's authorisation framework is difficult to use because it is too complex, including because it is overly prescriptive, and inflexible. Being both difficult to use, and entirely voluntary for data custodians, uptake of the DAT Act for public sector data sharing has been very limited.

132. Though the complexity and inflexibility of the DAT Act are not the only reasons for limited uptake, they have been counterproductive to overcoming some of the barriers to data sharing which the DAT Act was intended to address (e.g. low data maturity, cultural factors, and lack of incentives to share data). Compounding the effect of these barriers is the fact sharing data under the DAT Act is entirely discretionary for data custodians, and there are few constraints or requirements on decisions to refuse data sharing requests. These features also do not overcome the cultural risk aversion to share data.

Legislative complexity

What is legislative complexity and why does it matter?

133. Legislation is complex when it is difficult to understand (Burton Crawford et al. 2022; Australian Law Reform Council (ALRC) 2021). Recognising that complexity is not completely avoidable in legislation, the key question is whether legislation is more complex than it needs to be to achieve its purpose (ALRC 2021).

134. Legislative complexity is not unique to the DAT Act, nor is it new. There have been significant efforts to understand and address legislative complexity in Commonwealth laws. For example, the ALRC has undertaken in-depth analysis of legislative complexity in the context of corporations and financial services regulation (ALRC 2023),[54] and the Tax Law Improvement Project, established in 1993, was a three-year programme to

[54] See also the ALRC's DataHub resource on Measuring Legislative Complexity: https://www.alrc.gov.au/datahub/legislative-complexity-and-law-design/measuring-legislative-complexity/.

reduce the complexity of income tax law (Nolan and Reid 1994). This report has drawn on such work to test and analyse the assertion that the DAT Act is prohibitively complex.

135. Legislative complexity is problematic when it results in increased costs for regulated entities to understand their obligations. It makes compliance and enforcement difficult for regulated entities and regulators. The uncertainty created by legislative complexity and the difficulty participants face in ensuring compliance can have a 'chilling effect' (ALRC 2021:8). This 'chilling effect' is evident in the submissions of some data custodians with respect to willingness to use the DAT Act.[55]

136. Legislative complexity is also cited as a barrier to sharing public sector data more generally, including in the initial PC Inquiry and in other jurisdictions, such as the UK (PA Consulting et al. 2025; OSR 2023; Lievesley 2023; OSR 2024).[56]

137. Legislative complexity is particularly problematic for the DAT Act because its use is voluntary for data custodians, many of whom can rely on other legislative frameworks to facilitate data sharing. The Review heard from many entities that had invested significant resources to understand and use the DAT Act but ultimately concluded either that the DAT Act could not authorise certain activities, or that using the DAT Act would be too difficult or costly relative to other pathways. This has occurred even where the activities, particularly for the purposes of service delivery or for a Commonwealth body's use of its own data, were clearly intended to be enabled by the DAT Act.

138. The Office of Parliamentary Council (OPC) notes that the complexity of particular legislation should be considered 'by reference to the standards of the intended audience' (OPC 2016). The perception of the entities eligible to use the DAT Act's framework are therefore highly salient for judging the degree of complexity in the DAT Act. It is not unreasonable for some initial costs to be incurred by participants to understand a new legislative framework when it is first established. However, given that the DAT Act was introduced in part to overcome the barriers caused by legislative complexity to improve the sharing of government data (PC Inquiry 2017), the degree to which stakeholders view the complexity of the DAT Act as an additional barrier to data sharing is both significant and highly detrimental to its efficacy.

Examples of legislative complexity in the DAT Act

139. Many of the common drivers and measures of legislative complexity feature in the DAT Act's authorising framework.

140. Drivers of complexity are factors external to legislation that can impact on the degree of complexity in the legislation (ALRC 2021). These drivers include complexity of the field being regulated and the underlying policy, stakeholder demands, and legislative design preferences (ALRC 2021; OPC 2016; AGD 2014).

141. The complexity of the data ecosystem and the range of stakeholders will be relevant for any data sharing legislation, and so a revised DAT Act is unlikely to be 'simple'. However, it is possible to reduce the measures of complexity in the legislation itself. This

[55] See for example, Submission 9, ABS; Submission 12, AIHW; and Submission 21, Department of Social Services.

[56] It should be noted that the Independent Review of the UK Statistics Authority by Professor Denise Lievesly (2023:39) took the view that the relevant legislative framework was actually 'enabling', even though it is often 'cited as an excuse for not sharing'.

section summarises the most significant examples. Further detail about the legislative complexity of the DAT Act is included in Appendix D.

142. The DAT Act is long relative to other legislative frameworks that data custodians use to share public sector data. This covers both the comparative length of the DAT Act in absolute terms, as well as the length of the key provisions relevant to the DAT Act's authorising framework. The length of these provisions results in a significant volume of detail that participants are required to digest and understand, to know what is required for sharing to be authorised.

143. There is excessive prescription in the DAT Act's authorising framework. In particular, the number of requirements for data sharing agreements is commonly raised by stakeholders as complex and burdensome (ONDC 2024).[57] There is a total of just under 70 requirements for data sharing agreements set out in the DAT Act and the two data codes. Many core obligations in the DAT Act are given effect through data sharing agreements, rather than through operation of the DAT Act alone. Many requirements are conditional, and so only apply when a data sharing project has certain features (for example, when the project involves personal information). Additionally, participants must understand concepts and obligations in other parts of the DAT Act to know whether a particular requirement applies.

144. Data sharing agreements are one of a significant number of requirements for the sharing, collection and use of data to be authorised under the DAT Act. There are also more requirements for data custodians (or 'sharers' of data) than for other types of entities (section 13 cf. sections 13A and 13B).

145. Other significant structural legislative features contributing to the DAT Act's complexity include its interdependency with other legislation – in particular with the Privacy Act – and the number of conditional statements and cross references. Detailed analysis of these features is included at Appendix D.

146. The combination of structural complexity and excessive prescription in the DAT Act is a clear and significant barrier to the degree of difficulty data custodians face when considering whether to use the DAT Act. These issues are compounded by the fact that the complexity and degree of prescription has resulted in a common and legitimate view that the DAT Act is an inflexible framework.

Inflexibility

147. In addition to creating inhibitive complexity, the degree of prescription and specificity in the DAT Act has limited the flexibility of its authorising framework. It can therefore be difficult for participants to work out how or whether a particular data sharing activity can be authorised by, and undertaken consistently with, the DAT Act. This is particularly significant in an evolving system. This has contributed to the view that the DAT Act's requirements are too burdensome or that the bar of assurance which participants must clear is disproportionately high in cases other than those which are the most high-risk.

[57] Submission 1, ACT Government; Submission 9, ABS; Submission 12, AIHW; Submission 13, Australian Research Data Commons; Submission 21, Department of Social Services.

148. Numerous stakeholders have highlighted the problem with the DAT Act's limiting conception of the data sharing 'project'.[58] Specifically, there is a perception that the DAT Act can only authorise simple, defined instances of a data custodian sharing, on a one-off basis, very specific data with a user for very restricted purposes, and that each instance must be authorised separately. It is not readily apparent how or whether the DAT Act can authorise 'multi-way' or 'two-way' data sharing. This is particularly significant with respect to state and/or territory data (see further at Finding 10 below).[59]

149. As the DAT Act appears to authorise only (or at least most clearly) simple data sharing projects, the protections in the DAT Act may appear to be disproportionate and unreasonably burdensome. This may be largely because of the degree of prescription and complexity in the legislation, but there are instances in the DAT Act where the protections appear to be disproportionate.

150. Further detail and analysis with respect to the inflexibility of the DAT Act's authorising framework and the disproportionate burden of the DAT Act's requirements is included in Appendix D.

Unfettered discretion and lack of parameters in responding to data sharing requests

151. Data sharing decisions by data custodians under non-DAT Act frameworks are generally not subject to the requirements which usually apply to government decision-making, or to any review process. This is because data is usually shared under a defined exception to a secrecy provision (which is frequently tied to an offence or civil penalty provision), rather than under a legislated discretionary decision-making power granted to an official.[60] The DAT Act framework, by contrast, is an express decision-making power granted to data custodians about whether to share data.[61]

152. The DAT Act makes clear that data custodians' discretion is absolute: data custodians cannot be required to share data and can refuse a data sharing request 'for any reason' (section 25). While data custodians are required to consider requests 'within a reasonable period' and are required to give written reasons for refusal, data sharing decisions are not reviewable. Though there is a complaints mechanism that could cover requests made under the DAT Act, the scope of regulatory oversight of decision-making by custodians is extremely limited.

153. This is problematic and frustrating for entities who have invested significant resources in obtaining accreditation – especially those accredited as both ADSPs and users of data. Not only are these entities unable to confidently predict that data will be shared with them, they may be refused for reasons that are contestable, or refused due to concerns that could be (or have been) substantially mitigated, or without meaningful dialogue or negotiations with the requestor. This also frustrates a core objective of the

[58] E.g. Submission 9, ABS; Submission 38, National Data Commissioner.
[59] Submission 1, ACT Government.
[60] The ALRC noted in a report published in 2010 that '[a]pproximately 65 per cent of secrecy provisions contain an exception to permit the disclosure of information in the performance of a person's functions and duties or for the purposes of particular legislation' (ALRC 2010b:10.49). At paragraph 10.37 of report, the ALRC notes the 'tension inherent in using a prohibition on the disclosure of information to authorise the disclosure of that information in some circumstances'.
[61] Though the DAT Act does not require decisions to agree to or refuse a request to be made by the authorised officer of the relevant entity.

DAT Act, which is to authorise the disclosure of data where it would serve the public interest.

154. While requesting entities could make a complaint under the DAT Act (sections 88 and 94), the scope of data custodians' discretion is so broad that refusal is unlikely to amount to an actual breach of the DAT Act, other than where no reasons are provided. There is therefore no reliable avenue for requestors to seek redress for, or review of, refusals. While the DAT Act does currently recognise external dispute resolution or conciliation as a possible resolution pathway (e.g. paragraphs 91(b) and 95(d)), this would require a commitment of further resources from accredited entities with no guarantee of a favourable outcome. This lack of certainty and predictability is particularly problematic where funding for research or policy development is time-limited and/or contingent on the ability to access specific data. The Review has also heard from key stakeholders that there is similarly no transparency, consistency of practice or predictability where requests are made for data under non-DAT frameworks.

Recommendation 2

The DAT Act's authorising framework should be amended to take a principles-based approach to ensure clarity and flexibility.

155. The Review considers that a principles-based approach to the DAT Act's authorising framework would substantially address its issues of complexity and inflexibility, and promote a more useable and clear authorising pathway for data sharing that can accommodate the widest possible variety of data sharing activities.

156. A principles-based approach to legislation (or regulation) – also referred to as the 'coherent principles approach' (Pinder 2005) or 'coherent principles drafting' (OPC 2016:3) – is a statement or articulation of the desired or intended outcome in a particular area (ALRC 2010a). This is contrasted with a rules-based approach, which sets out detailed steps that must be followed in order to satisfy obligations.

157. As Pinder (2005:77) notes (emphasis in original):

> …a principle is not just a less specific rule; it is a statement about the essence of all outcomes intended within its general field. When a principle works, it does so because the essence it captures appeals to readers at other than an abstract intellectual level; it *means* something to readers because it relates to their understanding of the real world.

158. A principles-based approach is most effective when the principles work together (i.e. coherently), and when applied as an approach to designing rather than simply drafting legislation (see Figure 1) (Pinder 2005: 80).

Figure 1: Hierarchy of steps in principles-based legislative design

Policy outcome	Policy
Policy means	
Legislative purpose	Law
Coherent principle/s	
Lower level detail (unfolding)	
Interpretation/systems	Admin

159. A principles-based approach can reduce complexity by avoiding setting out detailed steps which must be complied with to achieve a desired outcome. It also affords greater flexibility and is better able to accommodate changes in technology and a wider variety of activities than highly prescribed rules, which is particularly relevant in fields such as data sharing, which are highly impacted by technological developments.

160. Some stakeholders may consider a principles-based approach to legislation to be unclear because it lacks detail and concrete standards, and will not provide certainty to data custodians about how to share data safely.[62] This concern is not uncommon with respect to principles-based approaches in legislation generally (see e.g. ALRC 2021; ALRC 2010a), and accords with the experience of drafting the original Bill, which was intended to be principles-based.[63] If this recommendation is accepted and implemented, stakeholders are very likely to request particular circumstances or requirements be addressed or prescribed in specific detail. However, consistent with the analysis above, greater specificity and prescription is more likely to obscure the core outcome being sought by the relevant principle and make that outcome harder to achieve. It is not possible for legislation to cover every possible scenario, and in attempting to prescribe requirements for any number of specific cases, the clarity of the relevant principle is likely to be undermined (Pinder 2005).

161. An example of this in the submissions that the Review received is a suggestion to more precisely define the 'public interest' test under the project principle (Submission 23). Further clarity regarding how a project's or activity's outcome should be assessed in relation to the public interest is likely to be helpful to participants. However, this is unlikely to be successfully achieved by prescribing additional requirements about data sharing to be in the public interest (or not in the public interest). It is highly likely that some proposed activity will not neatly fit into the legislated list, but which may nevertheless be in the public interest.

162. To the greatest extent possible, detail addressing specific activities and requirements should be elaborated in subordinate legislation or administrative guidance. The legislation should therefore include clear powers to make subordinate instruments to enable further detail to be developed where necessary. Adequate explanations and examples of the relevant principles should be provided in the explanatory memorandum that accompanies any amending legislation.

[62] Submission 10, Australian Computer Society.
[63] Submission 70, Dr Phillip Gould.

163. To avoid highly prescriptive rules and complexity being moved from primary to subordinate legislation, there should be a focus on producing instruments that are as practical as possible. For example, the DAT Code, which includes additional considerations and procedural detail for applying the data sharing principles, is set out quite formally, resembling a 'black letter law'-type instrument. By comparison, the Data Sharing Code of Practice made by the UK's Information Commissioner is expressly intended to be a 'practical guide' (2022: Executive Summary). While the UK's Data Sharing Code of Practice is long, it is relatively clear and easy to navigate, and includes checklists, templates and case studies.[64]

164. It is also important to note that taking a more principles-based approach to the DAT Act's authorisation framework is more than simply legislating the 'Five Safes' or 'data sharing principles'. The DAT Act's current approach to the Five Safes is not strictly a principles-based approach, noting that they are embedded within and enabled through the DAT Act's very prescriptive, rules-based approach.

165. The Review considers that the data sharing principles should be retained. In general, there is agreement among stakeholders that the Five Safes is an appropriate framework for assessing and mitigating against the risks associated with a particular data sharing activity.[65] However, the way in which they are used in the authorising framework should be reconsidered to ensure they are truly able to operate as principles in a legislative design sense. There is also a role for further guidance on how they should be applied in particular circumstances, or how they are satisfied if specific requirements apply. For example, if there is a requirement that sharing may only occur using a secure access service, this may comprehensively address the 'setting' principle for that project (though this would still require a holistic, case-by-case assessment). Most importantly, it should be clear to prospective participants that – and how – the amended framework can enable one-off transfers of data, ongoing access, two-way data flows, and/or large-scale enduring linkage, and the administrative burden of each type of activity should be proportionate and minimised to the extent possible.

166. There are additional principles which the DAT Act's authorising framework should set out. For example, the Review considers that highly detailed data sharing agreements should not be the primary mechanism to authorise sharing.[66] However, data sharing agreements currently serve two important functions under the DAT Act: documenting the agreement between the parties (as any contract or memorandum of understanding would) and acting as a vehicle for transparency as a consequence of registration with the National Data Commissioner (i.e., inclusion on the public data sharing agreement register). Therefore, it may be appropriate to instead introduce principles that data sharing activity must be:

- appropriately documented, to ensure the parties' responsibilities are clear and that there is a record of what the parties to the sharing agree to, and

[64] This Code of Practice is currently under review as a result of recent amendments made to the UK's data sharing legislation.
[65] There are exceptions. For example, the Australian Computer Society (Submission 10) advocates a quantitative measure of output disclosure risk. The Review considers that there may be circumstances where this approach is appropriate, but as this may not always be the case, the principled approach afforded by the Five Safes framework is more effective to achieve flexibility.
[66] Submission to the Review's draft findings and recommendations support this, e.g. Submission 87, Western Australia Department of Premier and Cabinet; Submission 87, Data Synergies).

- made sufficiently transparent, for members of the public to be adequately informed of the data sharing activity.

167. The National Data Commissioner could support participants to comply with these principles by providing agreement templates for different types of projects and activities, and by specifying what details about data sharing activities should be made public.

168. A principles-based approach can also assist with ensuring applicable safeguards are proportionate to the risk of the particular project by recalibrating the privacy protections so that they are consistent with, rather than in excess of, Privacy Act requirements. For example, a principle that sharing under the DAT Act would be authorised where it would be permitted under the Privacy Act would ensure alignment of both frameworks – without requiring participants to traverse duplicative (and voluminous) requirements.[67]

169. To the extent that any additional protections for personal information need to be included in the legislation, careful consideration should be given to whether they are proportionate, clear and reasonable in the context of a particular data sharing activity. This should also be done in coordination with relevant reforms to the Privacy Act. While the scope of a second tranche of reform of the Privacy Act is still to be settled, this may include measures to permit broad consent to use personal information for general research purposes and change requirements around the use of biometric data.

170. Further, a principles-based approach could be used to reframe the authorisation as enabling and permissive, rather than proscriptive and overemphasising risk. The current approach of the DAT Act is that secrecy provisions are only overridden if the sharing is authorised, which will only be the case if all of the numerous requirements are met. By contrast, a more enabling framing would leave no doubt that adherence to the principles in essence positively authorises the data sharing activity. While this distinction may seem largely cosmetic, the latter approach has a better prospect of success for overcoming the disincentives for data custodians to share data that arises because of perceived risks. This may not fundamentally change a custodian's obligation to ensure that data sharing is lawful; but in enabling custodians to be more confident that the requirements are understandable and achievable, they are better placed to determine that sharing under the DAT Act will be lawful.

171. Again, and for the avoidance of doubt, the Review is not suggesting that there should be no protections for sharing personal or otherwise sensitive information. It is the Review's opinion that, to the contrary, ensuring the legislation is simpler and truly principles-based will more effectively enable protections to be applied. This is because it will be easier for participants (and the regulator) to discern and apply the relevant protections. This can also encourage data custodians to use the DAT Act's authorising framework to share data by reducing their compliance costs.

172. Recommendation 2 is further supported by, and relates to Recommendations 5 to 7 regarding the accreditation framework, and Recommendation 10 regarding the purposes for which data can be shared, especially with respect to data curation.

[67] This could include sharing information that would otherwise be prohibited under a secrecy provision – so long as the sharing occurs consistently with the Privacy Act requirements.

Recommendation 3

The DAT Act should embed a default posture of agreeing to share data, with data custodians able to refuse requests in appropriately limited circumstances, subject to oversight and review.

173. In concert with amendments to improve the DAT Act's useability, amendments should be made to ensure data custodians take a default position of agreeing rather than refusing to share data. This default position of agreeing to share data in the public interest is consistent with the role of data custodians as collectors and storers of government data, holding that data on behalf of the government and the Australian public, and enabling that data to be used for public benefit.

174. There are two related components to this recommendation: providing assurance to data custodians regarding their risks in sharing data (i.e., improving incentives for custodians to share data), and introducing transparency rigour, and oversight to data sharing decisions (i.e., improving outcomes for requestors of data).

Addressing data custodian risks and incentives

175. The DAT Act should improve the incentives for data custodians to use the DAT Act by addressing the risks data custodians' face in sharing data. That is, in addition to being easier to use, it should be clear that if data custodians share data consistently with the DAT Act, they will not be liable for misuse by the user of the shared data, or inadvertently contravene other legal prohibitions on sharing the data.

176. This point is strongly linked to Recommendation 2: increasing the clarity and navigability of the DAT Act's requirements will make it easier for data custodians to both understand and comply with their obligations. Under current settings, data custodians are uncertain about whether and how the statutory override operates. This is likely a function of the general complexity and excessive prescription of the DAT Act, but may also be because there is no unambiguous positive statement about the lawfulness of sharing data under the DAT Act, or clarity regarding the limits of data custodians' liability for mishandling and misuse of data by authorised recipients of data.

177. Assurance could be provided to data custodians by introducing a 'safe harbour' in the legislation, which would protect data custodians from liability if they have taken certain steps. The concept of 'safe harbour' is referred to – and recommended as – an 'alternative compliance pathway' for privacy obligations in the Productivity Commission's Interim Report on Harnessing Data and Digital Technology (2025). This idea is also supported in submissions received by the Review. For example, Data Synergies suggests a 'limited' safe harbour may be appropriate where a data custodian exercises 'reasonable diligence in relation to a particular stated data use and relies upon a higher level accreditation of a downstream entity'.[68] Along similar lines, the Population Health Research Network's (PHRN) submissions highlight risks for data custodians sharing data which may be subject to a common law or equitable duty of confidentiality.[69] The PHRN

[68] Submission 67, Data Synergies, pg. 4.
[69] Submission 45, PHRN; Submission 79, PHRN.

suggests the DAT Act should make clear that, where sharing is authorised by the DAT Act, it is 'not in breach of a common law or equitable duty of confidentiality, and that data custodians and recipients are protected from liability in this respect'.[70]

178. There are examples of clear statements regarding the limits of liability on data custodians in other legislation. For example, section 188 of the *Privacy and Responsible Information Sharing Act 2024* (WA) provides that a person handling information 'believing in good faith that the handling of the information is authorised' does not incur civil or criminal liability and is not to be regarded as breaching any duty of confidentiality or secrecy. Similarly, under the UK's *Digital Economy Act 2017*, disclosing personal information under the relevant provisions of that Act (e.g. subsection 40(7)) 'does not breach—

a) any obligation of confidence owed by the person making the disclosure, or

b) any other restriction on the disclosure of information (however imposed).'

179. These provisions are clearer than the DAT Act's statutory override, which simply states the DAT Act's authorisations have effect despite any other law of the Commonwealth, a state or a territory. Though broadly the same in effect (apart from the common law duty), section 23 is not as direct as the above examples. A safe harbour provision would go a step further in ameliorating risk as a driver of data custodians' reluctance to share data by making it clear that the DAT Act's framework is an affirmative rather than contingent authorisation.

180. Further improvements could be made by resolving the issues around the definition of 'data custodian' under the DAT Act raised by Services Australia and noted by the Department of Health, Disability and Ageing.[71] To lawfully share data under the DAT Act, the sharing entity must be the 'data custodian' of the relevant data (paragraph 13(2)(a)). However, there may be more than one data custodian: an entity will be the custodian of data if it 'controls' that data. Control can be physical possession but can also be a lawful authority to decide how the data should be handled – including to provide access to it. The DAT Act requires that, where there are joint data custodians of data, all custodians must give their permission for the data to be shared (paragraph 13(2)(b)). This issue, in combination with data custodians' concerns about liability for sharing data, have resulted in additional impediments to sharing data under the DAT Act, as any joint custodian has an effective veto against any other joint custodian's decision to share. [72]

181. This could be addressed either by narrowing the definition of 'data custodian', so that the instances where there are joint custodians are reduced, or by dispensing with the term 'data custodian' generally (the authorisation to share data in section 13 and the 'data sharing project' provision in section 11A refer to 'the sharer' as the relevant entity). If the DAT Act retains a concept that continues to recognise multiple 'data custodians', then the DAT Act could provide that approval by any relevant data custodian is sufficient to authorise the sharing (and that no other joint custodian bears any liability in relation to the sharing). Alternatively, the National Data Commissioner or Minister could be given a

[70] Submission 79, PHRN, pg. 10.
[71] Submission 53, Services Australia; Submission 18, Department of Health, Disability and Ageing.
[72] Potential issues regarding the definition of, and use of the term, 'data custodian' were identified prior to the passage of the DAT Bill 2022 by Bennett Moses (2020:638).

power to designate a single custodian as the relevant decision maker upon request by joint custodians or a data requestor.

Improving decision-making processes and outcomes for data requestors

182. There should be concrete parameters for the exercise of data custodians' discretion over whether to share data. Clear requirements for data sharing decisions should be introduced to ensure that data sharing requests are dealt with in a timely, reasonable and transparent manner.

183. These requirements should include a clearer obligation that requests be considered in a timely manner (rather than the current requirement to consider requests 'within a reasonable period'). This will afford requestors a more concrete basis on which to escalate legitimate concerns about the time taken by data custodians to respond to requests.

184. This could also include an option for specific timeframes and processes to be prescribed in subordinate legislation and guidance. Acknowledging that timeframes may reasonably vary based on a number of factors, it may be appropriate to allow exceptions to apply to any prescribed or default timeframes in particular circumstances. It may be feasible to prescribe timeframes for particular classes of requests, for example, if the requested data does not include personal or otherwise sensitive information. The determination of any prescribed timeframes should be done in close consultation with data custodians, to take into account their existing capabilities and processes. There could also be an option to extend timeframes in relation to particular requests for a limited period if both the requesting and the sharing entity agree. Implementation of this recommendation should emphasise the overarching goal of standardising and encouraging transparency in the time Commonwealth agencies take to consider and respond to data sharing requests.

185. The discretion to refuse data sharing requests should also be limited so that data custodians may only refuse requests where it is reasonable to do so. A standard of reasonableness for refusal decisions could be established by having regard to relevant (non-exhaustive) considerations. These could include:

- the level of accreditation of the requesting entity and the sensitivity of the requested data
- any steps that could be taken to mitigate the risks of the particular activity, and the relative burden of those steps on particular parties
- where the resource impact would be disproportionate or prohibitive for the data custodian
- any timing constraints on the requestor's funding or reliance being placed on the request for a grant application, and
- where the request, within a reasonable timeframe, will be, or has been substantially met under a different legislative framework.

186. As an example, it may be unreasonable to refuse a particular data sharing request from an entity with a suitable accreditation (i.e., with the requisite demonstrated

capability), considering the public benefit that will be met by the proposed activity. By contrast, it may be reasonable for the data custodian to refuse the request because it has committed to fulfilling that request under a different framework within a well-defined, reasonable time frame. Considerations of this kind would allow data custodians to continue to use familiar and well-established frameworks for data sharing, while also recognising the interests and capability of, and investments made by, data requestors. This is a key way in which an amended DAT Act can materially contribute to and improve data sharing practices, and, over time, may become the preferred method to request, and, ultimately, provide access to, data – particularly if an amended DAT Act is easier to use and more reliable than other frameworks.

187. A standard of reasonableness as a concrete parameter for refusing to share data can also be supported by a pathway for requestors to escalate data sharing requests. Such a pathway could require a request to be escalated in the first instance to another, more senior individual in the data custodian's organisation (e.g. the authorised officer), and then to the National Data Commissioner – potentially with the support of the National Data Advisory Council – to review the request and refusal decision. This process could result in recommendations to mitigate particular risks (e.g. to recruit the services of a third-party ADSP or negotiate in respect of the granularity of the requested data), and provide assurance to data custodians that sharing will be 'safe'.

188. Consideration could also be given to a legislated Ministerial power to direct that sharing must occur, subject to appropriate safeguards, as a last resort. These safeguards could include that the power only be exercisable on advice from an independent office or body (such as the National Data Commissioner), where the requestor is accredited to the appropriate level, and where the appropriate escalation processes have been exhausted.

Recommendations 2 and 3 in concert

189. Recommendations 2 and 3 will be optimally effective if they are both implemented. While improved clarity and useability of an amended DAT Act would improve its operation, it is unlikely to deliver substantially improved data sharing outcomes without changes that overcome data custodians' disincentives to share data, or the incentives to deal with data sharing requests in a manner that is sub-optimal at a systems level.

190. Without these amendments, opportunities to derive public benefit from the data held by the Commonwealth, and the effective sharing of that data, will continue to be missed. If these recommendations are not able to be implemented, it is the Review's opinion that the DAT Act's authorisation framework should instead be allowed to sunset.

Enhancing the value of the DAT Act: a ministerial power to authorise sharing

191. The DAT Act's proposed role is to provide an authorisation to share data where no other legal pathway is available, or where it would be preferable over other systems. Some types of data are excluded from being shared under the DAT Act, and there are some purposes for which data cannot be shared (e.g. national security and law enforcement information; and enforcement-related purposes). These are blanket

exclusions and the Review does not, for the most part, recommend they be substantially revised (but see Recommendation 10).

192. It is likely there will be future data sharing initiatives of national significance that the DAT Act cannot authorise because of these exclusions. It is also possible that there is uncertainty or disagreement about whether the DAT Act can authorise a significant initiative. Examples of nationally significant data sharing initiatives that the DAT Act has not been deployed to authorise are: the Veterans' Data Asset, recommended by the Royal Commission into Defence and Veteran Suicide (2024: Volume 6, section 29.3.2) and a national linked criminal justice data asset to provide evidence about perpetrators of family, domestic and sexual violence (Coade 2024; AIHW n.d.).[73]

193. In the Draft Findings and Recommendations, the Review outlined a draft Recommendation that the Minister should have an express power to authorise data sharing that is not otherwise authorised under the DAT Act where the sharing is in the national interest, subject to appropriate safeguards. The draft Recommendation was that this power should only be available to be used in exceptional circumstances where there is a clear national interest or benefit, to enable discrete instances of data sharing. It was suggested that such a power should be subject to appropriate controls and safeguards – for example, by requiring a disallowable instrument to be made to ensure the exercise of the power is subject to parliamentary scrutiny or only being exercisable on the advice or recommendation of an appropriate office holder or body.

194. The draft report recommended that this power should be tied to a demonstrable national interest to allow the Minister to consider and balance a broader range of interest than the existing public interest purposes, but which would also set an appropriately high threshold for exercising the power. Submissions on the Draft Findings and Recommendations tend not support such a power, or express considerable hesitance about it. For example, the AIHW, the Department of Health, Disability and Ageing, explicitly do not support the draft Recommendation: the AIHW, because the AIHW's legislation already includes a ministerial directions power;[74] the Department of Health because such a power displaces the discretion of responsible ministers, who are better placed to make informed decisions about data within their portfolios.[75]

195. Other submitters hesitant to support this draft Recommendation call for further detail about how the 'national interest' would be defined and what the proposed safeguards would be, further consultation, and additional information about why such a power would be justified.[76] Concerns are also raised that use of an 'elastic' concept such as the 'national interest' to justify this power may undermine public trust.[77]

196. The Review still considers that there may be merit to a ministerial power of this kind to drive greater data sharing outcomes and overcome barriers to sharing in exceptional circumstances. However, it has not made a final Recommendation about a power of this kind as such a power is not critical for the DAT Act to be effective in its usual operation.

[73] In the first example, it is possible the DAT Act could be used to authorise the building of, and access to, the asset. However, under current settings, there may be some doubt about whether the DAT Act could be relied on to authorise this activity, and doing so may be prohibitively complex and burdensome. In the case of the second example, the DAT Act could not be used because the purpose of the sharing is precluded as it is an enforcement-related purpose.

[74] Submission 64, AIHW, pg. 5.

[75] Submission 69, Department of Health, Disability and Ageing, pg. 5-6.

[76] Submission 82, Services Australia; Submission 68, Department of Education; Submission 87, Western Australia Department of Premier and Cabinet; Submission 83, University of Melbourne.

[77] Submission 67, Data Synergies, pg. 5.

The following points are made to assist with any further consideration the Government may wish to give to developing such a power.

197. Consideration could be given to whether the national interest is an appropriate threshold or trigger for exercising a ministerial power. It may also be appropriate to limit the scope of the power in relation to data that originated from a state or territory. Preconditions and safeguards for such a power could also be considered, such as requiring:

- the NDAC to provide advice on the appropriateness of the exercise of the power (similar to the role of the Review Boards in the UK – see Appendix C, Part 5)
- the approval of multiple relevant Ministers (e.g., the Minister responsible for the data proposed to be shared as well as the Minister with whole-of-government data policy responsibility)
- appropriate consultation to be undertaken before sharing is approved
- a maximum time for which data sharing can be authorised
- parliamentary and public scrutiny and oversight, for example, by requiring the making of a legislative instrument that is subject to disallowance.

198. A ministerial power as described above would help ensure that the DAT Act can be used effectively in exceptional, unforeseen circumstances that would have a significant public benefit, and subject to appropriate safeguards. This would also prevent the need for a blanket broadening of the DAT Act, while improving the overall value of the DAT Act's data sharing framework. The Review puts this forward as a suggestion for consideration, but not as a formal recommendation.

The National Data Commissioner's functions and powers

Finding 5

The National Data Commissioner's current functions and powers do not effectively enable them to support uptake of the DAT Act, or to drive improvements across the broader public sector data sharing system. The National Data Commissioner is therefore not empowered to successfully advance the objects of the DAT Act.

199. The Review considers that the National Data Commissioner's regulatory and enforcement powers are too heavily focused on compliance once data sharing under the DAT Act is occurring, without sufficient ability to support participants to establish data sharing arrangements and facilitate transparent and consistent decision-making by data custodians.

200. Additionally, the National Data Commissioner's functions and responsibilities in respect of supporting best practice data sharing and handling across the Commonwealth significantly exceed the regulatory tools that would be required to realise meaningful system-wide improvements.

201. Overall, the National Data Commissioner's functions and powers are not effectively calibrated to enable the advancement of the DAT Act's objectives in improving the availability and use of public sector data in the public interest.

202. The National Data Commissioner's current functions under the DAT Act are to (sections 42 to 45A):

- provide advice on the application and operation of the DAT Act, including to provide advice on particular aspects of the DAT Act to the Minister
- provide guidance on the DAT Act's operation and requirements through the making of data codes (with which participants must comply) and guidelines (to which participants must have regard)
- regulate and enforce the DAT Act's data sharing framework through the exercise of regulatory and enforcement powers (including as the accreditation authority for certain types of entities and DAT Act roles)[78]
- provide education and support data custodians and Commonwealth bodies to respond to requests for data, share data and safely handle data, including by providing information, educational material and support for the use and controlled sharing of public sector data.

Overemphasis on compliance

203. The National Data Commissioner has significant powers relating to data sharing activities authorised by the DAT Act. The National Data Commissioner can conduct assessments to ensure entities are complying with the DAT Act, and investigations to determine whether an entity is breaching, or has breached, the DAT Act (including in response to complaints made under the Act) (section 99 and 101). This includes powers to require information and documents and to issue binding directions (section 112). The National Data Commissioner also has monitoring and investigation powers under the *Regulatory Powers (Standard Provisions) Act 2014* (Cth), including powers to issue infringement notices, enforce undertakings, apply for injunctions, and seek to enforce civil penalty provisions (sections 113 to 116). The DAT Act also establishes criminal offences for unauthorised sharing and collection and use of data (a standard of recklessness distinguishes offences from civil penalty provisions) (sections 14 and 14A).

204. These are significant regulatory and enforcement powers, but they are only operative – and therefore only effective – if sharing is occurring under the DAT Act. As outlined in earlier sections, the DAT Act is not currently (meaningfully) used for data sharing. As the National Data Commissioner's powers do not apply to Commonwealth data sharing broadly, their ability to meaningfully oversee data sharing activities is significantly limited in practice.

205. There are potential benefits to these functions and powers for data custodians from an oversight and assurance perspective: data custodians (and the Australian public) can rely on an independent party to monitor users' activity to ensure compliance with the DAT Act. This could, in theory, bolster data custodians' confidence in sharing data under the DAT Act, by 'holding participants accountable to robust standards of privacy, security and transparency' (Revised EM: paragraph 22). Data custodians could, for example,

[78] Matters regarding the accreditation framework are discussed in depth later in this report.

complain to the National Data Commissioner if they thought an ADSP or accredited user was breaching a DAT Act data sharing agreement. This would trigger the National Data Commissioner's investigation powers, which could lead to further regulatory or enforcement action. Data custodians should be more confident, therefore, that any non-compliance would be detected and acted upon.

206. In part, this benefit has not been realised because of the barriers to uptake outlined above. Further, the significant focus on the regulation and enforcement aspects of the National Data Commissioner's role, along with potentially significant civil and criminal penalties for unauthorised sharing, collection and use, underscores the perception that data sharing is a high-risk activity. Instead of providing assurance, these features have provided a further disincentive to share in an already risk-averse cultural environment. Data custodians may also avoid using the DAT Act as they would also be subject third-party scrutiny to an extent they likely wouldn't be under their own frameworks.

207. The focus on monitoring rather than facilitating sharing also has an impact on the effectiveness of key transparency mechanisms in the DAT Act. These mechanisms include the requirements in section 34 that data custodians report the number of data sharing requests received and refused, and the reasons for refusal. The requirement to register data sharing agreements with the National Data Commissioner under section 33 is also a transparency mechanism to the extent that details regarding data sharing projects must be included on the public register (under section 130). The value of these mechanisms is only realised if the DAT Act's authorising framework is used. Without the required uptake of the DAT Act, these mechanisms will not be effective in achieving the objects of the DAT Act.

Overly broad education and support functions

208. The National Data Commissioner has broad education and support-related functions under section 45A of the DAT Act. These functions are to:

- foster best practice by data custodians when responding to requests to share, and sharing, public sector data, as well as safe data handling practices by Commonwealth bodies
- provide information, educational material and support to Commonwealth bodies related to using and proving controlled access to public sector data.

209. While these functions are intended to drive improvements in data handling and data sharing practices broadly, they have not resulted in material system-wide improvements.

210. The education and support-related functions replaced a proposed advocacy function in the original DAT Bill (Supplementary Explanatory Memorandum, DAT Bill 2022 (Supplementary EM): paragraph 294). The advocacy function was replaced in recognition of the potential conflict that may arise with the National Data Commissioner's regulatory role.[79] The education and support functions were intended to enable the National Data Commissioner 'to work with Scheme entities to support best practice [data sharing], including when responding to requests to share public sector data'

[79] Submission 23 from Electronic Frontiers Australia notes the ongoing potential conflict between the National Data Commissioner's education and support functions and their regulatory functions. The Review does not consider the tension between the National Data Commissioner's functions as a conflict-of-interest issue so much as an issue for the efficient and effective allocation of attention and resources.

(Supplementary EM: paragraph 294). This function was 'to support the overall functioning and operation of the Scheme' (Supplementary EM: paragraph 303).

211. The education and support functions are intended to support data handling and sharing practices by Commonwealth agencies more generally. However, they are not supported by any mechanisms to mandate centralised platforms, consistent practices, or the reporting of information about data sharing outside of the DAT Act. Without such levers, and without a substantial proportion of Commonwealth data sharing occurring voluntarily under the DAT Act, the National Data Commissioner cannot effectively foster consistency across the data ecosystem more broadly.

212. The products and guidance the ONDC has produced under this function have been valuable, but their reach and uptake have been limited. For example, the ONDC's guides to developing a data inventory and metadata attributes, and the Australian Government Data Catalogue, are both resources that can support best practice data handling and sharing, and uplifting capability (see e.g. Mesman 2024). Similarly, the Dataplace platform is a tool that has been developed to support data sharing broadly (not just sharing that occurs under the DAT Act). Dataplace is a tool that custodians can use for recording and tracking their data sharing activities, and provides a mechanism to interact with data requestors.

213. However, using these tools and practices is not mandatory for Commonwealth agencies. They therefore have limited efficacy in facilitating consistency and standardisation across Commonwealth agencies, as agencies can continue to use their own systems (or no system at all).[80] Agencies are also incentivised to continue to use their own systems particularly if the costs of adopting new voluntary systems exceeds the potential benefits (e.g. if the new system is more complex or onerous than the agency's established system). This undermines the ability to advance the objects of the DAT Act, in particular to establish institutional arrangements for sharing public sector data (paragraph 3(e)).

214. Further, key initiatives to uplift data maturity, capability and governance are undertaken by the Department of Finance, not the National Data Commissioner or the ONDC (e.g. the Data Maturity Assessment Tool (Department of Finance 2025)). The overlaps and distinctions between the National Data Commissioner's education and support functions and the Department's function in relation to whole-of-Australian-government data policy are unclear and potentially duplicative or conflicting, and may give rise to gaps in initiatives that uplift data sharing and handling practices more broadly.

215. For example, as set out above, the reporting requirements applicable to data custodians only apply in relation to requests and sharing under the DAT Act. No other reporting requirements apply to data custodians that capture data sharing outside of the DAT Act. There is therefore no complete picture of data sharing activities at a whole-of-government level.[81]

---

[80] Some agencies have adopted these tools for non-DAT Act data sharing, e.g. the Department of Employment and Workplace Relations (Submission 17). But, in general, uptake, particularly of Dataplace, has not been widespread or consistent. This has been frustrating for data requestors (see e.g. submissions from Monash University (Submission 36) and the University of Melbourne (Submission 58).

[81] The number of data sharing arrangements reported by Commonwealth agencies is an indicator of success in strengthening partnerships in the Implementation Plan to deliver the Data and Digital Government Strategy (Australian Government 2023:23)). The figure included in the updated Implementation Plan (Australian Government 2024:28) comes from an

Lack of functions and powers to facilitate and enable data sharing

216. The importance of playing a facilitative role to support data sharing is recognised in the explicitly 'facilitative' regulatory posture of the ONDC (ONDC 2024: 3; ONDC n.d.). This facilitative role includes, for example, assisting entities to understand and navigate the DAT Act, as well as helping data requestors and data custodians progress data sharing requests and activities. This role is particularly important considering the complexity of the DAT Act's authorising framework, and can assist participants to navigate the framework. A facilitative approach provides assurance that safeguards and requirements are being adhered to, by helping to ensure participants understand what the relevant requirements are.

217. Undertaking a facilitative function aligns with the National Data Commissioner's general functions in establishing the DAT Act framework, and is also supported by the National Data Commissioner's advice function under paragraph 43(aa).[82] This function allows for the provision of regulatory advice, potentially reducing the need for individual entities to obtain legal advice on the operation of the DAT Act, and was 'intended to drive best practice by supporting safe sharing of data' (Revised EM, paragraph 324).

218. The submissions to the Issues Paper indicate broad support for bolstering the facilitative role of the National Data Commissioner and the ONDC. For example, the South Australian Department for Health and Wellbeing recognises the benefits of the ONDC playing a facilitative role and undertaking enabling functions.[83] The Department of Health, Disability and Ageing suggest that the ONDC should be empowered 'to play a more active role in providing guidance and support to participants who are new to Commonwealth data sharing processes'.[84] The Department of Employment and Workplace Relations also suggest 'extending the Commissioner's role in providing education and support for entities participating in the DATA Scheme', and highlighted as an example the role of the Data Sharing Network of Experts in the UK.[85] The University of Melbourne advocates for an expanded and strengthened 'broker'/'coordinator' role for the ONDC.[86]

219. The approach taken by the ONDC recognises that entities are more likely to use the DAT Act's authorising framework, and participate in DAT Act data sharing activities, if the regulatory approach assists entities to understand their obligations and work through challenges collaboratively. This benefit is less likely to be realised by taking a compliance-focused approach which could be perceived by potential participants as more restrictive or prohibitive.

220. However, notwithstanding these efforts, the ability for the ONDC and the National Data Commissioner to play an effective facilitative role is practically limited. The National Data Commissioner does not have an express function to mediate between requestors

---

informal survey referenced at footnote 11. The original Implementation Plan recognises that Dataplace could be used by agencies to record their data sharing arrangements (Australian Government 2023), though this would be on a voluntary basis.

[82] The ONDC has established a formal process for the provision of advice on the operation of the DAT Act (ONDC n.d.).

[83] Submission 55, South Australian Department for Health and Wellbeing.

[84] Submission 18, Department of Health, Disability and Ageing, pg. 4. The Review considers this more active role needn't be limited only to new participants.

[85] Submission 17, Department of Employment and Workplace Relations, pg. 3.

[86] Submission 58, University of Melbourne, pg. 6, 11.

and data custodians to resolve barriers to data custodians agreeing to share data or to effectively oversee decisions to refuse data sharing requests.

Recommendation 4

The National Data Commissioner's functions and powers should be recalibrated to focus on assurance, oversight and assistance in facilitating data sharing decisions.

221. The National Data Commissioner's functions and powers should be amended to support the revised role and settings of the DAT Act's authorising framework outlined in Recommendations 1 to 3. The scope of the National Data Commissioner's role should be refined to more effectively enable and support sharing under the DAT Act, and should reflect the refined scope and purpose of the DAT Act in the data sharing ecosystem, as outlined in Recommendation 1.

222. In particular, the National Data Commissioner should be empowered to facilitate decisions to share data by:

- providing assurance to data custodians and requestors about how data can be shared lawfully and in a manner that reduces and mitigates risks (supplementing and enhancing the National Data Commissioner's existing advice functions and their education and support-related functions)
- assisting requestors to make requests of data custodians effectively and providing oversight of data custodians' decisions, to ensure transparency and consistency
- mediating and acting as an independent broker between requestors and data custodians to navigate and overcome barriers to undertaking data sharing activities.

223. Many stakeholders are supportive of a more expressly facilitative function in their submissions to the Draft Findings and Recommendations. Several stakeholders support this recommendation.[87] The PHRN suggests that independent mediators certified by the National Data Commissioner could more effectively play this role.[88] At this stage, the Review considers that this role should be carried out by the National Data Commissioner through ONDC, noting the resources that would be required to establish an additional administrative process for certification.

224. Shifting the focus of the National Data Commissioner's functions and powers away from a regulatory posture of strict enforcement and compliance will be enabled by recalibrating the legislative approach in the DAT Act's framework (as outlined in Recommendation 2). That is, a more principles-based, outcomes-focused approach to the authorising framework can enable the National Data Commissioner to take a more facilitative, collaborative approach to supporting entities' compliance. An example of this is the recommendation to move away from highly complex and detailed data sharing agreements as the main mechanism for authorising sharing. This would reduce the resource impost on the National Data Commissioner and participants in ensuring compliance with the DAT Act's existing requirements. The National Data Commissioner

[87] Submission 69, Department of Health, Disability and Ageing (in principle); Submission 86, University of Tasmania; Submission 73, Monash University; Submission 83, University of Melbourne; Submission 85, University of Sydney; Submission 87, Western Australia Department of Premier and Cabinet.
[88] Submission 79, PHRN.

could instead redeploy resources to produce practical and specific guidance, including through subordinate instruments that would support the principles-based approach in the primary legislation.

225. Consideration should be given to ensuring that the functions and role of the National Data Commissioner does not duplicate the role of the Australian Information Commissioner under the Privacy Act. Where data sharing activity includes personal information, the Information Commissioner should have regulatory authority and responsibility. This is recognised by the DAT Act in its current form, for example, in the 'privacy coverage condition' (section 16E), requirements for compliance with an 'APP-equivalence term' (section 16F), notification of eligible data breaches (section 37), and the ability for the National Data Commissioner to transfer matters to an appropriate authority (section 107). The ONDC and the OAIC should continue to work together to ensure the regulatory purview of each office holder is clear to participants and the Australian public in relation to data sharing.[89]

226. Noting that personal information is not the only type of sensitive data that could be shared under the DAT Act (in its current or recommended form), regulatory powers and penalty provisions should be retained. However, the extent of the monitoring, investigation and enforcement powers available to the National Data Commissioner could be scaled back without unduly compromising the oversight of, and safeguards for, sharing under the DAT Act. This is particularly the case if the National Data Commissioner is more effectively empowered to facilitate and support entities to establish compliant, best-practice arrangements. Relatedly, the Review does not consider that the National Data Commissioner should be given a broad power to regulate, oversee, and undertake inquiries into data sharing activities that occur outside of the DAT Act.[90] Adequate assurance can be achieved by ensuring that the DAT Act is an attractive option for data requestors (by introducing rights to have decisions reviewed), as the National Data Commissioner will have greater oversight overall than is currently the case.

227. The Review considers that the National Data Commissioner's existing educative and support-related functions that are directed toward broader capability uplift across the Australian Public Service should be the responsibility of other appropriate Commonwealth agencies, equipped with the positional authority, tools and levers to secure such uplift. This would ensure greater alignment of these functions with the development and implementation of whole-of-government data policy and capability-building initiatives (see further at Recommendation 15). It would also allow for the more effective allocation of resources to ONDC's proposed role in facilitating and supporting the establishment of data sharing arrangements under the DAT Act.

228. In the Review's opinion, it is appropriate for the DAT Act to be implemented and overseen by an independent statutory office holder, supported by an office such as the ONDC. That is, the functions, powers and responsibilities of the National Data Commissioner should not be transferred to a departmental official or undertaken by a different Commonwealth agency. Doing so would undermine the integrity and neutrality

[89] As the OAIC notes in their submission to the Draft Findings and Recommendations (Submission 77), the two Offices are already working together on sharing information 'in areas of mutual significance'. The Review also supports the OAIC's suggestion of working together to produced 'streamlined regulatory guidance and templates on how to conduct effective Privacy Impact Assessments which will simplify the privacy safeguards in the DAT Act'.

[90] This aligns with responses the Review received to the focus question under Draft Recommendation 6, for example, from the AIHW (Submission 64) and the Department of Education (Submission 68).

of the role, as the relevant functions would be undertaken by an agency that is also a regulated entity – as a data custodian and possibly an accredited entity – which would introduce unnecessary potential for conflicts of interest.

229. Regulatory independence is desirable, especially in the mediation/neutral broker function being proposed, where independence and neutrality are important for the legitimacy and efficacy of the role. Maintaining this independence also allows resources of other key data and data policy agencies to continue to be deployed to support the ongoing success of key data initiatives (such as the NHDH, the PLIDA, and the Data and Digital Government Strategy).[91]

230. It may be beneficial to reconsider the title of the office holder to make the refined scope of functions clearer. That is, the title 'National Data Commissioner' gives the impression of being responsible for all data sharing, rather than, as proposed, sharing only under the DAT Act.

Accreditation framework

231. Accreditation is one of several general approaches to quality assurance. Others include audit, peer review, ranking systems, and external review (Harvey and Green 1993; Kumar et al. 2024). Accreditation is a process in which status is granted to an institution by an accreditation authority which indicates the applying institution meets or exceeds established standards relevant to a particular domain or sector (van Damme 2004). Grepperud and Pedersen (2020) identify two forms of accreditation, one which relates to the assessment of 'output' and one which relates to 'process'. Output accreditation infers the adequacy of the processes employed to produce a particular output from the quality of that output, while process accreditation considers input-adequacy with an emphasis on continuous improvement and the maintenance of long-run sector capability.

232. Governments and industry associations establish accreditation frameworks to support sectors in maintaining standards of output and/or quality of practice. Although they vary in design and application, most accreditation frameworks contain core features which distinguish them from other modes of quality assurance. Typical features include:

- a certified set of accreditation standards
- a competent body (accreditation authority) which assesses accreditation applications against the accreditation standards
- binary (yes/no) and time-limited accreditation decisions, and
- a mechanism which allows the competent body (accreditation authority) to undertake ongoing post-accreditation monitoring (van Damme, 2004; Hämäläinen, Mustonen, and Holm, 2004).

233. In Australia, all levels of government play a critical role in the development, implementation, and coordination of accreditation frameworks to support critical sectors including health services (hospital and health care facilities), health professions, disability services, aged care, construction, education, environmental management, food safety,

[91] If a decision is made to allow the DAT Act's authorising framework to sunset, the relocation of some of the National Data Commissioner's proposed functions to another Commonwealth agency should be reconsidered.

and transport. Similarly, government-administered accreditation frameworks support the provision of digital services both in Australia and abroad.

234. Accreditation frameworks all navigate similar challenges and are subject to disruption from technological and other trends. The primary challenge for regulators is the need to translate accreditation status, which is obtained through periodic assessment and/or audit processes, to year-round operational quality.

235. Regulators must also balance the competing priorities of accreditation rigor with its regulatory load on participants. Accreditation frameworks impose initial (application) and ongoing (compliance) costs on sector participants and it is important that the benefits of accreditation exceed these costs. An important factor in regulatory load are its distributional impacts, which can be exacerbated when access to government funding or other benefits are tied to accreditation status.

Non-data and digital government-administered accreditation frameworks in Australia

236. Table 1 summarises the features of extant accreditation frameworks which support the Australian health services, health professions, disability, and aged care sectors. Further details on these accreditation frameworks are provided in Appendix E.

Table 1: Non-data and digital accreditation frameworks in Australia

Sector	Regulatory Body	Key Standards	Impact
Health Services	Australian Commission on Safety and Quality in Health Care	Clinical governance, infection control, medication management, comprehensive care, blood management, acute deterioration management	Mandatory for Medicare/government funding; strong economic incentive for compliance
Health Professions	Australian Health Practitioner Regulation Agency & National Boards	Faculty qualifications, student support, facilities, curriculum content, examination processes	Required for professional registration; barrier to entry into health professions

Sector	Regulatory Body	Key Standards	Impact
Disability Services	National Disability Insurance Scheme (NDIS) Quality and Safeguards Commission	Person-centred support, rights and empowerment, health and well-being, governance, operational management, and support environment	Required for NDIS registration and funding; limits market access without registration
Aged Care	Aged Care Quality and Safety Commission	Consumer dignity and choice, assessment and planning, personal and clinical care, daily living support, physical environment, feedback and complaints, human resources, organisational governance	Required for government subsidies; ensures quality of residential aged care services

Digital identity accreditation frameworks

237. Digital identity accreditation frameworks assess and regulate institutions adherence to standards in respect of the delivery of digital identity verification services.[92] Data accreditation frameworks, in contrast, accredit and regulate institutions based on their capability to engage safely and securely in data sharing activities.

238. Several countries have implemented digital identity legislation (with supporting frameworks) to ensure providers of digital identity services meet defined standards of data security, privacy, and service quality. Implementations in the United Kingdom, European Union, Canada, and Australia are summarised in Table 2 below. Additional discussion of these frameworks is provided in Appendix F.

[92] Given digital identity services involve the sharing and use of identifiable citizen data, their associated regulatory frameworks are most closely aligned with those in place for the sharing of public sector data and hence are included in this analysis over other digital accreditation regimes (such as those relating to ICT hardware and software, cloud computing, and cybersecurity).

Table 2: Digital identity accreditation frameworks in the UK, EU, Canada, and Australia

Country	Regulatory Body	Key Standards	Impact
United Kingdom	UK Government (under the *Data (Use and Access) Act 2025* (UK))	Identity verification confidence levels, secure authentication (e.g. MFA), attribute validation, privacy and consent management.	Required for obtaining a trust mark and inclusion on public register; enables access to government data
European Union	National Supervisory Authorities (under EU Commission oversight)	User control, privacy, interoperability, security, and data protection.	Mandatory for cross-border recognition; regulated by national supervisory authorities
Canada	Digital ID and Authentication Council of Canada	ICT security, privacy by design, interoperability, inclusivity, accessibly, governance, and transparency.	Voluntary; used as a reference model; recognised at federal and provincial levels
Australia	Australian Competition and Consumer Commission	Technical integration, authentication, security, data handling, data exchange, and interoperability.	Mandatory for participation in the Australian Government Digital ID System

Public sector data sharing accreditation frameworks

239. Public sector data sharing accreditation schemes evaluate organisations on their capability to meet the standards required for the sharing, use, and/or provision of services in relation to public sector-held data. Table 3 summarises examples of public sector data sharing accreditation frameworks in the United Kingdom, European Union, and Canada with further detail provided in Appendix G.

Table 3: Data sharing accreditation frameworks in the UK, EU, and Canada

Country	Regulatory Body	Key Standards	Impact
United Kingdom	UK Statistics Authority	Researcher training, public register of accredited researchers, project approval for public benefit, secure access environments, processor accreditation	Mandatory for access to de-identified public sector data; ensures secure and ethical use
European Union	National Authorities under EU Commission	Neutrality, transparency, data security; safeguards for public sector data sharing (e.g. de-identification, use of intermediaries)	Voluntary accreditation; trust mark enhances credibility; safeguards required for data access
Canada	Statistics Canada	Individual researcher-level security clearance and confidentiality agreements, approved public-interest projects, secure access via Research Data Centres	Mandatory for access to microdata; ensures vetted researchers and secure data environments

DAT Act accreditation

240. Public sector data sharing in Australia is currently facilitated through several domain-specific legislative channels. For research data, most apply the Canadian model in managing quality assurance at the individual project/program and researcher-level. An exception is the DAT Act which systematises organisation-level accreditation in respect of data sharing activities involving Commonwealth data.

241. An accreditation framework is enshrined in Part 5.2 of the DAT Act. Organisations seeking to access Australian Government data (users) or provide specialist data services (ADSPs) must be accredited. Data custodians do not require accreditation to participate in sharing under the DAT Act. The National Data Commissioner administers this accreditation framework and assesses eligible entities against the criteria for accreditation (section 77). As at 30 September 2025, the ONDC has accredited 36 Users and 14 ADSPs.

242. The DAT Act accreditation framework includes the 'expected characteristics' for accreditation (a detailed set of characteristics which underpin the general legislative criteria), application forms, guidance material, and assessment methodologies.[93]

243. The National Data Commissioner maintains separate application and assessment processes for user and ADSP accreditation. Application forms elicit information on an applicant's data management and data governance, ICT and security, and personnel capability (subsection 77(1)). The ADSP application form includes the additional requirement for applicants to identify the policies, practices, skills and capability they have in place to support the delivery of specific data services (subsection 77(1A)).

244. The DAT Act assessment methodology (Standard Operating Procedures) operationalises the assessment of user and ADSP accreditation applications. The Standard Operating Procedures detail roles and responsibilities, timeframes for assessment, the stages of the assessment process (including checkpoints and approval requirements), the preparation of material for decision by the accreditation authority, and include guidance, templates and reference documentation for assessors.

245. Despite growing recognition of the value of DAT Act accreditation, some data custodians identify a general lack of clarity on its evidence requirements and standards. This has resulted in instances of accredited entities accreditation being re-assessed by data custodians when reviewing data sharing requests.

246. The intended purpose of DAT Act accreditation is to improve the efficiency of data sharing by shifting both the initial and ongoing costs associated with performing baseline data capability assessments of users and ADSPs from data custodians to the National Data Commissioner (and therefore improve the efficiency of downstream data sharing agreement setting processes). Accreditation is positioned as an 'entry point' to participation (and regulation) under the DAT Act. Individual data sharing agreements still require negotiation and agreement on any finer controls specific to the sharing being proposed. Nevertheless, it is evident that DAT Act participants do not uniformly understand the difference between accreditation and the requirement to set finer controls when negotiating and establishing individual data sharing agreements. This has resulted in both real and perceived relitigating of accreditation status, and in turn, has somewhat impacted on the recognition of the accreditation process itself.[94]

247. To build awareness and trust in DAT Act accreditation, the ONDC initiated two independent reviews in 2024 to investigate the adequacy of assessment practices underpinning the accreditation framework. The findings, released in late 2024, identify DAT Act accreditation as an effective assurance mechanism to support data sharing.[95]

248. The DAT Act accreditation framework has also been considered alongside other assurance frameworks as part of the Trusted Entities program. The Trusted Entities program have identified the attributes of a 'trusted entity' to support national public sector data sharing (endorsed at the DDMM in August 2025 meeting). The Program is to be finalised at the next DDMM meeting in late 2025. The findings from the Program, which

[93] The expected characteristics for User and ADSP accreditation, sample application forms, and related guidance material are publicly available on the ONDC website. The accreditation assessment methodology is not publicly available. The assessment framework for accreditation continues to be refined by the ONDC, in consultation with external experts with experience in the implementation of similar schemes, and knowledge of current cyber, IT, and statistical standards (Submission 39, National Data Commissioner).

[94] Submission 9, ABS.

[95] Submission 38. National Data Commissioner.

were shared with the Review, state the trusted entity attributes are wholly consistent with the expected characteristics for DAT Act ADSP accreditation, and align with most of the expected characteristics for user accreditation, indicating that the DAT Act accreditation framework is generally robust and valuable. Outcomes from such evaluations, coupled with the priority of making the basis for DAT accreditation more transparent, indicate it is an important assurance mechanism for not only the DAT Act, but for the data system in general.

The value of DAT Act accreditation

Finding 6

DAT Act accreditation is a valuable framework which supports trust in the data system, however, its processes are perceived as burdensome, complex, and inflexible. The uniformity of accreditation standards, requirements for organisational-level accreditation, and strict authorised officer and eligible entity definitions act as barriers to participation under the DAT Act.

249. The significance, function, and structure of DAT Act accreditation features prominently in submissions and stakeholder engagements to the Review. While the Review has found broad support for DAT Act accreditation as a valuable contribution to the data system, further refinement is needed.

250. DAT Accreditation is widely viewed as both an important quality assurance mechanism which underpins the DAT Act and a pillar which supports trust in the data system generally, providing an independent assurance of data capability across data management and governance, ICT security, personnel capability, and data service provision.[96]

251. Despite the general lack of data sharing under the DAT Act, there are views from data custodians which highlight the utility of DAT accreditation as a mechanism which facilitates broader public data sharing. For example, the Department of Health, Disability, and Ageing note:

> The accreditation of jurisdictional data linkage centres as Data Service Providers under the Scheme has provided assurance for the sharing of the Commonwealth's Medicare Consumer Directory data with five States to enable the creation of national data linkage infrastructure, which facilitates interoperability between Commonwealth and State data systems.[97]

252. Further, accreditation is viewed as 'comprehensive', 'fair', and 'transparent'; with accreditation status leveraged and acknowledged by data custodians as evidence to support non-DAT Act data sharing engagements.[98] It has also been acknowledged, both anecdotally, and in submissions to the Review, that the standards established under the DAT Act accreditation framework support entities in uplifting their data capability.[99] At the same time, the accreditation framework has also been described as overly complex, with

[96] Submission 1, ACT Government; Submission 12, AIHW; Submission 18, Department of Health, Disability, and Ageing; Submission 17, Department of Employment and Workplace Relations; Submission 32, KPMG.
[97] Submission 18, Department of Health, Disability and Ageing, pg 2.
[98] Submission 58, University of Melbourne.
[99] Submission 61, University of Tasmania.

inadequate regulation of standards to support its use as 'an appropriate risk mitigation for sharing sensitive datasets'.[100]

253. Perspectives on the value of accreditation presented to the Review are consistent with the findings from ONDC-initiated reviews (completed in late 2024) and the Trusted Entities program,.[101] Further, findings from the Trusted Entities program identify the trusted entity attributes (established by the Trusted Entities program) broadly align with the DAT Act expected characteristics for ADSP and user accreditation.

254. Despite recognition of the general value of DAT Act accreditation, the Review finds in-general, the complexity, perceived uniformity of accreditation standards, and the separation of DAT Act accreditation from data sharing use-cases creates barriers to increased data sharing. Further, the DAT Act requires accreditation at the organisational level and has strict role and eligibility definitions which complicate its administration.

Application and assessment processes

255. Submissions to the Review indicate that applications for accreditation are burdensome and resource intensive.[102] This burden is coupled with uncertainty on the benefits accruing to applicants once accredited.[103]

256. Despite this, it is acknowledged that DAT Act accreditation is a rigorous process which promotes trust-building across the data sharing system. Balancing the application of a robust approach to accreditation with the regulatory burden of making accreditation applications and meeting post-accreditation compliance requirements is a common issue faced by regulators (van Damme 2004). Submissions to the Review suggest that DAT Act accreditation application and assessment processes could be further streamlined through addressing duplicative assessment processes (such as through recognising pre-application markers of applicant capability),[104] implementing measures which provide greater transparency on the evidence requirements for accreditation, and by adopting a risk-based approach to accreditation.[105]

257. The complexity and burden of accreditation processes are also due to the general design of the DAT Act. There is a lack of visible and obvious alignment between DAT Act accreditation standards and applicant use-cases, which is compounded by limited publicly available information on the evidence and capability requirements for accreditation. Further, the DAT Act is unduly restrictive insofar as it requires accreditation to be granted at the organisational level and imposes strict definitions of eligible entities and authorised officers. These features of the DAT Act limit administrative discretion and therefore the ability to develop and adapt the accreditation

[100] Submission 53, Services Australia, pg 3.
[101] Submission 53, Services Australia.
[102] See for example, Submission 19, Department of Home Affairs; Submission 16, Department of Education; Submission 60, University of Sydney; Submission 62, University of Western Australia.
[103] Submission 45, PHRN; Submission 56, Universities Australia; Submission 55, South Australian Department for Health and Wellbeing.
[104] An example of a duplicative process is the current separation of user and ADSP accreditation assessments and decisions. Entities accredited as ADSPs are required to meet higher capability thresholds relative to accredited users. Despite this the DAT Act requires separate applications and assessments for accreditations of ADSPs and users. Entities that are accredited as ADSPs but not users are able to handle data under the DAT Act for another party but are not able to request and use that same data.
[105] In this context, a risk-based approach to accreditation explicitly aligns accreditation requirements with applicant use-cases, therefore more closely balancing the need to maintain rigor in the accreditation process with regulatory load on participants (Submission 9, ABS, pg 4).

framework to flexibly respond to the needs of data sharing participants and changes in the broader data system.

Accreditation and its alignment with participant use-cases

258. Submissions to the Review identify the separation of uniformly applied accreditation standards from data sharing use-cases as problematic.[106] Further, there is a view among stakeholders that user and ADSP accreditation is applied on a one-size-fits-all basis. This has likely limited accreditation uptake among:

- smaller organisations who may not be able or willing to bear the costs of engaging with the accreditation process
- organisations which self-select away from applying for accreditation due to their limited data capability, and
- organisations with narrow data sharing use-cases (for example, those who intend to access a limited set of de-identified data assets through a third-party secure access service for research purposes).

259. The perception of a uniform accreditation does not reflect how it has been implemented. In practice, the National Data Commissioner has recognised organisational differences through accreditation 'conditions', which limit the actions that accredited entities can perform when engaged in data sharing, consistent with Part 5.2 Division 2 of the DAT Act.[107] A relatively common and straight forward condition has been applied to entities that do not intend to use or store data on their own ICT networks. This condition requires entities who intend to access data under the DAT Act to use a secure access service provided by an ADSP. This condition, being so commonplace, is featured in the ONDC 'Sample User Application' form (Office of the National Data Commissioner (ONDC) 2022, pg 25).[108]

260. The divergence between this practice and participant perceptions reflects a problem with the accreditation process. Although the current approach to moderating accreditation is functional, it is effectively backwards in that it sets high overarching standards that are then moderated down on a case-by-case basis.

261. Submissions to the Review support a more explicit approach to accreditation conditions under which more information (including guidance, rules, and/or codes) could be made available to prospective applicants on accreditation parameters up-front and to better balance ease of access with regulatory burden.[109]

262. Explicit accreditation 'tiers' have also been proposed in several submissions as a mechanism which would assist in more closely aligning accreditation requirements with

---

[106] Submission 9, ABS.
[107] Submission 18, National Data Commissioner.
[108] The commonality of this condition is unsurprising given the objectively low cyber security capability of the average entity eligible for user accreditation. To illustrate this point, an Australian Signals Directorate 2024 report on the Commonwealth's cybersecurity posture identified that 'the proportion of government entities that reached overall Maturity Level 2 across the Essential Eight mitigation strategies has declined. In 2024, 15 per cent of all entities reached overall Maturity Level 2, decreasing from 25 per cent in 2023' (Australian Signals Directorate, 2024, pg 2).
[109] Submission 18, Department of Health, Disability, and Ageing; Submission 48, Psithur; Submission 13, Australian Research Data Commons; Submission 7, Australian Academy of Science.

data sharing use-cases.[110] Accreditation tiering makes explicit the basis for accreditation on a continuum from, for example, 'highly conditional' to 'full' or 'unrestricted' accreditation. This not only facilitates entry to accreditation applicants with varied levels of data maturity but also sets the bounds for the negotiation of data sharing arrangements post-accreditation.

263. Specifically, tiering would provide applicants with greater clarity, at the outset, on which 'tier' of accreditation aligns most closely with their data sharing needs, and has the potential to substantially reduce the burden of the application process, through for example, the expedition of 'lower tier' accreditation assessments. From a data system perspective, feedback received from the Trusted Entities program, in-particular, support such a refinement and streamlining of DAT Act accreditation. The Program identifies that both an 'accredit once, use many times' approach and an alignment of accreditation standards with data sharing use cases is critical to enabling more effective national data sharing.

Organisation-level accreditation

264. The DAT Act applies accreditation at the organisational level. Accreditation at the organisational level may not be suitable in instances where applicants seek accreditation for dedicated units within a larger organisation. Further, most large organisations eligible for accreditation have several functionally separate units, many of which may seek to obtain accreditation status independently of one another. For example, a state or territory health department typically includes hospital networks, system-wide health services, and research and policy units. Individual business units within such departments tend to have their own specific data requirements, and possibly independent governance. If two or more units of such an organisation are granted accreditation, their accreditation status *must* be managed through conditions applied at the department level accreditation.

265. Organisational level accreditation also limits the autonomy of organisational sub-units (such as data units) and has downstream implications on accreditation continuity in the case of organisational restructures. A case-in-point is the recent experience of the disruption to DAT Act accreditation brought about by machinery of government changes impacting the ACT Government:

> Whilst the accreditation process itself tests the broader data and related capabilities in an organisation, the accreditation, once obtained, is linked to a legal entity due to the restrictions in the DAT Act. This means that when machinery of government (MoG) changes are enacted and entities are moved between units, they are required to re-apply for accreditation – there is no transfer of accreditation process that accounts for MoGs. This restriction is currently impacting the ACT – the unit currently accredited with the ONDC is transitioning into a new legal entity (Digital Canberra) from 1 July 2025 through a MoG change. Given the relative frequency of MoG changes within the Commonwealth and state and territory governments, this represents an example of where legislation can result in unintended and burdensome consequences.[111]

[110] Submission 13, Australian Research Data Commons; Submission 48, Psithur; Submission 33, Medical Software Industry Association Ltd; Submission 30, James Cook University.
[111] Submission 1, ACT Government, pg 4.

266. The above scenario occurs regularly and is an issue not only for the accreditation status of organisations experiencing a restructure, but also for the continuity of data sharing arrangements.[112]

Authorised officers and eligible entities

267. Submissions to the Review have outlined a number of cases where the prescriptive and complex definitions of authorised officers and eligible entities in the DAT Act have caused undue delays and complications in the accreditation process. The definitions, although functional for the purposes of identifying organisations with 'standard' features, take limited account for the diversity of structures, and accountabilities among other organisation's eligible for accreditation.[113] This has been particularly problematic for certain Commonwealth bodies such as Jobs and Skills Australia (a Secondary Statutory Authority) when attempting to apply for accreditation. Jobs and Skills Australia identify how both the prescriptive entity and authorised officer definitions have hampered attempts at obtaining accreditation:

> JSA is a Secondary Statutory Authority operating alongside the Department of Employment and Workplace Relations. JSA has been seeking to become an Accredited User and participate in data sharing under the DAT [Act] but are currently clarifying legal questions which have delayed our onboarding. The DEWR Chief Data Officer has submitted DEWRs response to the Review and our response should be read in conjunction with this.
>
> JSA is established under section 6 of the Jobs and Skills Australia Act 2022 (JSA Act). However, section 8 of the JSA Act provides that JSA is part of DEWR for the purposes of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act). JSA also meets part (a) of the definition of 'prescribed authority' in the Freedom of Information Act 1982, and not parts (c) or (d) of the definition. Therefore, none of the entity types listed in Section 137(1) of the DAT Act apply to JSA.
>
> As such, JSA is not able to appoint an Authorised officer under the DAT Act. Responsibility for operating within the bounds of the DAT Act would require DEWR to perform those functions on JSA's behalf, which creates a potential conflict of interest since DEWR and JSA are separate entities for DAT Act purposes (e.g. if DEWR were to request data from JSA under the DAT Act.[114]

268. The above does not align with the objects of the DAT Act; having the potential to undermine safe data access and use through assigning accountabilities which may be inconsistent with an accredited entities organisational structure as well as unnecessarily restricting or prohibiting otherwise reasonable accreditation decisions. Prescriptive eligible entity definitions have also unnecessarily prevented select Australian universities from obtaining accreditation, which again, is inconsistent with the objects of the DAT Act.[115]

---

[112] Submission 38, National Data Commissioner.
[113] Submission 17, Department of Employment and Workplace Relations; Submission 38, National Data Commissioner.
[114] Submission 31, Jobs and Skills Australia pg 1.
[115] Submission 56, Universities Australia.

Recommendation 5

The DAT Act should establish a permissions-basis for accreditation which replaces the current strict 'user' and 'data service provider' accreditation designations.

269. The Review recommends replacing the existing user and ADSP accreditation designations with a single 'accredited entity' designation. This recommendation solves for multiple problems, including reducing the complexity of data sharing processes under the DAT Act. Currently, data sharing under the DAT Act is conceived as an activity that is both linear and tractable, involving data being provided by a data custodian either:

- directly to an accredited user, or
- indirectly to an accredited user through an ADSP which either transforms the data (through the provision of de-identification, complex data integration and/or data linkage services) or provides access to data on a secure access platform.

270. Although this form of data sharing is appropriate for simple cases, complexities arise when data sharing participants perform multiple roles within a data sharing process, such as is the case when provisioning data into, developing, and providing access to integrated data assets.

271. As an alternative, the Review proposes accreditation based on 'actions' that an accredited entity is permitted to perform in a data sharing project, where actions are broadly categorised into 'access and use' and 'data services'. Consolidating the user and ADSP roles into a singular 'accredited entity' designation assists with a more principles-based and less prescriptive design for the DAT Act. This is intended to better enable data custodians and accredited entities to design data flows in a manner which suits their requirements without needing to 'switch' roles within a data sharing process.

Application and assessment processes

272. Although transitioning to permissions-based sharing does not impact the underlying basis for DAT accreditation, implementation will require changes to accreditation guidance and application forms. A permissions-basis for accreditation is also expected to result in a more efficient application and assessment process.

273. It is anticipated that entities seeking accreditation to perform one or more data services under the DAT Act would also be automatically granted accreditation to access and use data, given the higher data capability requirements and thresholds applicable to data service provision. Currently, the DAT Act requires separate accreditation applications and assessments of ADSPs and users. This means that entities accredited as ADSPs but not users are permitted to perform services on data on behalf of a third party but are unable to use or access that data (which would require user accreditation).

Recommendation 6

Explicit accreditation categories should be introduced to more simply reflect the application of different accreditation standards and to facilitate alignment between accreditation and data sharing use-cases.

274. The Review recommends the introduction of accreditation categories which incorporate the set of possible actions entities can be accredited to perform in relation to both data use and data service provision (Recommendation 5).[116]

275. Recommendation 6 intends to address the view that DAT Act accreditation is inflexible and one-size-fits-all by 'front-ending' the accreditation options available to prospective applicants. This recommendation could be implemented through a publicly available matrix.

276. An example of such a matrix is presented in Table 4, although implementation of Recommendation 6 will ultimately require considered engagement with data custodians, accredited entities and other experts. Further, the Review recommends that accreditation categories are implemented non-legislatively, consistent with the existing principles-based spirit of accreditation assessment; ensuring that it can be adjusted over time with changes in accreditation eligibility and data system standards more broadly. An example of 'data system standards' include those investigated by the Trusted Entities program. The Program recommends that DAT Act accreditation, as an established assurance mechanism, is leveraged to support national data sharing. Therefore, a non-legislative implementation of accreditation categories allows DAT Act accreditation to remain flexible and relevant in its support of national data sharing initiatives.

[116] Based on feedback received in response to the Draft Findings and Recommendations paper, the Review has modified Recommendation 6, replacing the reference to 'accreditation tiers' with 'accreditation categories'. Given the term accreditation 'tiers' may imply that there are 'quality' or 'value' differences among the categories of accreditation, it is the Reviews position that this change in phrasing more closely reflects the intent of Recommendation 6—improved alignment of accreditation standards with data sharing use cases.

Table 4: Proposed accreditation categories

i. Accreditation categories (permitted actions)

Permission	Data	Storage	Other
Access and Use			
De-identification services			
Data curation services[117]			
Complex data integration services			
Secure access services			

ii. Accreditation parameters

Parameter	Sub-category		
Data	Capability to access and use identifiable person-level data at the unit record level	Capability to access and use de-identified person-level data at the unit record level	Capability to access and use de-identified personal data, at the aggregate level
Storage	Data held and accessed on own IT system	Data held and accessed through an accredited third-party secure access service	Not applicable
Other	Only personnel in specific business areas can access or perform services on data	Only specific IT systems can store data	Others (case-by-case)

Table 4 explanation:

Part i of Table 4 presents a generalised example of accreditation categories which could be implemented, consistent with Recommendation 6. Accreditation categories specify permitted actions that entities may be accredited to undertake. The shades of blue identify general sub-categories that entities could be accredited against, with a greater span of permitted actions able to be performed by entities with accreditation for categories with a darker shade relative to those with a lighter shade.

The general standards which underpin the sub-categories in Part I are expanded on in Part ii of Table 4. In Part ii , *Permission* identifies the general action(s) an entity is accredited to perform and *Data*, *Storage*, and *Other* are the parameters for accreditation.

Part i of Table 4 could be considered as a high-level publicly available reference point for use by both data custodians and prospective accreditation applicants when considering the alignment of accreditation status with data sharing use-cases.

Part ii of Table 4, on the other hand, provides examples of the possible standards of capability required for accreditation against each of the sub-categories and which underpin the determination of accreditation categories identified in Part i of Table 4. These sub-categories would be the main pillars which form the basis for accreditation application forms and the accreditation assessment criteria.

[117] See Recommendation 10.

Additional notes:

An entity's capability with respect to data management and governance (paragraph 77(1)(a)), and the skills and capability of personnel (paragraph 77(1)(c)) are taken as mandatory (threshold) requirements for all accreditation types with no gradations (and therefore do not feature in Table 4).

If an entity is accredited to perform complex data integration and/or secure access services they will require assessment against the higher standards of access and use of identifiable person-level data at the unit record level, and storage of data on own IT systems with no gradations. This is why the *Data* and *Storage* categories against the *Complex data integration services* and *Secure access services Permissions* are completely shaded in dark blue in Part i of Table 4.

For the provision of de-identification and/or data curation services, there *may* be gradations of *Data* and *Storage* parameters in certain circumstances. This could occur where the de-identification and/or data curation services are performed by personnel of the accredited entity within the data custodians IT environment (and therefore there is no movement and/or third-party storage of data).

277. The Review considers that accreditation categories could be implemented in a way that streamlines new accreditation applications without adversely disrupting existing accreditation arrangements. Since the proposed categories align with existing accreditation conditions, current accreditations can be mapped to this new model. The only addition, if adopted, is the granting of data 'Access and Use' permission to existing entities accredited to provide data services (as outlined in Table 4).

278. The transition to a model which categorises accredited entities would have several benefits, in addition to informing prospective applicants of their accreditation options. These include:

- providing a point of reference to facilitate the fielding of data sharing requests and/or the negotiation of agreements
- supporting transparency measures proposed in Recommendation 7
- providing a basis for the application of procedural rights for accredited entities that request data (in support of Recommendation 3 and 4), and
- enabling more effective national data sharing through greater consistency and transparency on the application of accreditation standards, in line with the priorities of the Trusted Entities program.

Recommendation 7

Transparency and other measures which promote greater regulatory flexibility in respect of DAT Act accreditation should be introduced and have consideration to broader developments in the data system.

Accreditation transparency

279. Submissions to the Review note there is limited publicly available information on accreditation standards and the evidence requirements that underpin those standards.[118] Although the ONDC continues to work closely with its stakeholders to foster greater trust

[118] Submission 9, ABS; Submission 53, Services Australia.

in accreditation (such as 'Accreditation Profiles'), the Review recommends that these efforts be accelerated and formalised (ONDC 2024; ONDC 2025).

280. To this effect, the Review proposes the introduction of transparency measures for accreditation, including:

- detailed guidance on the reasons for which accreditation decisions are based
- approved form/s for accreditation applications, and
- rules to prescribe evidence requirements that support the criteria for accreditation and which prescribe conditions of accreditation for classes of entities.

281. Such measures set the foundation for greater trust and awareness of the evidence basis for accreditation generally, in addition to supporting the implementation of Recommendations 3 and 4. In the longer run, greater transparency empowers stakeholders to peer review and advise on accreditation standards. Further, greater use of rules would enable standards to be refined with evidence requirements for specific classes entities and facilitate the proposed expansion of accreditation eligibility (Recommendation 8).

Greater administrative discretion

282. The Review recommends the eligible entity (section 9) and authorised officer (section 137) definitions be generalised, and greater regulatory powers be granted to the National Data Commissioner.

283. These changes would enable more efficient and flexible consideration of issues relating to entity definitions, transitional arrangements, and authorisations. The existing definitions have limited otherwise eligible entities from obtaining accreditation, and/or resulted in the perverse allocation of decision-making accountability in respect of data sharing.[119]

284. Further, the DAT Act does not allow for the flexible administration of transitional accreditation arrangements for entities experiencing restructures including machinery of government changes.[120] Currently, if an accredited entity experiences a restructure where, for example, sub-units are moved between legal entities, this requires the affected entity to reapply for accreditation. The Review therefore recommends the National Data Commissioner be granted additional powers to empower them to take reasonable actions to manage accreditation.

Participation and data sharing purposes

Not-for-profit users of public sector data

285. Currently eligibility to obtain DAT Act accreditation is limited to Commonwealth, state, and territory government bodies, and Australian universities. In contrast, public sector bodies routinely share restricted data outside of the DAT Act with other organisations.

[119] Submission 17, Department of Employment and Workplace Relations; Submission 31, Jobs and Skills Australia; Submission 38, National Data Commissioner; Submission 56, Universities Australia.
[120] Submission 1, ACT Government; Submission 38, National Data Commissioner.

These include ACCOs, not-for-profit research institutes, and not-for-profit service delivery organisations.

ACCOs

286. ACCOs are legally incorporated not-for-profit entities initiated, governed, and operated by First Nations communities for the delivery of community services (Coalition of Peaks and Council of Australian Governments 2020).

287. Their core purpose is to deliver culturally safe, holistic, and locally responsive services to First Nations communities. Examples of services provided include health services (such as primary healthcare, mental health, and prevention services), child and family services (including supporting child protection, family, and early intervention programs), education and employment services, and housing and justice services (including housing assistance, legal aid, and justice reinvestment) (Government of Western Australia 2022).[121]

288. Approximately half of First Nations people access primary health care through ACCOs, which has contributed to improved immunisation rates and chronic disease management, particularly in remote areas (AIHW 2016). ACCOs are also significant employers in First Nations communities, often hiring predominantly Aboriginal and Torres Strait Islander staff which reinvest their wages in local economies (Mackean et al. 2025).

Not-for-profit research institutes

289. Not-for-profit research institutes are organisations dedicated to advancing knowledge and innovation for public benefit (Australian Charities and Not-for-profits Commission (ACNC) 2025). Australia's not-for-profit health and medical research institutes alone directly employ approximately 32,000 people (in high-value, knowledge-intensive occupations), with a further 78,000 people supported in related industries such as medical technology and pharmaceuticals (KPMG 2018a). The 2018 Economic Impact of Medical Research in Australia Report, prepared for the AAMRI, found that past Australian medical research (1990–2004), much of which was performed by not-for-profit research institutes, yielded an estimated net present value benefit of approximately $78 billion from a net present cost of $20 billion.[122]

Not-for-profit service delivery organisations

290. Not-for-profit service delivery organisations are entities which provide a range of services for public benefit (ACNC 2025). Many of these services involve significant government funding. Not-for-profit service providers make significant contributions to the Australian economy through service delivery, employment, and innovation. For example, the aged care sector, 42 per cent of which consists of non-for-profit providers,

[121] Clause 44 of the National Agreement on Closing the Gap defines ACCOs as (Coalition of Peaks and Council of Australian Governments 2020, pg. 8):

a. incorporated under relevant legislation and not-for-profit;
b. controlled and operated by Aboriginal and/or Torres Strait Islander people;
c. connected to the community, or communities, in which they deliver the services;
d. governed by a majority Aboriginal and/or Torres Strait Islander governing body'.

[122] Approximately two-thirds of gains were improved health outcomes for Australians, and one-third were identified as economic gains derived from increased productivity and research commercialisation (KPMG 2018).

contributes approximately $17.6 billion to the Australian economy annually (1.1 per cent of GDP) (Aged & Community Services Australia 2021; Centre for International Corporate Tax Accountability and Research 2020). Further, PHNs manage over $1 billion in federal funding annually which supports the administration of local health services (Department of Health 2018).

Expansion of accreditation eligibility

Finding 7

Expanding DAT Act accreditation to include ACCOs, not-for-profit research institutes, and not-for-profit service delivery organisations would enhance the value derived from public sector data sharing. Nevertheless, such expansion should be balanced with careful consideration of both the mechanisms available to support the participation of new entrants and preserving public trust and social license in the data system.

291. There is a consensus view that the restrictions on accreditation eligibility significantly limit potential whole-of-society benefits accruing from public sector data sharing. Feedback from stakeholders, in general, support the expansion of DAT Act accreditation eligibility,[123] although there are varying views on the extent of expansion, its timing, and the enabling factors required to facilitate its success. The Review finds that expanding DAT Act accreditation eligibility to ACCOs, not-for-profit research institutes, PHNs, and not-for-profit service delivery organisations is necessary to:

- meet the objective of improved government service delivery
- strengthen the public benefits that can flow from the DAT Act
- improve consistency with existing (non-DAT Act) data sharing between the Commonwealth and not-for-profit sectors, and
- support the Commonwealth's commitment to the National Agreement on Closing the Gap.

292. These types of organisations have demonstrated capacity to use data to deliver value in the public interest. Leading organisations and networks in these sectors already work in partnership with Commonwealth, state and territory governments, and Australian Universities, are often wholly or partially funded by them, and are critical to the delivery of public policy, research and innovation, and government services.

Not-for-profit research institutes

293. Submissions to the Review call for expansions to accreditation eligibility to include not-for-profit research institutes, with arguments for specific not-for-profit research institute types generally reflecting respective stakeholder interests. The PHRN, for example, supports extending accreditation eligibility to include 'not-for-profit research

[123] Exceptions include, for example the views expressed by Monash University, who although not completely against the expansion of accreditation eligibility, consider that that expansion should be phased; ensuring that the data sharing system established by the DAT Act is functional *before* other organisation-types are made eligible for accreditation (Submission 36, Monash University).

institutes and (health centric) quality assurance bodies'.[124] Further, the PHRN presents the Sax Institute as an example of a highly capable independent research institute and provider of trusted linkage services which is currently ineligible for accreditation under the DAT Act; emphasising that the absence of such organisations limits the potential of the DAT Act to enable national data sharing.

294. Submissions to the Review further argue that excluding not-for-profit research institutes prevents collaboration with data custodians, not just for academic research, but in implementing critical government policies and programs.[125] The AAMRI submission includes a case study of the Murdoch Children's Research Institute-led Generation Victoria (GenV) project, which is further expanded on in Box 1.[126] This case study provides a concrete example of how the current exclusion of not-for-profit research institutes from accreditation under the DAT Act necessitates accessing Commonwealth data through non-DAT Act means which are characterised as 'time consuming and costly'.[127] Further, excluding such organisations limits the DAT Act's ability to facilitate collaborative data sharing between the Commonwealth and not-for-profit research institutes.[128]

295. Box 2 presents the Sax Institute's 45 and Up Study as an example of the value that can be derived from the sharing of public sector data with not-for-profit research institutes.

[124] Submission 45, PHRN, pg 7.
[125] Submission 5, AAMRI.
[126] The GenV project, led by the Murdoch Children's Research Institute, is a whole-of-state longitudinal research initiative which aims to recruit and track over 150,000 children born between 2021 and 2023 and their parents to improve health and wellbeing outcomes across Victoria (Hughes et al. 2025). GenV collects extensive data and biosamples to explore links between genetics, environment, and health, enabling faster, more inclusive research into conditions such as mental illness, obesity, allergies, and developmental challenges (Victorian Department of Jobs, Skills, Industry and Regions 2024).
[127] The case study continues to elaborate on the process of obtaining project-specific Public Interest Certificates to enable access to protected data, linkage requirements, and obtaining access and use permissions (Submission 5, AAMRI).
[128] Submission 5, AAMRI; Submission 1, ACT Government; Submission 9, ABS; Submission 18, Department of Health, Disability, and Ageing; Submission 27, Indigenous Data Network; Submission 38, National Data Commissioner; Submission 45, PHRN; Submission 51, Research Australia; Submission 52, Seer Data & Analytics, Greater Shepparton Lighthouse Project and Maranguka Community Hub; Submission 38, University of Melbourne.

Box 2: The Sax Institute's 45 and Up Study

The Sax Institute's 45 and Up Study is Australia's largest longitudinal study of ageing, surveying over 250,000 adults aged 45 and over in New South Wales. The Study, established in 2005, consists of baseline survey data (2005-2009), and two additional follow-up surveys (2012-2015 and 2018-2020), of New South Wales residents over the age of 45 randomly sampled form the Medicare Australia enrolment database. The survey consists of questions designed to capture demographic, personal health behaviour (for example tobacco and alcohol use), and general health-related data. The 45 and Up Study combines this survey data with linked government administrative data to generate policy-relevant health research. When surveyed individuals enrolled in the Study, they consented to allow data linkage with other administrative data sources. Routine data linkage with administrative datasets is performed by the NSW Centre for Health Record Linkage who maintains a Master Linkage Key of the study participants (Bleicher et al. 2023).

The study provides key insights on the impact of socioeconomic and lifestyle factors on cardiovascular disease outcomes and have been used by more than 50 government and non-government organisations to inform the production of health guidelines, prevention programs and legislative change, including those relating to tobacco control measures (Paige et al. 2022).

Not-for-profit service delivery organisations

296. Submissions to the Review suggest that the exclusion of not-for-profit service delivery organisations has affected the extent to which government-held and government-funded data can be utilised. This exclusion has also impacted the availability of data custodians to access growing (and in many cases more advanced) expertise to support the delivery of government services.[129] Therefore, submissions to the Review identify broad support for expanding accreditation eligibility to not-for-profit service delivery organisations, including, for example, Approved Aged Care Providers and PHNs.

297. The operations of Approved Aged Care Providers are regulated by the Aged Care Quality and Safety Commission which requires them to meet defined standards of service delivery. Failure to meet these standards has implications on a providers accreditation status and their eligibility to receive government funding. Although Approved Aged Care Providers, by virtue of their accreditation against the Aged Care Quality Standards, maintain relatively sophisticated governance and operations, there are limited publicly available indicators of their data capability. DAT Act accreditation eligibility may, therefore, provide both an avenue for such organisations to demonstrate their data capability, and may also support the implementation of ongoing data and digital reforms of the aged care sector following the 2021 Royal Commission into Aged Care Quality and Safety (Royal Commission into Aged Care Quality and Safety 2021; Department of Health 2021).

298. Similarly, PHNs, which are independent organisations wholly funded by the Australian Government, perform three principal purposes, namely:

[129] Submission 9, ABS; Submission 38, National Data Commissioner; Submission 52, Seer Data & Analytics, Greater Shepparton Lighthouse Project and Maranguka Community Hub; Submission 56, Universities Australia.

- coordinate and integrate local health care services in collaboration with Local Hospital Networks to improve quality of care, people's experience and the efficient use of resources
- commission primary care and mental health services to address population health needs and gaps in service delivery and to improve access and equity
- capacity-build and provide practice support to primary care and mental health providers to support quality care delivery (Department of Health, Disability, and Ageing 2025).

299. There are 31 PHNs across Australia that operate in concert with local hospital networks; maintaining sophisticated data functions which are deployed for the purposes of establishing citizen health requirements, service resourcing, and health service coordination in their constituent region(s) (Department of Health, Disability, and Ageing 2025). Box 3 discusses the use of public sector data to support the delivery of the NSW Lumos program.

Box 3: The NSW Lumos Program

The Lumos program is a New South Wales-based collaboration between the NSW Ministry of Health, the South Western Sydney PHN, and general practices. The Program links anonymised general practitioner patient records with public hospital data. The Lumos data asset is strictly used for the 'planning, monitoring, funding and evaluation of health services', which includes the provision of customised reports to general practitioners and PHNs on the health characteristics of the patients in their care (NSW Health 2025).

ACCOs

300. There is strong and consistent support for expanding DAT Act accreditation to include ACCOs.[130] In addition, the Review considers the current exclusion of ACCOs from accreditation to be inconsistent with securing outcomes under the Framework for Governance of Indigenous Data, and by extension, Priority 3 and 4 of the National Agreement on Closing the Gap.

301. Given the services typically provided by ACCOs, opportunities for greater access to public sector-held data on individuals in-community would greatly enhance their effectiveness and broadly progress efforts at addressing Priority Reform 3 and 4 of the National Agreement on Closing the Gap. However, the Review considers that DAT Act accreditation eligibility is necessary but insufficient for facilitating better participation and outcomes for ACCOs in the data system. Specifically, the Review notes the requirement for resourcing and supporting mechanisms to ensure that ACCOs, if made eligible for accreditation, are *practically* capable of attaining and using this status to enable access to and use of public sector data (Recommendation 12).

[130] See for example, Submission 1, ACT Government; Submission 9, ABS; Submission 20, Department of Industry, Science and Resources; Submission 27, Indigenous Data Network; Submission 35, Melbourne Institute of Applied Economic and Social Research; Submission 38, National Data Commissioner, Submission 40; National Indigenous Australians Agency (NIAA); Submission 52, Seer Data & Analytics, Greater Shepparton Lighthouse Project and Maranguka Community Hub.

302. Box 4 presents outcomes from the Maranguka Justice Reinvestment Project; an ACCO-led project which accessed public sector data to support improved justice outcomes for the community of Bourke, NSW.

Box 4: Maranguka Justice Reinvestment Project

The Maranguka Justice Reinvestment Project was the first significant justice reinvestment project in Australia and commenced in 2014 as a pilot to support the community of Bourke, NSW. The Project accessed NSW government police and court data to design community-led interventions aimed at reducing crime and community member encounters with the NSW justice system. Between 2014 and 2017 domestic violence incidents and juvenile charges in the Bourke community decreased by 23 per cent and 38 per cent, respectively and the Year 12 retention increased by 31 per cent (KPMG 2018b). The Maranguka Justice Reinvestment Project has since been heralded as a model for other communities and demonstrates that when ACCOs have access to relevant government data and the opportunity to contribute to decision-making on matters impacting their community, they can deliver solutions that make communities safer, stronger, and less reliant on costly government interventions (Bryant and Spies-Butcher 2022).

For-profit service delivery, research, and other sectors

303. Some submissions to the Review advocate for broader expansion of accreditation eligibility to include the 'private sector' generally. The Review notes that not-for-profit organisations operate in both public and private sectors and therefore classifying entities as 'public' and 'private' for the purposes of accreditation eligibility expansion is ambiguous.

304. Instead, the Review has considered entities through the lens of for-profit and not-for-profit, therefore distinguishing them, at a base-level by their 'principal objective' (Australian Accounting Standards Board, 2021, p. 5). The Review finds significant support for expanding eligibility to a variety of private sector entities who act independently of government but who also have a principal objective of providing community or social benefit. Some submissions to the Review advocate explicitly for expanding accreditation eligibility to commercial organisations,[131] while there are others who consider that *all* organisation-types should be eligible for DAT Act accreditation. The latter position proposes that if an entity can meet the standards for DAT Act accreditation they should be able to participate, noting that the *purposes* for sharing data should be the primary concern for data sharing and not the organisation-type of the data requestor.[132]

305. While there are some arguments for extending accreditation eligibility to commercial organisations, the Review considers that eligibility must be balanced with the broader priority of continuing to build and maintain social license and community trust in public sector data sharing (OAIC 2018). Public sector data, including data on citizens health, education, welfare, and taxation characteristics is routinely collected compulsorily. This creates a unique responsibility on Government to ensure that the primary and secondary use of this accumulated data aligns with public expectations and values. The

[131] See for example, Submission 2, ANDHealth.
[132] Submission 79, PHRN; Submission 13, Australian Research Data Commons.

Review considers that this Government responsibility, as it relates to the possible expansion of accreditation eligibility to cohorts of commercial organisations, may be best exercised in discrete stages (consistent with Recommendation 9).

The timing of participation expansion

306. Although only some submissions to the Review outline how expanded accreditation eligibility should be implemented, support was provided for a 'staged process' dependent on the continued maturation of the DAT Act and the implementation of other changes arising from the Review.[133] The National Data Commissioner proposes a staged approach through the following mechanism:

> Eligibility could be built out in a flexible manner with suitable checks, such as Parliamentary scrutiny. Advice from the National Data Commissioner (taking advice from the National Data Advisory Council) could be provided to the Minister, who would then act on this advice to decide whether or not to expand the Act to certain types of entities through a disallowable legislative instrument (such as a Ministerial determination/rule).[134]

307. This option would involve a Ministerial power that could be used to expand accreditation over time, rather than exhaustively prescribing additional eligible organisation-types in the primary legislation. In contrast, the PHRN indicate that caution should be exercised when considering such an approach as:

> Expanding the categories of entities that are eligible to participate in the Scheme in a piecemeal fashion has the potential to create unnecessary, definitional complexities that may inadvertently exclude the same or similar types of entities from being able to access data under the Act as a result of specific governance, incorporation, or funding arrangements.[135]

Recommendation 8

The entities that can seek accreditation to request and use data under the DAT Act should be expanded to include ACCOs, not-for-profit research institutes (including independent research organisations and medical research institutes), PHNs, and not-for-profit service delivery organisations (including Approved Aged Care Providers).

308. The Review considers that expanded DAT Act accreditation eligibility is appropriate and necessary to ensure the composition of entities eligible for DAT Act accreditation:

- reflects current (non-DAT Act) public sector data sharing practices, and
- captures the breadth of unmet demand for access to and use of Commonwealth data in the public interest.

Defining additional eligible entities

309. The Review considers the proposed refinements of DAT Act accreditation arrangements (Recommendations 5, 6, and 7) coupled with the maturity and

[133] Submission 36, Monash University; Submission 44, Office of the Victorian Information Commissioner.
[134] Submission 38, National Data Commissioner, pg 9.
[135] Submission 79, PHRN, pg 8.

demonstrated robustness of current-state DAT Act accreditation is sufficient to support the practical implementation of Recommendation 8.

310. Nevertheless, the Review recommends the *general* identification and defining of ACCOs, not-for-profit research institutes, and not-for-profit service delivery organisations in the primary legislation, to ensure that the pitfalls and complications caused by existing prescriptive DAT Act eligible entity definitions are not repeated. General eligible entity definitions will be supported by greater administrative discretion being provided to the National Data Commissioner (see Recommendation 7).

311. To assist implementation, the following provides an outline of common legal characteristics of ACCOs, not-for-profit research institutes, and not-for-profit service delivery organisations.

312. ACCOs are defined in clause 44 of the National Agreement on Closing the Gap (Coalition of Peaks and Australian Governments 2020, pg. 8):

> Aboriginal and Torres Strait Islander community control is an act of self-determination. Under this Agreement, an Aboriginal and/or Torres Strait Islander Community-Controlled Organisation delivers services, including land and resource management, that builds the strength and empowerment of Aboriginal and Torres Strait Islander communities and people and is:
>
> a. incorporated under relevant legislation and not-for-profit
>
> b. controlled and operated by Aboriginal and/or Torres Strait Islander people
>
> c. connected to the community, or communities, in which they deliver the services
>
> d. governed by a majority Aboriginal and/or Torres Strait Islander governing body.

313. ACCOs can take various legal forms and may be incorporated associations or companies limited by guarantee (CLGs) under the *Corporations (Aboriginal and Torres Strait Islander) Act 2006* (Cth) (CATSI Act). Further, ACCOs are often registered charities (which require an ACCO to both meet the definition of a charity under the *Charities Act 2013* (Cth) and demonstrate its compliance with governance standards as determined by the ACNC), and/or registered with the Office of the Registrar of Indigenous Corporations under the CATSI Act.

314. Not-for-profit research institutes (established independently of the government or university sectors) are most often structured as CLGs and registered as charities under the *Charities Act 2013* and as Deductable Gift Recipients for the purposes of accessing philanthropic and grant funding, as well as tax concessions. In some cases, not-for-profit research institutes may be established by specific legislation or royal charter.[136] Not-for-profit research institutes are typically governed by boards of eminent researchers and community leaders which allocate funding received to the delivery of research for public benefit, including for the generation of knowledge, innovation, and solutions within their research domain.

315. Not-for-profit service delivery organisations are similar in legal structure to not-for-profit research institutes insofar as they are also commonly structured as CLGs,

[136] For example, the Garvan Institute of Medical Research is established by the *Garvan Institute of Medical Research Act 1984* (NSW), and the Australian Academy of Science operates under its original Royal Charter of 1954.

registered as charities and Deductable Gift Recipients, and may be established and/or approved under relevant legislation.

Facilitating expanded accreditation eligibility

316. The Review acknowledges that expanding accreditation eligibility should be coupled with investments which support capability uplift.[137] To this effect, implementation efforts should closely consider the need for focused supporting mechanisms for new entrants, including through appropriate guidance, developing communities of practice, and considering accreditation conditions for cohorts of organisations to support participation.

317. To enable effective ACCO participation, the Review considers the submission by the NIAA to the Draft Findings and Recommendations as providing a comprehensive and appropriate set of supporting mechanisms. Chief among these is the requirement for coordinated and focused consultation with ACCOs and other impacted First Nations organisations. To this effect, the NIAA suggest the following as 'critical enablers':

- Increase accessibility through inclusion of culturally appropriate and plain language knowledge documents and fact sheets. These would assist in uplifting capability and understanding of members of organisations applying for accreditation or otherwise interacting with the DATA scheme. This aligns with GID Guideline 2 to build data-related capabilities providing First Nations people with skills needed to actively participate in decision making around their priority issues.
- A simplified accreditation pathway. Some ACCOs have less immediate access to the skills needed to complete the accreditation process. A simpler accreditation pathway and practical support will help address Finding 6 that the accreditation process is resource intensive. This aligns with National Agreement on Closing the Gap Priority Reform 4.
- Capacity building through targeted funding, resources, and training. Training to provide an uplift in technical skills, data governance and data literacy skills to enable more ACCOs to participate in decisions and discussions as equal partners. This also includes access to technical infrastructure and ICT support required to participate in the DATA scheme. This aligns with National Agreement on Closing the Gap Priority Reforms 2 (Building the ACCO sector) and 4.
- Recognising the rights of First Nations people to control their data is a positive step towards self-determination that could be actioned through the redesign of data sharing agreements to reflect culturally safe data practices. Consideration needs to be given to ensuring both the personal and collective privacy of individuals and communities is respected in data sharing agreements.
- Balancing privacy should also consider decisions about who has control over access to culturally sensitive data.[138]

[137] Submission 83, University of Melbourne.
[138] Submission 76, NIAA, pp 1-2.

Recommendation 9

The DAT Act should include a power which allows the Minister to expand accreditation eligibility further, subject to advice from the National Data Commissioner (or other appropriate office or body with appropriate expertise).

The Review proposes a power to allow the Minister to expand eligibility beyond those identified in Recommendation 8. This will provide a mechanism for further expansions of DAT Act accreditation to specific entities or other cohorts or classes of entities. Such a power would support greater flexibility in enabling unforeseen data sharing use-cases in the public interest.

The basis for accreditation expansion decisions

318. The Review proposes that a public ministerial power be implemented to enable the Minister to grant DAT Act accreditation eligibility to specific organisations or classes/cohorts of organisations beyond the scope of eligibility established in the primary legislation. In Australia, the use of ministerial powers in legislation is commonplace and allow a Minister to determine or adjust the scope of regulated organisations. These powers are typically exercised through delegated powers (such as regulations, rules, or other statutory instruments), and supported by procedural safeguards, including requirements about pre-decision consultation and parliamentary scrutiny and disallowance.

319. The Review recommends the exercise of a Ministerial power be subject to a set of generally applicable considerations. These could include requiring the Minister to have regard to whether a proposed expansion to accreditation eligibility would:

- further the public interest (as distinct from national interest)[139]
- be consistent with the objects of the DAT Act, and
- not adversely or be seen to adversely impact public trust in relation to the ethical and acceptable use of public sector data.

320. Consistent with existing provisions, the proposed Ministerial power should be subject to transparency and consultation requirements, and to parliamentary scrutiny and disallowance.

321. This may include, for example, the requirement that public submissions be sought and analysed on any proposal to expand accreditation eligibility (detailed in an assessment report) and considered by the Minister with advice from the National Data Commissioner, and the Australian Information Commissioner, prior to a ministerial decision being made.

[139] National interest refers to the goals and ambitions of a sovereign state and which often encompasses national security, economic prosperity, and international standing, whereas public interest pertains to the welfare of the community or society as a whole, including considerations for individual rights, the common good, and the fair-minded treatment of all citizens (McLeod 2017; Wheeler 2006).

Data sharing purposes

322. Data sharing under the DAT Act is permitted for three purposes:

- delivery of government services
- informing government policy and programs, and
- research and development.

323. Sharing that is authorised by one of these purposes is also subject to other conditions, including the requirement for sharing to adhere to the public interest principle and meet standards of privacy and security. Importantly, the use of data for enforcement (compliance) and national security-related activities is prohibited.

324. 'Delivery of government services' includes activities such as providing information to individuals, facilitating access to public infrastructure and/or systems, determining eligibility for benefits, and making payments. Providing such services typically requires the sharing of personal information and therefore engages additional requirements such as the need to obtain individual consent. Nevertheless, the DAT Act allows the sharing of personal information without consent when data is used to *directly* deliver a service to individuals. Examples include issuing driver's licences, sending emergency alerts, or processing benefit applications.

325. 'Informing government policy and programs' refers to the use of data to support evidence-based decision-making across the policy lifecycle (including development, implementation, and evaluation), and 'research and development' involves investigative and analytical activities which generate new knowledge and/or result in the production or improvement of products, systems, and processes.

326. All data sharing projects must adhere to the five data sharing principles, including the project principle, which mandates that projects must reasonably be expected to serve the public interest (section 16). Further, all data sharing under the DAT Act requires the production and registration of a data sharing agreement (section 19). Together, the data sharing purposes and requirements for data sharing agreements establish the boundaries for data sharing under the DAT Act.

Data curation

327. The above purposes all rely on an end-use to be specified, which does not explicitly permit data custodians to unilaterally procure or undertake data curation. For the purposes of the Review, data curation is taken to be the active and ongoing management of digital data throughout its lifecycle to ensure its accessibility, quality, and long-term preservation. It includes a combination of technical and intellectual processes, including data selection, annotation, integration, documentation, and preservation, with the goal of enabling data reuse and supporting transparency and reproducibility (Johnston 2017).

328. Access to data curation services is particularly important for data custodians who maintain large amounts of potentially high-value (but often unstructured) administrative data to support their delivery of government services, but who also intend to make this data available for use by third parties to enable research and/or policy and program development. It is often the case that such data, although functional for enabling service

delivery, is not fit for use for secondary purposes. In other cases, data custodians obtain vast amounts of data in the course of providing government services, but lack the resources or expertise to leverage it effectively to support improved service delivery. Data custodians may also simply lack the expertise or capacity to curate data to appropriate standards to enable its reuse. This can adversely impact the number of possible Commonwealth-held data assets available (both 'open' and 'restricted') to be shared under the DAT Act and within the data system generally.

The intersection of government service delivery and enforcement-related purposes

329. The use of public sector-held data for service delivery is complex due to established legal constraints and privacy considerations. Further, the line between the use of data for service delivery and its inadvertent use for enforcement-related purposes is often unclear (or clearly prohibitive), which can prevent otherwise worthwhile data sharing activity.[140]

330. Typical intersections of data use for service delivery and enforcement-related activities are summarised in the following extract from a guidance note published by the National Data Commissioner discussing the DAT Act data sharing purposes (ONDC 2025):

> Enforcement and government service delivery can involve similar activities and the distinction depends on the specific circumstances of the proposed data sharing activity. Where data relates to a payment, a key distinction between service delivery and enforcement might be whether the activity occurs before or after the payment or service is provided. For example, using data about an individual to determine eligibility for a payment before the payment is made is not an enforcement related activity. However, using data to verify eligibility after a payment is made will likely constitute enforcement activity, particularly if that verification results in the recovery of overpayments and any enforcement action.

331. Here timing on the use of data, and inclusion of 'detection' as an enforcement-related activity adds complexity to the use of data for the delivery of government services under the DAT Act.

Improvements to the data sharing purposes

Finding 8

The current DAT Act data sharing purposes are generally appropriate, however improvements are needed to enable sharing for the purposes of data curation. The use of data for government service delivery under the DAT Act is complex and requires a recalibration of settings which balance the need for more simplified data sharing processes with privacy protections.

[140] The DAT Act prohibits the use of data for enforcement-related purposes. Examples of enforcement-related purposes include the use of data for the detection, investigation, and/or response to:
- 'offences or breaches of laws punishable by criminal or civil penalties, and
- acts or practices that harm public revenue (e.g. fraudulent benefit claims)' (ONDC 2025).

332. The Review finds the current data sharing purposes authorised by the DAT Act are broadly appropriate but could be improved.

333. Specifically, the DAT Act does not provide an intuitive model to support efforts at data curation and the creation of data assets without a specific end-use (and users) identified at the authorising stage of sharing. Further, the Review finds that the service delivery purpose is currently impeded by both extensive privacy protections in the DAT Act as well as the strict prohibition on the use of data for enforcement-related purposes. The intersection of data sharing for government service delivery and enforcement-related purposes is, in certain instances, ambiguous, which has impacted on the potential utility of government service delivery as a data sharing purpose under the DAT Act.

Data curation

334. There is broad support for including data curation as an approved data sharing purpose.[141] In particular, submissions to the Review comment on the important role data curation might perform in streamlining the future development and provision of access to high value integrated data assets.[142]

335. In contrast, the Information and Privacy Commission NSW argue that any extension of the data sharing purposes to include data curation should carefully consider potential privacy concerns to the extent that 'the sharing of data for 'data curation', including data cleansing and enhancements, would be detached from a defined end-use'.[143]
The Review acknowledges the position that data sharing should be tied to defined objectives and considers the separation of data curation from the end-use of data as a temporal matter. The Review supports the requirement that any subsequent sharing of curated data under the DAT Act should be exclusively for one or more of the permitted uses. Nevertheless, the Review considers that it should not be a necessary requirement for the permitted end-use of curated data to be established at the authorising stage and that any such requirement unduly restricts the management, refinement, and creation of data assets.

Delivery of government services

336. The Review finds some support among data custodians for clarifying the DAT Act's government service delivery purpose.[144] Submissions to the Review also support changes to the DAT Act which assist data sharing participants to navigate the intersection of data sharing for government service delivery and enforcement-related purposes. Alongside mentions of the complexity of sharing data for the delivery of government services under the DAT Act, the Attorney-General's Department note that any efforts to simplify arrangements should be balanced with the consideration of Privacy Act protections and the ongoing Privacy Act Reform agenda.[145]

---

[141] Submission 45, PHRN; Submission 38, Monash University; Submission 58, University of Melbourne; Submission 48, Psithur; Submission 69, Department of Health, Disability, and Ageing; Submission 64, AIHW; Submission 87, Western Australia Department of Premier and Cabinet.
[142] Submission 38, Monash University; Submission 48, Psithur.
[143] Submission 72, Information and Privacy Commission NSW.
[144] Submission 64, AIHW; Submission 69, Department of Health, Disability and Ageing.
[145] Submission 6, Attorney-General's Department.

337. The position of the Attorney-General's Department is further expanded on in other submissions to the Review which caution against a recalibration of the current privacy and other protections as they relate to the delivery of government services.[146]

338. Specifically, submissions to the Review identify the risk that any balancing of the existing Privacy Act protections may undermine public trust in data sharing (particularly among vulnerable communities) and may limit the effective implementation of other recommendations made by the Review.[147]

Recommendation 10

Expand the data sharing purposes to include data curation and the creation of data assets

339. The current DAT Act data sharing purposes (delivery of government services, informing government policy and programs, and research and development) are end-use focused. Data curation, on the other hand, is a data sharing purpose which permits the development and maintenance of data assets for *subsequent* use.

340. A simple example of one-off data curation may be where a data custodian seeks to share an administrative data asset with an organisation accredited to perform data curation services to transform and provide quality assurance services on that data. On providing the services, the accredited entity returns the curated data to the data custodian. More complex examples of curation (integrated data asset creation and management) may involve multi-directional data sharing between several parties and the provision of other services (de-identification, secure access, and complex data integration/linkage). Here data curation may include a variety of treatments in respect of the shared data, including the provision of data cleansing, metadata creation, and long-term management including the application of data updates and the administration of user access.

341. Important to both examples is the idea that data curation can be performed in a data sharing process independent of understanding the immediate use of the curated data. Establishing a break between data asset creation and data use would remove a temporal constraint on data asset creation, refinement, and administration. Although the Review proposes that sharing data for the purpose of curation may not necessarily require consideration of subsequent use at the time of service provision, any future use of this curated data under the DAT Act would itself need to be for a permitted purpose. Removing the need for data custodians to identify immediate use in data sharing arrangements allows parties to flexibly curate data assets without having to identify the purposes for subsequent data use until it is feasible to do so.

342. A major barrier to data sharing under the DAT Act, and throughout the data system, is the resource-constrained environment that most data custodians face when attempting to coordinate and administer data sharing arrangements. For many data custodians, data sharing is not core-business and is therefore often under-resourced and under-funded. This can result in highly valuable datasets not being shared because the data

[146] Submission 54, NIAA; Submission 67, Data Synergies; Submission 68, Department of Education; Submission 72, Information and Privacy Commission NSW; Submission 69, Department of Health, Disability and Ageing.
[147] Submission 67, Data Synergies; Submission 68, Department of Education; Submission 76, NIAA.

custodian does not have the resourcing or capability to properly curate them to the point that they are 'fit' for broader sharing. The addition of data curation as a data sharing purpose under the DAT Act would allow data custodians to outsource this function to entities accredited to perform relevant data curation services, thereby removing the need for them to invest in employing, training, and equipping staff in the provision of these services.

343. It is important to note here, and consistent with the definition of data curation, that the existing data services under the DAT Act (de-identification, complex data integration, and secure access data services) are subsets of data curation and not themselves authorised purposes. As such, the accreditation framework should also be adapted to enable entities to be accredited to perform a broader suite of data curation services.

Recommendation 11

Improve the operation of the service delivery purpose, and particularly the interaction with the prohibition on enforcement-related purposes.

344. The Review recommends the existing DAT Act privacy safeguards be re-examined and moderated, consistent with the ongoing reforms to the Privacy Act. Recalibrated settings should more closely reflect the practical realities of data sharing for the purposes of government service delivery and should better balance privacy protection and the sharing of data for public benefit.

345. Further, the Review recommends the settings for data sharing for the purposes of delivering government services should be proportionate to the risk attached to individual instances of data sharing. Balancing innovative service delivery and compliance should be the imperative of the DAT Act.

346. The Review notes that the inadvertent or improper use of data for government service delivery can rapidly translate into compliance crises in the absence of appropriate oversight and risk management. Currently, the margin between data sharing for the purpose of government service delivery and enforcement-related purposes (including detection) is slim and dependent on the precise timing of actions. Therefore, clarifying processes and mechanisms which support data sharing participants in navigating the service delivery-enforcement intersection is vital for enabling the use of data for government service delivery under the DAT Act.

347. Any changes should consider how DAT Act settings could permit the inadvertent detection and provision of notifications to relevant authorities in relation to the inadvertent detection of compliance issues in the course of using data for the delivery of government services.

348. To inform implementation, the Review presents the following options for striking a better balance between the uses of data for government service delivery and enforcement-related purposes:

- If the *primary* purpose for accessing and using data under the DAT Act is for the delivery of government services and using data for that purpose results in the inadvertent detection of compliance issues, such inadvertent detection should not constitute the use of data for enforcement-related purposes.

- Notifying relevant authorities of the inadvertent detection of compliance issues should not be a precluded activity. Consistent with the prohibition on the use of data for enforcement-related activities under the DAT Act, the relevant authorities who may be notified of potential compliance issues should not be permitted to access DAT Act data to conduct further investigations. Instead, the relevant authorities would be required to source and investigate data through alternative means.
- If an inadvertent detection of compliance issues occurs in the course of using data for the delivery of government services, this should not unnecessarily preclude the continuation of service delivery.

349. The Review recommends that guidance material and other supporting mechanisms are implemented by the National Data Commissioner to assist in the proactive management of service delivery-enforcement intersections. These mechanisms should be developed in consultation with the Australian Information Commissioner, Attorney-General's Department and other relevant integrity bodies including auditors-general or anti-corruption commissions.

The spectrum of data sharing interests

The DAT Act does not empower First Nations people

Finding 9

The DAT Act is not well positioned to help Government achieve its commitment under the National Agreement on Closing the Gap or support data sharing consistent with the Framework for the Governance of Indigenous Data.

350. The National Agreement on Closing the Gap recognises that data is a cultural, strategic and economic asset for First Nations people and essential for self-determination and community-led development (Coalition of Peaks and Council of Australian Governments 2020). Through the National Agreement on Closing the Gap, Commonwealth, State and Territory governments have committed to improve how government works with First Nations people. Priority Reform 3: Transforming Government Organisations and Priority Reform 4: Shared Access to Data and Information at a Regional Level are relevant to how government should work with both First Nations people and the data held on First Nations communities.

351. The Framework for the Governance of Indigenous Data came into effect after the DAT Act's introduction and has been co-designed by Commonwealth agencies, First Nations people and other partners to provide a foundation to implement data governance policies that align with the objectives of the Australian government and the objectives of Indigenous Data Sovereignty (Australian Indigenous Governance Institute and Maiam nayri Wingara 2018; NIAA 2024).

352. The Priority Reforms and the Framework for the Governance of Indigenous Data are not explicitly enabled by the DAT Act in its current form. As a result, individual agencies must design their own solutions to progress the Priority Reforms which can result in a broad range of approaches being used across the Commonwealth.

Exclusion from data sharing decisions

353. Section 13 of the DAT Act sets out the requirements[148] that must be met before a data custodian can authorise the sharing of data. There is no explicit requirement or process in the DAT Act for data custodians to consider the Priority Reforms or the Framework for the Governance of Indigenous Data when a data sharing project intends to use Indigenous data or reveal insights with a primary focus on First Nations communities.

354. Generally, data sharing legislation will not contain explicit requirements to align sharing activities with the National Agreement on Closing the Gap or other Government commitments. Instead, Commonwealth custodians lawfully adapt their processes as

[148] Requirements include general considerations, such as establishing a data sharing agreement, managing risks using the Five Safes framework and gaining authorisation from other data custodians (if the data has multiple data custodians). It also sets out special considerations depending on the context for data sharing and privacy protection practices for the sharing of personal information (grounded in the Privacy Act).

policy, best practice and ethical standards evolve. This can result in different approaches to affect Priority Reform 3: Transforming Government Organisations. For example:

- The AIHW's Human Research Ethics Committee operates consistently with the National Statement on Ethical Conduct in Human Research, a non-legal document (AIHW 2024; NHMRC 2023). It requires the Committee to review the ethical conduct of research (including research using public sector data) into First Nations people and communities. The review must include input from a representative with networks to, knowledge of research into, or familiarity with, the culture and practices of First Nations people.
- The ABS does not operate its own ethics committee but under certain scenarios will require data access projects to be reviewed by a recognised ethics committee. In addition to any ethics requirements, the ABS performs a cultural review of any project using Indigenous data through its Centre of Aboriginal and Torres Strait Islander Statistics (ABS 2021).
- Sections 62 and 63 of the DAT Act do not require the National Data Advisory Council to include a First Nations member, however in practice the National Data Commissioner has appointed a First Nations person as a member (ONDC 2025).

Constraints on First Nations people accessing data about their communities

355. Section 74 of the DAT Act authorises a First Nations person or community organisation to be accredited only if they are also an 'Australian entity' which is defined in the DAT Act as a Commonwealth and state and territory government body or Australian university.

356. Based on input from state and territory government agencies, the National Data Commissioner has compiled a list of 118 NSW Local Aboriginal Land Councils and 39 other organisations which focus on First Nations issues and operate as Commonwealth, state and territory bodies.[149] These organisations could apply for accreditation as users under the DAT Act and make requests to access public sector data about their communities.

357. While this may afford some organisations, communities and people with the prospect of accessing data under the DAT Act, that opportunity is denied to many other First Nations organisations. Organisations such as ACCOs or not-for-profit research institutes may be blocked from accessing data that could be used to improve First Nations outcomes.

358. As a result, the current scope of entities who are eligible to access public sector data under the DAT Act unnecessarily limits the ability of the Government to deliver on Priority Reform 4: Shared Access to Data and Information at a Regional Level.

359. In addition, entities eligible to be accredited must still apply for, and satisfy the requirements to be an accredited user, which may impose an extra layer of constraint for First Nations organisations unless changes to the accreditation framework are made (as proposed in Recommendation 8).

[149] The National Data Commissioner has provided the Review with a September 2024 letter on eligible Indigenous entities.

Support for expanding First Nations participation, and embedding Indigenous data governance frameworks

360. Feedback to the Review indicates clear and universal support to reform the DAT Act to better align with the National Agreement on Closing the Gap and the Framework for Governance of Indigenous Data, and promote greater access and transparency for First Nations organisations. To achieve this outcome, feedback focussed on several consistent themes.

Expanding accredited users to include First Nations organisations

361. As noted previously, including ACCOs in an expanded list of organisation types capable of being accredited users was strongly supported.[150] Feedback on the Draft Findings and Recommendations, also questioned whether First Nations access to data should be made broader than just ACCOs and extended to First Nations communities generally.[151]

362. Stakeholders view the expansion of accreditation eligibility to ACCOs as necessary but insufficient to achieve data sharing outcomes for First Nations organisations. This is because ACCOs are more likely to be small entities with focussed regional aims who may be unable to obtain accreditation due to not having the infrastructure and governance in place that meets the standards of the current DAT Act accreditation framework. Reforming the accreditation framework is necessary to avoid ACCOs facing prohibitively high accreditation standards that are disproportionate to the risk of proposed data sharing, especially where the data is about the community they service.[152]

Safeguards that do not reflect First Nations views on privacy

363. Feedback to the Review also identifies that the Privacy Act, and its consideration of personal information, does not always reflect how First Nations people value or view privacy. The use of the Privacy Act to determine personal information sharing safeguards may disproportionately deny First Nations peoples from accessing data about their communities (especially for small communities) insofar as they assert individual-focused, rather than or in addition to, community-focused privacy protections.

364. Rose et al. (2023), Kukutai et al. (2023) and other literature state that Australian laws and regulatory environments focus on rights to individual privacy and confidentiality for Indigenous data which can suppress the value of community-owned data as an asset.

---

[150] Submission 1, ACT Government; Submission 6, Attorney-General's Department; Submission 9, ABS; Submission 20, Department of Industry, Science and Resources; Submission 27, Indigenous Data Network; Submission 35, Melbourne Institute of Applied Economic and Social Research; Submission 38, National Data Commissioner; Submission 40, NIAA; Submission 41, Northern Territory Government; Submission 52, Seer Data & Analytics, Greater Shepparton Lighthouse Project and Maranguka Community Hub; Submission 53, Services Australia.

[151] Submission 40, NIAA.

[152] Submission 1, ACT Government; Submission 16, Department of Education; Submission 30, James Cook University; Submission 36, Monash University; Submission 49, Queensland Cyber Infrastructure Foundation; Submission 55, South Australian Department for Health and Wellbeing; Submission 56, Universities Australia; Submission 62, University of Western Australia.

365. Community-focused privacy considerations should also extend to how data custodians assess a data sharing request. A public interest test may need to consider the privacy of a community as well as the privacy of an individual.[153]

The need for genuine co-design

366. Submissions stressed the need for greater co-design – a genuinely collaborative process that includes First Nations people in the design, implementation and conduct of Government operations to deliver favourable outcomes for First Nations people. The benefits of co-design and lessons from other case studies are well documented in the literature, most notable examples of which include Butler et al. (2025) and NIAA (2023).

367. Co-design is essential to establishing processes that help identify, manage, or minimise the risks or sensitivities that data sharing may have on First Nations communities. Further, effective implementation of co-design requires careful consideration of how design parameters interact with other recommendations made by the Review. For example, changes to the existing prohibition on inadvertent detection of misconduct (as a consequence of the use of data for the purposes of service delivery) may disproportionately and adversely impact First Nations people and vulnerable communities due to their level of interaction with government services (Recommendation 11). Without co-designed and transparent practices on how incidental non-compliance issues are detected and escalated, it is likely that trust in Government agencies will fall.[154]

Building awareness, understanding and capability

368. Stakeholders also argue that DAT Act reforms should be supported by efforts to increase First Nations communities' participation in data sharing. This would require improving First Nations organisations and communities' awareness and understanding of the data sharing landscape.[155] The size of support required will vary based on organisational and community data capabilities.[156]

[153] Submission 40, NIAA; Submission 42, OAIC; Submission 76, NIAA.
[154] Submission 76, NIAA.
[155] Submission 27, Indigenous Data Network.
[156] Submission 76, NIAA.

Recommendation 12

Embed Indigenous data governance frameworks into decision-making processes and expand the participation in the DAT Act so that First Nations peoples are better heard, recognised and empowered to contribute to positive outcomes for Indigenous communities.

369. The DAT Act should be revised to enable data sharing that supports the Commonwealth Government's commitment under the National Agreement on Closing the Gap and Framework for the Governance of Indigenous Data, and ensure appropriate support is in place to encourage participation and engagement in the data sharing ecosystem.

370. An amended DAT Act could adopt a specific concept and application of privacy to clearly authorise the sharing of personal information with First Nations communities. Amendments could be designed to enable the flexible application of individual-focussed or community-focussed privacy protections as decision makers (data custodians and any First Nations representatives who engage in the decision-making process) deem appropriate. Amendments would need to authorise the sharing of personal information directly to the accredited user and, where appropriate, provide analytical results and insights to First Nations communities.

371. Empowering First Nations communities to access data under the DAT Act requires:

- expansion of accreditation eligibility to include ACCOs (proposed in Recommendation 8)
- calibration of requirements in the accreditation framework for ACCOs to ensure they can obtain accreditation (also proposed in Recommendation 8).

372. ACCOs who obtain accreditation should demonstrate sufficient levels of data capability and ensure information is safeguarded against unauthorised access or use when engaging in data sharing activities. The use of ACCOs to improve communities' access to data is preferred over granting accreditation eligibility to communities generally, given that the DAT Act's design and safeguards require data users to be organisations. There is also a lack of clarity on the level of data maturity that exists among communities and the extent to which they can safely use and draw insights from public sector data. The introduction of a Ministerial power to expand accreditation eligibility (proposed in Recommendation 9) provides a pathway which could permit specific First Nations communities or possibly all communities to engage in data sharing under the DAT Act, if appropriate safeguards can be designed for communities that have the capability to safely handle public sector data.

373. In conjunction with these changes, the engagement of First Nations communities with the data sharing ecosystem could be improved through:

- greater support to participate in co-designing practices, contribute to decisions and oversee ecosystem improvements (with funding if necessary)
- simplifying practices, language and templates (that include default settings for culturally safe data practices) to improve understanding and minimise burdens on participants

- greater support to co-design, pilot, evaluate and improve process for ACCOs to access data (with funding if necessary).

374. Appropriately framed guidance is also required to ensure that consistent approaches are employed by data custodians to include First Nations people in decision-making processes that influence how Indigenous data is used, and other data sharing that has a primary focus on First Nations people and communities. To ensure that First Nations people have a voice in leading system-level advice on the use and provision of access to public sector data, the National Data Commissioner should continue to appoint a First Nations representative to the National Data Advisory Council. While this is currently being done through non-legislative practice, an explicit legislative requirement about the membership of the National Data Advisory Council could be used to embed, and further signal the importance of, appropriate representation of First Nations people.

375. In the context of Recommendation 3 and a default posture of agreeing to share data, it may be reasonable that concerns and risks to First Nations communities are sufficient grounds to impose additional requirements when sharing data, or to refuse certain data requests outright.

376. Implementing this recommendation and achieving intended outcomes requires a genuine co-design process that includes First Nations people and public sector data sharing stakeholders. Reform of the DAT Act and supporting First Nations' understanding and knowledge of the data sharing ecosystem alone may not be sufficient in aligning public sector data sharing with the Government's commitments in the National Agreement on Closing the Gap. Action may also be required to ensure that the Privacy Act can support First Nations views on privacy and enable data sharing with First Nations organisations that have appropriate privacy safeguards in place.

377. A co-designed solution for embedding Indigenous data governance frameworks may not need legislative change, or need to be embedded in legislation, to be effective. A government-wide policy or requirement, anchored by the Framework for the Governance of Indigenous Data or other emerging initiatives such as the Data Policy Partnership (PC 2025), may be a preferred approach. As demonstrated by the AIHW and ABS' use of ethics committees, non-legislative enablers can be effective, adaptive and applied more broadly to mandate a consistent and genuine approach to embed First Nations people in the data sharing decision making process.

Recognition of state and territory data custodianship

Finding 10

The DAT Act does not provide equivalence to state and territory data custodians, which limits its capacity to enable two-way data sharing between jurisdictions.

378. Government policy and service delivery can be greatly enhanced by connecting datasets generated by different jurisdictions to create a more complete picture about regional economies, society and populations. States and territories are essential creators and custodians of public sector data and regularly share their data with the Commonwealth for the purposes of improving policy development and service delivery.

379. However, a lack of recognition and inconsistency between jurisdictions can impede co-ordinated, multi-jurisdictional initiatives. This has entrenched a perception that, despite the states and territories' essential role in supporting and enabling public sector data sharing, the DAT Act does not provide equivalence between Commonwealth and state data custodians.[157]

380. The issue of equivalence is demonstrated in two provisions that exclude states and territories from holding a level of control over data:

- Paragraph 13(2)(b) does not require Commonwealth data custodians to consult with, or seek approval from, state data custodians when authorising data sharing that includes state data. This is because for the purposes of the Act, subsection 11(2) defines a data custodian to be a Commonwealth body only.
- Subsections 20F(2) and 20F(5) deny state government agencies ownership and control over derivative products that they produce. This is because only a Commonwealth body can be appointed as a data custodian of the output of a data sharing agreement.

381. These exclusions largely reflect constitutional limits on the Commonwealth's ability to authorise and regulate the activities of jurisdictions as data custodians. However, outside the DAT Act, many Commonwealth agency processes better recognise that states and territories have equal standing when making data sharing decisions (ABS 2024; AIHW 2023).

382. The DAT Code 2022 introduces measures to explicitly recognise, protect and preserve state data custodians' conditions or requirements when their data is to be shared under the DAT Act, but this does not grant equal status with Commonwealth data custodians.

A nationally consistent data sharing framework

383. Cross-jurisdictional initiatives are enabled by a range of jurisdictional authorisations to supply and use data for certain purposes. As is the case with the Commonwealth, the jurisdictional authorisations are largely legislative enablers designed and adapted for specific agencies and their functions or responsibilities. Some jurisdictions have established state-wide data sharing frameworks to remove barriers to sharing and facilitate greater data sharing, but these also differ in approach across each jurisdiction.

384. As a result, organisations requesting data held by multiple jurisdictions experience different data custodian requirements (which can include information requirements necessary to assess a request, and requirements imposed on how data can be used), response times and data sharing decisions. While an updated DAT Act may provide a solution for similar issues that occur within the Commonwealth government, it is unlikely to resolve these issues at the national level.

385. An updated DAT Act faces constitutional constraints to harmonising jurisdictional frameworks. In general, a Commonwealth Act cannot authorise the sharing of state data (including to the Commonwealth) due to constitutional limitations on the Commonwealth's ability to authorise and regulate the activities of jurisdictions as

[157] This finding is consistent with ONDC (2024).

custodians. However, harmonisation is possible if jurisdictions undertake equivalent legislative reform. If achieved, the reform would improve the effectiveness and expediency of two-way data sharing between jurisdictions by providing a common foundation across all government data custodians. It would also provide a standard approach for government and non-government users to request data.

Support for recognising states and territories and a harmonised nationally consistent framework for data sharing

386. Feedback to the Review supports recognising state data custodians and targeting improved interoperability between Commonwealth, state and territory data sharing schemes.

387. In submissions and discussions with the Review, state data custodians consistently stress the importance of ensuring that they retain effective control over their data, which can be addressed by granting states and territories status equal to Commonwealth data custodians.[158] It is also recognised that the DAT Act's inability to authorise states to share data impedes the creation of connected datasets by the Commonwealth.[159] Improving equality with state data custodians would enable more efficient data flows across agencies to set up and operate connected, national datasets and reduce administrative burdens.

388. Discussions with state and territory government agencies reveal support for a harmonised data sharing framework beyond establishing equivalence in the DAT Act between Commonwealth, state and territory data custodians. Submissions and discussions with Commonwealth Government agencies and non-government organisations also indicate support for equivalence and for using the DAT Act to advance cross-jurisdictional collaboration and data sharing outcomes.[160]

389. Other submissions do not specifically focus on equivalence between jurisdictions but recognise that a nationally consistent framework has many benefits for requestors. These submissions note that requestors seeking to access data from multiple jurisdictions are frequently required to satisfy different requirements, or undertake duplicate processes, to satisfy each jurisdiction's request process. A consistent framework for jurisdictions would therefore result in user requests being actioned in a timelier manner, and with less burden. Additional, time and cost savings could be achieved if the consistent framework is supported by interoperable infrastructure, such as a single front door for making requests.[161]

390. It was also noted that the lack of interoperability between the DAT Act and state laws is just one example of uncertainties between the DAT Act and existing legislation. The APPs and existing secrecy provisions are other examples that create legal uncertainty when sharing data within, and across, jurisdictions.[162]

---

[158] Submission 1, ACT Government; Submission 41, Northern Territory Government.
[159] Submission 55, South Australian Department for Health and Wellbeing.
[160] Submission 9, ABS; Submission 12, AIHW; Submission 16, Department of Education; Submission 18, Department of Health, Disability and Ageing; Submission 21, Department of Social Services; Submission 38, National Data Commissioner; Submission 42, OAIC; Submission 51, Research Australia.
[161] Submission 5, AAMRI; Submission 7, Australian Academy of Science; Submission 24, Flinders University; Submission 32, KPMG; Submission 36, Monash University; Submission 58, University of Melbourne.
[162] Submission 53, Services Australia.

Recommendation 13

The DAT Act should explicitly recognise the roles of states and territories in Commonwealth processes that involve jurisdictional data.

391. There is a clear benefit and pathway for an amended DAT Act to grant state and territory agencies equal status to the Commonwealth when making decisions and designing operations to share state data that is held by the Commonwealth. There is also a clear pathway to enable state and territory data custodians to assume rights over new data they create through data sharing projects enabled by the DAT Act. These amendments would address some concerns states and territories have when sharing data to the Commonwealth for the creation of connected datasets. Productivity gains that can be realised by this approach will be influenced by the degree to which state or territory custodian's decision-making requirements or expectations align with the Commonwealth and other jurisdictions.

392. Elevating state and territory rights to control the use and sharing of their data can be given affect through a combination of primary legislation, subordinate legislation and policy. Noting that Recommendation 2 aims to streamline and reduce requirements in the primary legislation, the implementation approach should ensure that recognition of all public sector data custodians' rights and responsibilities are granted through the same mechanism.

393. At a minimum, the DAT Act should provide a contemporary overview of the public sector data sharing practice that recognises the essential role that the states and territories play in the creation and use of public sector data. This will provide a foundation to develop subordinate legislation or policy enablers that embed the rights of data custodians.

Recommendation 14

Longer term, there should be a nationally consistent data sharing framework that achieves full interoperability across jurisdictions and provides standardised pathways for users to access Australian public sector data held by any government.

394. The Government should work with jurisdictions to determine their level of interest in, and preferred model for, a nationally consistent data sharing framework to standardise pathways and deliver efficiencies when creating or sharing cross-jurisdictional data.

395. This would result in significant benefits for requestors whose needs span multiple jurisdictions and face additional burdens due to the current inconsistencies in requirements and approaches. A stand-alone piece of Commonwealth legislation is unlikely to be capable of achieving this goal due to constitutional limits that would need to be navigated. It would likely require reciprocal changes in state and territory government legislative authorisations to enable.

396. If sufficient appetite exists across the jurisdictions, pursuing the creation of a nationally consistent data sharing framework is a valuable reform that can deliver

productivity gains for data custodians and data users. It would require significant effort across jurisdictions to collaborate, co-design and implement, and may require a broader scope of reform, such as also harmonising privacy legislation or requirements like permitted disclosures of personal information. Achieving a nationally consistent framework for sharing data is likely to require more time to design and negotiate with the jurisdictions. The Government should liaise with the states and territories to establish their views on such a framework, and, if sufficient support exists add this proposal to the National Data Sharing Work Program.

397. A nationally consistent framework should be considered a separate body of work to, and be undertaken after, reforming the DAT Act.

398. The development of a nationally consistent framework can learn from how changes to the DAT Act, and other state data sharing legislation, influence data sharing and can incorporate the design elements that positively influence data sharing outcomes. A consistent legal framework for data sharing can also drive the use of common tools, platforms and standards nationally and realise further efficiencies for governments and users.

399. The Review does not suggest a preferred approach to designing such a framework, which should be left to Commonwealth, states and territories to co-design, but presents three broad options and their likely challenges.

- Option 1: The updated DAT Act is adopted as the central framework and uses an 'opt-in' mechanism for jurisdictions to participate. Jurisdictions update their legislation to permit sharing if it is authorised by the DAT Act (which may require a mirroring of conditions in their legislation).

  This approach may require rationalising certain powers in the DAT Act, such as limiting the proposed Minister powers to designate a single data custodian as a data sharing decision maker or to direct state bodies to share data.

- Option 2: A federated approach where data sharing frameworks remain decentralised but are each modified to broadly authorise cross-jurisdictional data sharing.

- Option 3: A hybrid of Option 1 and Option 2 is possible where some components of the DAT Act form the core of a national framework but the remaining DAT Act components (for example, the proposed powers that would be limited in Option 1) are not applicable to the jurisdictions if they are deemed to be undesirable or impractical. Jurisdictions also update their legislation to mirror the 'core' DAT Act components and retain any specific requirements that continue to apply within their jurisdictions.

Broader systems and capability

Non-legislative barriers to data sharing

400. Broad uplift in capability, capacity, platforms and tools across the Commonwealth data sharing ecosystem is required for the DAT Act to deliver data sharing outcomes while interoperating with other Commonwealth and state frameworks.

401. The Terms of Reference direct the Review to consider 'any other relevant matters'. Given that, the Review has considered non-legislative issues that need to be resolved to ensure a revised DAT Act can operate successfully within the broader data sharing ecosystem.

402. Throughout the Review's consultation process, stakeholder submissions and bilateral discussions identify a range of non-legislative issues that impede existing Commonwealth data sharing and would continue to impact data sharing into the future unless addressed. Data users and data custodians discuss similar themes from differing perspectives, and therefore present a diversity of insights into the underlying causes and possible remedies to overcoming barriers to data sharing.

403. Stakeholder feedback demonstrates some challenges observed by users, custodians and other interested parties, but may not be exhaustive or representative of the whole ecosystem. Some submissions offer broad feedback while others, such as the ABS submission, exclusively focus on legislative issues related to the DAT Act.

Non-legislative issues limiting data sharing

404. Data users from across government and non-government sectors (including users who are also data custodians) observe that, from a whole of system perspective:

- Better data discoverability is needed for users to more easily identify public sector data that is of interest to their work. Many data custodians do not make their data holdings readily discoverable, even if they operate a data sharing framework.[163]
- More clarity on the data sharing frameworks in operation is needed to assist users to understand how to request the data, once they have identified target datasets. Users, especially non-government users, do not distinguish public sector data as siloed holdings and are often unfamiliar with different agency's data sharing frameworks. To improve timeliness and positive outcomes, users need clear information about the data request process, including how to make a request, whether they are eligible to make a request, the custodian's information requirements to consider a request, and how the custodian will come to a decision.[164]

405. In the context of the DAT Act, users do not understand its advantages, application and interaction with emerging data access initiatives such as Digital ID and the Consumer Data Right as well as established mechanisms such as Freedom of

[163] Submission 7, Australian Academy of Science; Submission 35, Melbourne Institute of Applied Economic and Social Research; Submission 56, Universities Australia; Submission 58, University of Melbourne; Submission 62, University of Western Australia.
[164] Submission 36, Monash University.

Information.[165] Supporting information on the DAT Act can be unclear and difficult to access, requiring users to navigate through the process with limited support.[166]

406. As noted previously and contributing to discussions for Recommendations 1 and 3, data custodians also have incentives to use existing, non-DAT Act access pathways.[167]

407. However, agency-specific data request processes may not result in timely access to data and can be burdensome due to the range of complex, duplicative or non-standard practices that currently exist across different data custodians.[168]

408. Requestors may not have the resources available to navigate such processes in a timely fashion and, without support from the ONDC or a data custodian, this makes it difficult for some organisations to engage in data sharing.[169]

409. Data sharing decisions are perceived as being unfairly influenced by data custodian resourcing and risk postures. Requestors may face refusals because data custodians:

- have no duty to share or do not have resources available to consider or action requests, due to competing priorities[170]
- have low data maturity or confidence in their dataset's quality or suitability for sharing (both generally as well as for specific purposes)[171]
- have too high an aversion to, and are unable or unwilling to manage, data sharing risks. This includes a perceived lack of trust by custodians towards users, even when they can demonstrate higher levels of trust through processes such as DAT Act accreditation[172]
- support data sharing, but only within their own secure access data service, which may not always be a workable solution for the data user.[173]

410. Decisions can also be unpredictable in timing and outcome. Changes in personnel within a data custodian agency can result in different decisions, and there are perceptions that some data requestors can use their established relationships with decision-makers to gain a favourable decision.[174] Some data custodians are willing to negotiate a compromise to better enable data sharing while balancing their risks or resources, while others will refuse a request without attempting to engage in meaningful discussions to reach a compromise solution. As noted previously, there is also no standard recourse to formally appeal a decision to reject a data sharing request under the DAT Act.

411. As also noted in the background to this report, the data sharing capability and capacity of participants are key factors determining data sharing outcomes. When data is approved to be shared, users may experience further delays in obtaining access. This

---

[165] Submission 17, Department of Employment and Workplace Relations; Submission 42, OAIC; Submission 45, PHRN.
[166] Submission 22, Digital Transformation Agency.
[167] Submission 17, Department of Employment and Workplace Relations; Submission 45, PHRN.
[168] Submission 56, Universities Australia; Submission 60, University of Sydney.
[169] Submission 17, Department of Employment and Workplace Relations.
[170] Submission 16, Department of Education; Submission 30, James Cook University.
[171] Submission 36, Monash University; Submission 38, National Data Commissioner; Submission 48, Psithur; Submission 58, University of Melbourne.
[172] Submission 58, University of Melbourne.
[173] Submission 5, AAMRI.
[174] Submission 35, Melbourne Institute of Applied Economic and Social Research; Submission 36, Monash University; Submission 58, University of Melbourne.

can be due to competing priorities and the effort required for the custodian to retrieve, prepare or source data[175] as well as the effort required to perform additional functions on the data, such as undertaking data linkage or preparing a secure environment for the user to access the data.

412. Data users who use research grants or other time-limited finances to fund their analytical work often discover that by the time they access the data, their grant or funding source has expired. Analytical findings may also be subject to conditions that users feel are unreasonable. These conditions can vary in nature, but include:

- rights for custodians to reject the publishing or use of an analytical result
- requirements for custodians to validate outputs, and
- requirements that custodians be notified and provided a summary of insights when findings are released.[176]

413. Data sharing costs are incurred by data custodians and passed on to users, including costs associated with data linkage and the provision of secure access data services. These costs vary significantly and present a barrier to entry for some users. Uncertainty about costs also presents challenges for users that need to apply for funding and budget for costs they will incur throughout the data sharing process.[177]

414. Other feedback identifies broader issues, including that:

- technology infrastructure presents a challenge to adoption. Platforms like Dataplace impose specific roles and permissions that are complex, unintuitive and limit the ability for smaller agencies to manage their activities in the system. In other cases, there are no platform solutions for key data sharing activities, such as for transmitting data that is subject to a data sharing agreement.[178]
- users may not be able to interact with data custodians directly until a formal process is underway. Users may prefer to have preliminary or scoping discussions with data custodians to proactively identify issues that trigger additional processes, or cannot be supported by a data sharing framework. Currently, many users can only interact with data custodians once they have submitted a formal request and provided all accompanying information and assessments for consideration.[179]

415. Submissions and bilateral discussions with the National Data Commissioner and data custodians evidenced broad agreement with many of the non-legislative issues observed by users, including that:

- risk aversion or cultural resistance has increased for many agencies following the Royal Commission into the Robodebt Scheme and the clear signals that agencies are accountable for downstream misuse or unauthorised disclosure (which may be outside of their visibility and control, and risks of which may not be able to be completely mitigated)[180] The Review already discussed above how the DAT Act's focus on regulation and enforcement, along with penalties for misuse, adds to the perception that data sharing is a high-risk activity.

---

[175] Submission 36, Monash University.
[176] Submission 1, ACT Government; Submission 35, Melbourne Institute of Applied Economic and Social Research.
[177] Submission 5, AAMRI; Submission 36, Monash University; Submission 48, Psithur.
[178] Submission 22, Digital Transformation Agency.
[179] Submission 16, Department of Education.
[180] Submission 38, National Data Commissioner; Submission 53, Services Australia.

- the use of disparate data sharing frameworks with varying levels of sophistication makes standardised data sharing difficult[181]
- data custodians avoid the DAT Act because more effective, flexible alternative mechanisms exist, or apply to a broader range of data, uses or users[182]
- Dataplace is burdensome to use and providing transparency on non-DAT Act sharing is complex and resource intensive[183]
- the resourcing required to support DAT Act requests, curate data and establish transfer pipelines is costly and potentially redirects scarce capability or capacity away from supporting more data sharing via other methods.[184]

Finding 11

The data ecosystem, in general, requires a capability uplift to enable better outcomes for participants.

Solutions proposed by stakeholders

416. Stakeholder submissions offer suggestions on how to address these non-legislative issues. These are presented generally as solutions which encourage easier user participation, more responsive and informed decisions by data custodians, and better planning and coordination across the Commonwealth to address current and future data sharing bottlenecks.

Improve user understanding of the data sharing ecosystem to encourage participation

417. Arming users with advance information on how they can identify and access data, what requirements must be met when requesting or using that data, and providing standardised practices will improve their experience and drive more timely and targeted data sharing requests. This applies to users generally, and to user groups like First Nations who may require additional co-designed action (see Recommendation 12). Actions suggested in submissions and discussions with data users include to:

- clarify how different initiatives such as the DAT Act, Digital ID and the Consumer Data Right are intended to interact[185]
- establish policy guidelines to support data sharing expectations and uses, including an open science policy and a framework for data sharing for AI[186]
- mandate and resource data custodians to make datasets discoverable, using common standards for metadata, categories and formats to ensure the data is

[181] Submission 53, Services Australia.
[182] Submission 16, Department of Education.
[183] Submission 16, Department of Education.
[184] Submission 16, Department of Education; Submission 53, Services Australia.
[185] Submission 14, Business Council of Australia; Submission 45, PHRN.
[186] Submission 7, Australian Academy of Science.

interpretable, and including quality tags to help manage researcher expectations and for using AI[187]

- use common platforms that are framework-agnostic to simplify and facilitate data discovery and data request and access processes. Such platforms should also be leveraged to find opportunities to reduce complexity, remove unnecessary duplication in data request requirements and standardise processes across government and research data projects (for example, research integrity, ethics and intellectual property)[188]
    - This can include uplifting and extending Dataplace and the Australia Government Data Catalogue to service a broader range of data users and requests while improving transparency of the whole ecosystem.[189]
- greater transparency on the different data sharing legislation or frameworks that exist across the ecosystem (including their handling processes, timeframes, requirements, merit system and costs) and where the DAT Act or National Data Commissioner can be used to facilitate positive outcomes[190]
- provide users with kickstart funding to demonstrate successful pathways for users and data service providers to use the DAT Act[191]
- provide ongoing support and resources for users to access and use data sources.[192]

Drive better data sharing decisions and responsiveness by data custodians

418. Encouraging data custodians to willingly engage in the data sharing ecosystem, be responsive to data sharing requests, share data by default and grant access in a timely manner will improve data sharing outcomes. Actions suggested in submissions and discussions with data users include to:

- clarify government expectations that data is an output of any government activity, including actions arising from partnerships between government, research and industry sectors.[193] Non-sensitive datasets should be released as open data[194] and data sharing should be the default where the risk is low and the value is high.[195]
- establish consultative forums with representation from the ONDC, users, data custodians, service providers and other stakeholders to understand and agree on emerging opportunities and drive ecosystem improvements[196]

---

[187] Submission 5, AAMRI; Submission 7, Australian Academy of Science; Submission 45, PHRN; Submission 48, Psithur; Submission 60, University of Sydney.
[188] Submission 36, Monash University; Submission 38, National Data Commissioner; Submission 56, Universities Australia; Submission 58, University of Melbourne; Submission 62, University of Western Australia.
[189] Submission 17, Department of Employment and Workplace Relations; Submission 20, Department of Industry, Science and Resources.
[190] Submission 36, Monash University.
[191] Submission 30, James Cook University; Submission 58, University of Melbourne.
[192] Submission 24, Flinders University; Submission 27, Indigenous Data Network; Submission 51, Research Australia; Submission 61, University of Tasmania.
[193] Submission 30, James Cook University.
[194] Submission 7, Australian Academy of Science.
[195] Submission 8, Australian Banking Association; Submission 14, Business Council of Australia.
[196] Submission 27, Indigenous Data Network; Submission 36, Monash University; Submission 47, Prospection; Submission 58, University of Melbourne.

- improve data custodian's data maturity, tools, methods, skills and culture to ensure consistent policy interpretation and decision-making across different personnel[197]
- improve custodian understanding of the accreditation process to instil greater trust and confidence in users who are accredited under the DAT Act[198]
- make greater use of universities to support Commonwealth data sharing needs (e.g. training, curation, provision of infrastructure) and use industry and non-government organisations to provide data sharing ecosystem infrastructure[199]
- support user requirements, such as real time data flows different access mechanisms (e.g. APIs)[200]
- resource custodians to respond to demand[201]
- prioritise curation, improvements and access to high value datasets.[202]

Improve the strategic planning for data sharing

419. Leadership of the broader Commonwealth data sharing ecosystem, not just the DAT Act, is necessary to drive sustained improvements to data sharing outcomes. Actions suggested in submissions and discussions with data users include to:

- across all levels of government and the research sector, ensure that resources are efficiently allocated[203]
- strengthen data capability for all indicators of data maturity[204]
- invest in data sharing platforms and infrastructure, including viable system requirements for system-to-system data sharing.[205]

Non-legislative reform is required

420. Reforms to the DAT Act may create a safe and secure legal environment for data sharing by Commonwealth government agencies but are not sufficient to ensure actual data sharing and value creation will occur. The limitations of the current DAT Act are only one component limiting Commonwealth data sharing, which is also hindered by many data custodians having:

- poor data quality, discovery, curation and availability
- inconsistent data standards and processes for data sharing
- poor incentives for custodians to share data, aggravated by a risk averse culture
- inconsistent or duplicated systems for sharing data

---

[197] Submission 24, Flinders University; Submission 30, James Cook University; Submission 48, Psithur; Submission 57, University of Adelaide.
[198] Submission 53, Services Australia.
[199] Submission 35, Melbourne Institute of Applied Economic and Social Research; Submission 46, Professor Lyria Bennett Moses and Nicholas Hodgkinson; Submission 49, Queensland Cyber Infrastructure Foundation; Submission 58, University of Melbourne.
[200] Submission 8, Australian Banking Association.
[201] Submission 7, Australian Academy of Science.
[202] Submission 7, Australian Academy of Science; Submission 29, IoT Alliance Australia; Submission 36, Monash University; Submission 48, Psithur; Submission 58, University of Melbourne.
[203] Submission 38, National Data Commissioner.
[204] Submission 38, National Data Commissioner.
[205] Submission 53, Services Australia.

- higher priorities that limit resources available for improving the issues above.

421. While reforming the DAT Act in line with the recommendations of this Review will assist some of these issues (e.g. providing avenues to curate data by sharing it with expert organisations, creating a clear, consistent process for data access) most of these blockers will need to be directly dealt with in addition to the DAT Act reforms.

422. There is a strong case for the Commonwealth to implement greater accountability, responsibility and system leadership to drive urgent non-legislative reform across the data sharing ecosystem. This would provide a leadership function to coordinate uplift across the system that improves data sharing outcomes and to guide investment decisions that rationalise the use of overlapping platforms and the effectiveness of government funding used across the ecosystem. The National Data Commissioner and ONDC may not be suitable to perform this role.[206]

423. However, the lack of information on non-DAT Act data sharing is a barrier to understanding the extent of the issues raised by stakeholders, and making recommendations on priority areas for uplift.

424. As a result, while this report outlines stakeholder feedback and information for future consideration, more work is required to diagnose the state of the data sharing ecosystem and to identify opportunities to for investment in capability or capacity uplift.

Leadership and advocacy over the Commonwealth data sharing ecosystem

425. There is no clear leadership role in the Commonwealth that focusses on the data sharing ecosystem as a distinct component of broader government data policy, and coordinates with stakeholders to lead a strategic, whole-of-government approach to drive data sharing priorities.

426. The current regulatory and DAT Act-centric role of the National Data Commissioner does not extend to influencing and advocating at a system level or advising Government on the data sharing ecosystem. The changes to the role of the National Data Commissioner, as suggested in Recommendation 4, will only exacerbate the absence of a leader to coordinate uplift and problem solving in the ecosystem.

427. Establishing clear leadership for data sharing policy making and the direction of the data sharing ecosystem could address this issue. This leadership function would work with data sharing stakeholders to advocate and advise government on the health of the data sharing ecosystem and recommend strategies to address systemic, whole-of-government non-legislative barriers to data sharing.

428. Based on the stakeholder feedback this leadership function is not just a matter of convenience; it is essential to establish the right environmental conditions that will enable more data sharing agreements, improved timeframes and use of standardised systems and processes.

---

[206] As noted in the Review, the original DAT Bill included an advocacy role for the National Data Commissioner that was not implemented after recognising the potential conflict that may arise with its regulatory role.

Transparency on non-DAT Act data sharing is limited

429. There is insufficient information about the data sharing ecosystem for the Review team to determine the extent to which Commonwealth data sharing is impacted by the issues raised by stakeholders, and where to prioritise uplift in the data sharing ecosystem.

430. Aside from sharing under the DAT Act, there are no general legal or policy requirements for data custodians to report the number, nature or outcomes of data sharing requests made to them. Some data custodians are proactive in reporting data sharing, but the information can differ in location and presentation. For example:

- The ABS' 2023-24 Annual Report includes performance measures on access to its data products and services, including calls to API services, DataLab sessions, and website sessions. This is a measure of usage, rather than a measure of the number of data sharing projects (ABS 2024).
- The AIHW website maintains a list of active research projects and the 2023-24 Annual Report includes some performance measures such as the number of website sessions, but no measures of secure access attributed to active research projects (AIHW 2025a; AIHW 2024).

431. An additional evidence base is the 2024 report referenced in the Issues Paper, which conducted a one-off survey of 19 Commonwealth agencies and found that over 11,000 non-DAT Act data sharing agreements were in effect.[207]

Current levels of Commonwealth data maturity

432. To understand the extent that low data maturity may impact on the accessibility and risk posture of data custodians, the Review considered available evidence on data capability and maturity across Commonwealth data custodians.

- The Data Maturity Assessment tool (Department of Finance 2025b) provides an assessment of data maturity across the data lifecycle, helping inform agencies' future development needs as the data ecosystem evolves. The 2024 Data Maturity Assessment Report identified that the average data maturity score across the APS was 2.02 out of 5, a rating of 'developing'. which indicates that on average, agencies understand the importance of using and managing data effectively at the enterprise level, have some initiatives for increasing data capability, and have started using data to improve selected areas to advance operational efficiency, but that these improvements are still a work in progress (Department of Finance 2024).[208]
- The Data Inventories Pilot Program (ONDC 2024) was an initiative implemented by the ONDC, working with Commonwealth agencies to help them discover their data and to develop a standardised list of data assets they hold - known as a data inventory which was supported by a data inventory guide.

[207] The figure comes from the informal survey referenced in footnote 11 above.
[208] Note that this is based on agencies' self-assessment and may not reflect data maturity relating specifically to data sharing for non-core business purposes.

433. This evidence validates user perspectives that low data sharing maturity and capability are contributing to custodians' aversion to support data sharing, with some action taken by the ONDC to address capability gaps.

The interaction between the DAT Act and other frameworks is not clear

434. The DAT Act's development has coincided with the development of other Commonwealth government data initiatives such as the Consumer Data Right (Australian Government 2025) (which stems from the PC Inquiry findings) and Digital ID (Department of Finance 2025a). The DAT Act also sits within an environment where other information access schemes (which are not strictly viewed as data sharing) exist, such as the Privacy Act and the *Freedom of Information Act 1982* (Cth) (FOI Act).

435. The ONDC provides a range of public resources to help users understand the DAT Act, but this does not extend to outlining the advantages of using the Act compared to other existing and emerging data initiatives and information access schemes.

System-level coordination of data sharing platforms and infrastructure

436. Currently, data custodians share data using a range of platforms, data infrastructure and datasets. Many are developed in isolation to fulfil a specific agency or policy requirements. More extensive and complex data sharing may necessitate stricter use of certain platforms and infrastructure.

437. For example:

- APS Remuneration Data provides simple, aggregate information published using the agency website as a platform, and includes metadata, standards and classifications pertaining to the data (APSC 2025b).
- APS Employee Census datasets are relatively simple unit record data available on the data.gov.au open data platform, and includes metadata, standards and classifications pertaining to the data (APSC 2025a).
- ABS Census of Population and Housing detailed microdata datasets are relatively more complex and sensitive unit record data requestable through the ABS myDATA platform and accessible on the ABS DataLab platform (ABS 2025), and includes critical data infrastructure such as metadata, standards and classifications pertaining to the data.
- NDDA comprises complex unit record datasets created using the ANDII platform (NDDA 2025b), which hosts critical infrastructure like linkage spines, to create the dataset, requestable through the Dataplace platform (NDDA 2025a), and accessible on any approved ADSP secure access environment platform.
- All the above datasets are also requestable on the Dataplace platform (but data sharing may be serviced outside of the DAT Act).

438. There are some Commonwealth data sharing platforms that have been developed for whole of government use. Nevertheless, wholesale uptake of such platforms by data

custodians has not occurred for a variety of reasons. For example, the ONDC has highlighted that the utilisation of Dataplace and the Australian Government Data Catalogue (AGDC) has been low. This may be attributed to data custodians' misunderstanding of the platform's role in supporting data sharing both under and outside of the DAT Act, the complexity of how some system features are designed, and a resistance on the part of data custodians to move away from established data sharing practices and processes.[209]

439. The use of different platforms and data infrastructure is also occurs among data users. Many universities and research bodies operate their own secure infrastructure for hosting and analysing sensitive data (mirroring government platforms like the ABS DataLab), with examples including the following:

- The Melbourne Institute of Applied Economic and Social Research operates the Melbourne Institute Data Lab, a secure, purpose-built data enclave that enables virtual access to micro-level data for curation, analysis, and visualisation (MI 2025).
- The Sax Institute operates the Secure Unified Research Environment, a secure platform for the sharing and analysis of sensitive health and other data (Sax Institute 2025b).
- The University of New South Wales operates the E-Research Institutional Cloud Architecture, a secure cloud computing infrastructure for individuals working with sensitive, often large-scale data (UNSW 2025).
- Griffith University operates the Relational Insights Data Lab, a custom-built, secure research facility designed to store, manage, and analyse sensitive administrative data for research and teaching purposes (Griffith University n.d.).

440. Based on the information available, many platforms and data infrastructure used across government and non-government may have overlapping or duplicated functions. It is unknown whether these systems are intentionally developed with duplication in mind (for example, to encourage competition and market forces), have converged over time as they have adapted common technology or tools (for example, cloud computing and data science tools), or whether developers were unaware of existing systems that could service their needs.

441. There is evidence of sectoral leadership (for example, the ARDC drives the development of national digital research infrastructure for researchers), but no evidence of coordinated design and investment across sectors.

442. It is also possible that many of these systems were developed using common funding sources. Government appropriation is used to fund platform and infrastructure development by government agencies, and government grants can be used to fund similar activities in the research sector. The research sector can also access funds through industry partners and philanthropic foundations.

Supporting increasing demand for data

443. Data users and data custodians incur a variety of fixed and variable costs to be 'data sharing ready' and to share or use the data.

---

[209] Sourced from additional information provided by the ONDC to the Review.

444. Data custodians can incur fixed, ongoing costs to establish or maintain its levels of data maturity, platform functionality and cybersecurity, as well as the quality, currency and availability of data assets.

445. These costs, while fixed, can experience step ups or downs in response to emerging opportunities and user demand. For example, expanding an existing data asset to frequently link data from a new source will attract a higher ongoing fixed cost.

446. Variable costs incurred by custodians are influenced by the number and nature of data sharing requests received. This includes assessing data sharing requests, performing tailored tasks to address user's needs for customised datasets or tools, and usage costs incurred by users on the custodian's systems or platforms.

447. Depending on their circumstances, requestors incur fixed costs to apply for and maintain their accreditation status.

448. User's variable costs will vary depending on the complexity of their work and tools, but can include:

- effort required to explore datasets, prepare and submit data sharing requests
- effort required conduct their intended research
- custom work specified in an approved data sharing agreement (for example, undertake data linkage if the data custodian lacks the capability)
- usage costs of analysing data within their own platforms (if that is their preference).

449. Aside from the Data Inventories Pilot Program, the DAT Act came into effect with no additional funding for data custodians to uplift their data capabilities or support increasing demand for sharing sensitive data. Custodians can, and do, use cost recovery to manage and respond to growing demand for data.

450. The AIHW and ABS publish their secure access data service fees online. This demonstrates the potential costs that a custodian can incur to support a single research project (ABS 2022; AIHW 2025b). When considering the degree of customisation possible in a data sharing project (such as the creation of tailored datasets or establishing new data supply pipelines), growing demand may not achieve economies of scale. As a result, costs to access data may present a persistent barrier to entry if passed on to the data user.

451. Charging users fees based on their data sharing request is a retrospective approach to resourcing the data ecosystem. It may help custodian budgets by recovering costs incurred but present other challenges.

- There may be insufficient funds to perform proactive measures (e.g. updating an integrated dataset with the latest available data) which results in data requestors needing to wait for this action to be undertaken after their request has been approved and they have paid the user fee.
- Timeframes for decision making or providing access may not improve if a custodian underestimates the level of demand for data sharing, and the allocated staffing capacity is limited even though requestors are prepared to pay the user fee.

- Conversely, budget implications arise for data custodians who overestimate the level of demand for data sharing and result in underutilised staff capacity whose costs are never recovered from users.

452. Using third parties to access additional capability (for example, a secure access data service) may reduce the resource burden on the custodian directly, but the costs of these services may still need to be passed on to the user. Comparing AIHW and ABS secure access data service fees with equivalent non-government service fees shows comparable user fees (Sax Institute 2025a; UNSW 2025).

453. The reverse approach to the cost recovery model would be for the custodians to be resourced directly by the Government to remove the need for user charges. This may not be a sustainable approach as, on face value, it risks invoking a quintessential 'tragedy of the commons' scenario. The resources made available to custodians could be quickly consumed by individual projects and data users at the expense of the broader user community.

454. A mixed approach may open more sustainable opportunities and balance custodian resourcing while reducing barriers to entry. For example, if custodian's fixed costs are funded by the Government, then only the custodian's variable costs need to be charged back to user. Using this approach, the user only pays for the marginal work conducted by the custodian that is directly attributed with their data sharing project.

Recommendation 15

Further investment in the data ecosystem is required to improve capability and enable better outcomes for participants.

455. A new leadership function for Commonwealth data sharing could provide greater strategic direction for the data sharing ecosystem, including the National Data Commissioner and the DAT Act, and drive structural changes to help 'unblock' Commonwealth government data sharing. Initially, it could focus on the following outcomes across the entire Commonwealth government data sharing ecosystem.

456. Outcome 1: data is more accessible to users.

- Non-sensitive data continues to be released as open data, and custodians can access additional capability to curate or apply data protection treatments to the data (see Recommendation 10).
- Data custodians are confident that sensitive data is suitable for sharing and make their datasets discoverable and accessible to users (providing information such as metadata and pathways to access data).
- Data platforms and infrastructure make it easier for requestors to discover public sector data holdings available across the Commonwealth.

457. Outcome 2: data access pathways are easier for users to navigate.

- Requestors understand the difference between different data sharing and information access schemes and can confidently request access under the appropriate scheme.

- Data sharing processes and platforms achieve greater standardisation to streamline and simplify the data user journey (even though different legislative frameworks may be in effect).

458. Outcome 3: access decisions are timely, consistent and transparent.

- Data custodians are equipped to understand and manage risks when making a decision on a data sharing request.
- Data custodians are resourced to provide requestors with timely access to data once their request is approved.
- Effective and responsive dispute resolution pathways (including the National Data Commissioner – see Recommendation 4) allow for decisions to be reviewed.
- Data platforms and data assets are maintained and enhanced to proactively address emerging data needs.

459. Outcome 4: greater transparency and strategic decision-making for the ecosystem.

- The leadership function for Commonwealth data sharing provides a central role to lead and advocate for system-wide change or investment to realise improved data sharing outcomes.
- Information on data sharing outside of the DAT Act is available to diagnose the health of the ecosystem, inform decisions and prioritise improvements.
- Data custodians, users and other stakeholders collaborate to shape whole of system outcomes.

460. A baseline dataset of data sharing across the Commonwealth is needed to inform policy and investment decisions for the entire ecosystem. It should be a mandatory requirement across all data sharing frameworks and can be required by amending legislation (for example, the Public Governance, Performance and Accountability Rule 2014 or the DAT Act), or introducing non-legislative mandates (for example, through a Cabinet Minute).

461. It is clear from the feedback and facts gathered for this review that leadership of the data-sharing ecosystem can help to focus and lead initiatives, mandate solutions to improve discoverability and processes.

462. If the role of the National Data Commissioner is to be revised to focus more narrowly on enabling and supporting use of the DAT Act (Recommendation 4), the Department of Finance's Data Policy and Assurance Branch is an option to provide the leadership function for the Commonwealth data sharing ecosystem. The Branch currently provides strategic direction for public sector data generally and engages with stakeholders across government and non-government sectors on data-related issues. However, other parts of government are also capable of performing the leadership function.

463. The leadership function for the Commonwealth data sharing ecosystem should have a broad scope of responsibility and influence, including to:

- lead strategic decisions and collaboration between Commonwealth and government agencies and the research sector
- gather evidence on non-legislative issues that may impede public sector data sharing

- advise Government on the implications that changes in frameworks (including the DAT Act), platforms and capability will have on existing capacity and data sharing risks, and
- ensure that Government money (appropriation and grants) is spent effectively to improve the data sharing ecosystem and avoids unnecessary duplication.

464. Vesting data-sharing leadership in another agency will allow the National Data Commissioner to focus on its DAT Act role and is an opportunity for some work programs to be relocated under the remit of a new leadership function for Commonwealth data sharing with the positional authority, tools and levers to support the development and uplift of broader ecosystem solutions. Candidate programs for relocation include the Dataplace platform, which could be expanded in scope to better facilitate sharing requests made under other data sharing frameworks, and the Australia Government Data Catalogue, which could be hosted within Dataplace, or an alternative platform such as data.gov.au. The Department of Finance, which already supports whole of APS IT platforms, is an option to host and evolve these platforms under the responsibility of the new leadership function.

Implementation

465. Without legislative intervention, the DAT Act will sunset on 1 April 2027 (section 143).

466. The Review notes that if its recommendations are adopted, it may be necessary to extend the operation of the DAT Act while the necessary amendments are made to the Act to prevent it sunsetting before they can be implemented. This could be done through a targeted amendment to extend the sunsetting date ahead of substantive amendments being enacted.

467. Each of the recommendations proposed by the Review are intended to improve the operation of the DAT Act, or data sharing more generally. However, if only certain recommendations were to be prioritised, the Review considers Recommendations 1 to 3 to be essential.

468. These recommendations are critical to resolving the challenges experienced with the current DAT Act settings and will require legislative changes to the DAT Act. They are focused on delivering on the expectations of the DAT Act's framework, and increased data sharing will not occur without them. If these recommendations are not implemented, the DAT Act's authorising framework will continue to be ineffective and underutilised, and should instead be allowed to sunset.

469. While the other recommendations presented by this Review are important, they build on the foundations established in Recommendations 1 to 3 or relate to broader issues with data sharing.

470. Recommendations 4 to 11, 13 and 14 will require legislative changes to implement. In contrast, Recommendations 12 and 15 could be implemented without legislative change.

471. While specific changes to the DAT Act could be used to embed Indigenous data governance frameworks into decision-making processes under the DAT Act (Recommendation 12), such processes could also be implemented through requirements imposed administratively by the National Data Commissioner, or through policy decisions enacted at the Commonwealth level (for example, though Commonwealth data custodians).

472. Further investments in the data sharing ecosystem (Recommendation 15) could also be implemented through policy decisions or by leveraging existing legislative frameworks.

References

Origins of the DAT Act

Department of the Prime and Cabinet (2018) *The Australian Government's response to the Productivity Commission Data Availability and Use Inquiry*, Productivity Commission website, accessed 24 July 2025.

Deloitte Access Economics (2023) *The economic value of government precompetitive geoscience data and analysis for Australia's resource industry*, accessed 5 August 2025.

Department of the Treasury (2015) *Competition Policy Review – Final Report*, Department of the Treasury website, accessed 05 August 2025.

Department of the Treasury (2014) *Financial System Inquiry – Final Report*, accessed 5 August 2025.

Lateral Economics (2019) *Valuing the Australian Census*, Lateral Economics website, accessed 5 August 2025.

PC (Productivity Commission) (2017) *Data Availability and Use – Inquiry Report*, PC website, accessed 26 June 2025.

Current state of public sector data sharing

ABS (Australian Bureau of Statistics) (n.d.) *ABS Data Strategy 2021-22 to 2025*, ABS website, accessed 3 October 2025.

Australian Government (2023) *Government Response to the Privacy Act Review,* Australian Government website, accessed 11 August 2025.

AIHW (Australian Institute of Health and Welfare) (2022) *Strategic directions 2022-2026,* AIHW website, accessed 3 October 2025.

DCCEEW (Department of Climate Change, Energy, the Environment and Water) (2024) *Enterprise Data Strategy 2024-27,* DCCEEW website, accessed 3 October 2025.

Department of Education (2023) *Data Strategy 2023-25,* Department of Education website, accessed 3 October 2025.

Department of Finance (2023a) *Australian Government Charging Policy,* Department of Finance website, accessed 3 October 2025.

Department of Finance (2023b) *Australian Government Cost Recovery Policy,* Department of Finance website, accessed 3 October 2025.

Department of Finance (2024a) *Data Integration Partnership for Australia,* Department of Finance website, accessed 3 October 2025.

Department of Finance (2024b) *Data and Digital Ministers Meeting - Terms of Reference,* Department of Finance website, accessed 30 September 2025.

Department of Finance (2024c) *CDO pack attachments,* Department of Finance website, accessed 30 September 2025.

Department of Finance (n.d) *Intergovernmental Agreement on Data Sharing*, Department of Finance website, accessed 25 September 2025.

Department of Health and Aged Care (2022) *Data Strategy 2022-2025,* Department of Health and Aged Care website, accessed 3 October 2025.

DSS (Department of Social Services) (2024) *Data and Analytics Strategy 2025-2027,* DSS website, accessed 3 October 2025.

DEWR (Department of Employment and Workplace Relations) (2024) *Department of Employment and Workplace Relations Data Strategy 2024-2027,* DEWR website, accessed 3 October 2025.

Government of South Australia (2020) *PC 012 – Information Privacy Principles (IPPs) Instruction,* Premier and Cabinet Circular, Department of Premier and Cabinet website, accessed 3 October 2025.

Gruen, D. (2020) *The promise of data in government,* Address to IPAA ACT, ABS website, accessed 7 August 2025.

PC (2023) *Advancing Prosperity - 5-year Productivity Inquiry report,* PC website, accessed 3 October 2025.

PC (2025a) *Investing in Cheaper, cleaner energy and the net zero transformation, Interim report*, PC website, accessed 3 October 2025.

PC (2025b) *Harnessing data and digital technology, Interim report*, PC website, accessed 3 October 2025.

Operation of the DAT Act

Department of Finance (2025a) *Portfolio Additional Estimates Statements 2024-25: Finance Portfolio*, Australian Government, accessed 12 August 2025.

Department of Finance (2025b) *Portfolio Budget Statements 2025-26: Budget related paper no. 1.7*, Australian Government, accessed 12 August 2025.

ONDC (2022a) *Ministerial Statement of Expectations*, ONDC website, accessed 12 August 2025.

ONDC (2022b) *Statement of Intent*, ONDC website, accessed 12 August 2025.

ONDC (2025a) *National Data Advisory Council*, ONDC website, accessed 12 August 2025.

ONDC (2025b) *Annual Priorities 2025-26*, ONDC website, accessed 12 August 2025.

Revised Explanatory Memorandum (Revised EM 2022), Data Availability and Transparency Bill 2022, accessed 12 August 2025.

Effectiveness of the DAT Act and Commonwealth data sharing

Department of Finance (2024) Australian Public Service Data Maturity Report 2024, Department of Finance website, accessed 13 August 2025.

Digital Transformation Agency, Data and Digital Government Strategy, accessed 13 August 2025.

ONDC, *Accredited Entity Register*, ONDC website, accessed 13 August 2025.

ONDC (2024) DATA Scheme Working Group, November 2024, ONDC website, accessed 13 August 2025.

Legislative complexity and inflexibility in a voluntary framework

AIHW (n.d.) 'Key information gaps and development activities', *Family domestic and sexual violence*, AIHW website, accessed 30 September 2025.

ALRC (Australian Law Reform Commission) (2010a) 'Regulatory Theory', *For Your Information: Australian Privacy Law and Practice*, ALRC Report 108, accessed 22 September 2025.

ALRC (2010b) *Secrecy Laws and Open Government in Australia,* ALRC Report 112, Australian Government, accessed 2 October 2025.

ALRC (2021) *Background Paper FSL2 Legislative Framework for Corporations and Financial Services Regulation: Complexity and Legislative Design*, ALRC, Australian Government, accessed 22 September 2025.

ALRC (2022) Measuring Legislative Complexity, ALRC website, accessed 22 September 2025.

ALRC (2023) *Confronting Complexity: Reforming Corporations and Financial Services Legislation*, ALRC Report 141, Australian Government, accessed 22 September 2025.

AGD (Attorney-General's Department) (2014) *Clearer Commonwealth Laws: causes of complex legislation and strategies to address these*, Attorney-General's Department, Australian Government, accessed 22 September 2025.

Bennett Moses L (2020) 'Who owns information? Law enforcement information sharing as a case study in conceptual confusion', *UNSW Law Journal* 43(2):615-641.

Burton Crawford L, Akand E, Contractor S, and Scott Sisson (2022) 'Legislative complexity: what is it, how do we measure it, and why does it matter?' *AUSPUBLAW*, accessed 30 September.

Coade M (21 June 2024) 'Longitudinal data on gender-based violence in Australia to boost policy approach', *The Mandarin*, accessed 30 September 2025.

ICO (Information Commissioner's Office) (2022) *Data sharing: a code of practice*, UK Government, accessed 29 September 2025.

Lievesley D (2025) *Independent Review of the UK Statistics Authority by Professor Denise Lievesley CBE*, UK Government, accessed 22 September 2025.

Nolan B and Reid T (1994) 'Re-writing the Tax Act' *Federal Law Review* 22(3):448-460.

ONDC (n.d.) *The National Data Commissioner's Advice Function*, ONDC website, accessed 2 October 2025.

ONDC (2024) *Data Scheme Working Group Findings and Actions*, ONDC website, accessed 30 September 2025.

OPC (Office of Parliamentary Counsel) (2016) *OPC's Guide to Reducing Complexity in Legislation*, Office of Parliamentary Counsel, Australian Government, accessed 22 September 2025.

OSR (Office for Statistics Regulation) (2023) *Data Sharing and Linkage for the Public Good*, UK Government, accessed 22 September 2025.

OSR (2025) *Data Sharing and Linkage for the Public Good: Follow-Up Report*, UK Government, accessed 22 September 2025.

PA Consulting (2025) *Data-sharing: The beating heart of a successful public sector*, report prepared in partnership with the Office for National Statistics (UK), the Infrastructure and Projects Authority, and the Blavatnik School of Government (University of Oxford), UK Government, accessed 22 September 2025.

Pinder G (2005) 'The Coherent Principles Approach to Tax Law Design', *Economic Roundup* Autumn 2005:75–90.

PC (2025) *Harnessing data and digital technology: Interim report*, Australian Government, accessed 30 September 2025.

Revised Explanatory Memorandum (Revised EM 2022), Data Availability and Transparency Bill 2022, accessed 7 October 2025.

Royal Commission into Defence and Veteran Suicide (2024) 'Volume 6: Families, data and research, and establishing a new entity', *Final Report*, accessed 26 September 2025.

Supplementary Explanatory Memorandum (Supplementary EM 2022), Data Availability and Transparency Bill 2022, accessed 7 October 2025.

The National Data Commissioner's Functions and Powers

Australian Government (2023) *Data and Digital Government Strategy: Implementation Plan*, accessed 25 September 2025.

Australian Government (2024) *Data and Digital Government Strategy: Implementation Plan*, accessed 25 September 2025.

Department of Finance (2025) *Data Maturity Assessment Tool*, Department of Finance, Australian Government, accessed 7 October 2025.

Mesman D (8 May 2024) 'Move over big data: Data inventories are the next big thing', *The Mandarin*, accessed 25 September 2025.

ONDC (n.d.) *Annual Priorities 2025-26*, ONDC website, accessed 25 September 2025.

ONDC (2024) *Annual report 2023-24*, ONDC, Australian Government, accessed 25 September 2025.

Soncul M (7 April 2025) 'Unlocking data sharing across government', *Data in government blog*, UK Government, accessed 25 September 2025.

Accreditation Framework

Australian Signals Directorate (2024) *The Commonwealth Cyber Security Posture in 2024*, Australian Signals Directorate website, accessed 12 August 2025.

Grepperud S, and Pedersen P A (2020) 'Accreditation in regulated markets', *Managerial and Decision Economics*, 41(7):1287-1304, doi: 10.1002/mde.3175.

Hämäläinen K, Mustonen K, and Holm K (2004) 'Standards, criteria, and indicators in programme accreditation and evaluation in Western Europe' in Vlasceanu L, and Barrow L C (eds) *Indicators for institutional and programme accreditation in higher/tertiary education*, Bucharest: UNESCO-CEPES, 17-32.

Harvey L, and Green D (1993) 'Defining Quality', *Assessment and Evaluation in Higher Education*, 18: 9-34, doi: 10.1080/0260293930180102.

Kumar A, Paliwal J, Singh M, Pendse V, Gade R, Palav M, and Raibagkar S (2025) 'Focused literature review on accreditation and quality assurance: insights and future research agenda', *Quality Assurance in Education*, 33(3):376-392, doi: 10.1108/QAE-08-2024-0170.

ONDC (2022) *Sample user accreditation form,* ONDC website, accessed 12 August 2025.

ONDC (2024) *DATA Scheme Working Group: Findings and Actions*, ONDC website, accessed 5 August 2025.

ONDC (2025) *Updates from the DATA Scheme Working Group*, ONDC website, accessed 5 August 2025.

van Damme D (2004) 'Standards and indicators in institutional and programme accreditation in higher education: A conceptual framework and a proposal' in Vlasceanu L, and Barrow L C (eds) *Indicators for institutional and programme accreditation in higher/tertiary education*, Bucharest: UNESCO-CEPES, 127-160.

Participation Expansion

Aged & Community Services Australia (2021) *Pre-Budget Submission 2021–22,* Department of the Treasury website, accessed 29 August 2025.

Australian Accounting Standards Board (2021) *Standard-Setting Policies and Processes (*Not-for-Profit Entity Standard-Setting Framework*)*, accessed 1 September 2025.

ACNC (Australian Charities and Not-for-profits Commission) (2025) *Not-for-Profit,* Australian Charities and Not-for-profits Commission website, accessed 29 August 2025.

AIHW (2016) *Australia's Health 2016*, AIHW website, accessed 29 August 2025.

Bleicher K, Summerhayes R, Baynes S, Swarbrick M, Navin Cristina T, Luc H, Dawson G, Cowle A, Dolja-Gore X, and McNamara M (2023), 'Cohort profile update: the 45 and up study'. *International Journal of Epidemiology*, 52(1):e92-e101, doi: 10.1093/ije/dyac104.

Bryant G, and Spies-Butcher B (2024) 'From marketisation to self-determination: Contesting state and market through 'justice reinvestment''. *Environment and Planning A: Economy and Space*, 56(1): 216-234, doi: 10.1177/0308518X221125797.

Centre for International Corporate Tax Accountability and Research (2020) *Caring for Growth: Australia's Largest Non-Profit Aged Care Operators*, Centre for International Corporate Tax Accountability and Research website, accessed 1 September 2025.

Coalition of Peaks and Council of Australian Governments (2020) *National Agreement on Closing the Gap*, Coalition of Peaks and Council of Australian Governments, accessed 1 September 2025.

Department of Health (2018) *Evaluation of the Primary Health Networks Program*, Department of Health, Disability and Ageing website, accessed 1 September 2025.

Department of Health (2021) *Australian Government response to the final report of the Royal Commission into Aged Care Quality and Safety*, Department of Health, Disability and Ageing website, accessed 1 September 2025.

Department of Health, Disability and Ageing (2025) *What Primary Health Networks do*, Department of Health, Disability and Ageing website, accessed 1 September 2025.

Government of Western Australia (2022) *Aboriginal Community Controlled Organisation Strategy 2022–2032*, Government of Western Australia website, accessed 1 September 2025.

Hughes E K, Siero W, Clifford S A, Frugier T, Hall SM, *et al.* (2025) 'Generation Victoria (GenV): protocol for a longitudinal birth cohort of Victorian children and their parents, *BMC Public Health,* 25(2), doi: 10.1186/s12889-024-21108-1.

KPMG (2018a) *Economic Impact of Medical Research in Australia [pdf]*, Association of Australian Medical Research Institutes website, accessed 1 September 2025.

KPMG (2018b) *Maranguka Justice Reinvestment Project: Impact Assessment*, Australian Institute of Criminology website, accessed 1 September 2025.

Mackean T, Freeman T, Musolino C, Fry D, MacDougall C, Lewis V, and Baum F (2025) 'Leading the way: the contribution of Aboriginal community controlled health organisations to community health in Australia', *Australian Journal of Primary Health*, 31(3), doi: 10.1071/PY24223.

McLeod F (2017) *National interest and the rule of law*, ACT Law Society website, accessed 5 September 2025.

NSW Health (2025) *About Lumos, NSW Health website, accessed 4 September 2025.*

OAIC (Office of the Australian Information Commissioner) (2018), *New Australian Government Data Sharing and Release Legislation – Submission to the Department of Prime Minister and Cabinet*, Office of the Australian Information Commissioner website, accessed 1 September 2025.

Paige E, Welsh J, Joshy G, Weber M F, Banks E (2022) 'The 45 and Up Study: reflecting on contributions to global evidence using case studies on cardiovascular disease and smoking', *Public Health Research and Practice*, 13;32(4):e3242233, doi: 10.17061/phrp3242233.

Royal Commission into Aged Care Quality and Safety (2021) 'Volume 1: Summary and Recommendations', *Final Report*, accessed 25 August 2025.

Victorian Department of Jobs, Skills, Industry and Regions (2024) *Case study - Generation Victoria*, Victorian Department of Jobs, Skills, Industry and Regions website, accessed 29 August 2025.

Wheeler C (2006) 'The public interest we know it's important, but do we know what it means', *AIAL Forum*, 48:12-25, doi: 10.3316/ielapa.200605460.

Data Sharing Purposes

Johnston L R (ed) (2017) *Curating Research Data: Volume One – Practical Strategies for Your Digital Repository*, Association of College and Research Libraries, Chicago, IL.

ONDC (2025) *Data sharing purposes*, ONDC website, accessed 8 September 2025.

Spectrum of data sharing interests

ABS (2024) *PLIDA data and legislation,* ABS website, accessed 25 September 2025.

ABS (2021) *Using DataLab responsibly,* ABS website, accessed 25 September 2025.

Australian Indigenous Governance Institute and Maiam nayri Wingara (2018). *Indigenous Data Sovereignty Communique,* Indigenous Data Sovereignty Summit 20th June 2018, Canberra, ACT, Australian Indigenous Governance Institute website, accessed 25 September 2025.

AIHW (2024) *AIHW Ethics Committee (the Committee) Terms of Reference,* AIHW website, accessed 25 September 2025.

AIHW (2023) *Researcher resources,* AIHW website, accessed 25 September 2025.

Butler, Anderson et al (2025). *Co-design Versus Faux-design of Aboriginal and Torres Strait Islander Health Policy: A Critical Review,* Lowitja Institute website, accessed 25 September 2025.

Coalition of Peaks and Council of Australian Governments (2020) *National Agreement on Closing the Gap*, Coalition of Peaks and Council of Australian Governments, accessed 1 September 2025.

Kukutai, T., Cassim, S., Clark, V., Jones, N., Mika, J., Morar, R., Muru-Lanning, M., Pouwhare, R., Teague, V., Tuffery Huria, L., Watts, D. & Sterling, R. (2023) *Māori data sovereignty and privacy. Tikanga in Technology discussion paper,* accessed 25 September 2025.

NHMRC (National Health and Medical Research Council) (2023) *National Statement on Ethical Conduct in Human Research 2023,* NHMRC website, accessed 25 September 2025.

NIAA (National Indigenous Australians Agency) (2023) *Co-Design Lessons Learned Report,* NIAA website, accessed 25 September 2025.

NIAA (2024) *Framework for Governance of Indigenous Data,* NIAA website, accessed 25 September 2025.

ONDC (2024) *Data Scheme Working Group – Findings and actions, November 2024,* ONDC website, accessed 25 September 2025.

ONDC (2025) *National Data Advisory Council,* ONDC website, accessed 25 September 2025.

PC (2025) *Measuring outcomes for First Nations communities, Productivity Commission submission,* Select Committee on Measuring Outcomes for First Nations Communities, Submission 20, Australian Parliament House website, accessed 10 October 2025.

Rose, J., Langton, M., Smith, K., & Clinch, D. (2023) *Indigenous data governance in Australia: Towards a national framework,* The International Indigenous Policy Journal, Volume 14(1), accessed 25 September 2025.

Broader systems and capability

ABS (2025) *Microdata and TableBuilder: Census of Population and Housing*, ABS website, accessed 25 September 2025.

ABS (2024) *Annual report 2023-24*, ABS website, accessed 25 September 2025.

ABS (2022) *Charges - DataLab*, ABS website, accessed 25 September 2025.

Australian Government (2025) *Consumer Data Right*, Consumer Data Right website, accessed 3 October 2025.

AIHW (2025a) *National Health Data Hub, Approved projects and status*, AIHW website, accessed 25 September 2025.

AIHW (2025b) *National Health Data Hub – Researcher access, grant submissions & costs,* AIHW website, accessed 25 September 2025.

AIHW (2024) *Annual report 2023-24,* AIHW website, accessed 25 September 2025.

APSC (Australian Public Service Commission) (2025a) *2024 APS Employee Census,* data.gov.au website, accessed 25 September 2025.

APSC (2025b) *APS Remuneration Data, 31 December 2024*, APSC website, accessed 3 October 2025.

Department of Finance (2024) *Australian Public Service Data Maturity Report 2024*, Department of Finance website, accessed 25 September 2025.

Department of Finance (2025a) *Australia's Digital ID system,* Department of Finance website, accessed 3 October 2025.

Department of Finance (2025b) *Data Maturity Assessment Tool*, Department of Finance website, accessed 25 September 2025.

Department of Finance (2024) *Australian Public Service Data Maturity Report 2024*, Department of Finance website, accessed 25 September 2025.

Griffith University (n.d.) *Relational Insights Data Lab,* Griffith University website, accessed 25 September 2025.

Melbourne Institute of Applied Economic and Social Research (2025) *Melbourne Institute Data Lab,* Melbourne Institute of Applied Economic and Social Research website, accessed 25 September 2025.

NDDA (National Disability Data Asset) (2025a) *Apply for data access*, NDDA website, accessed 25 September 2025

NDDA (2025b) *Infrastructure*, NDDA website, accessed 25 September 2025.

ONDC (2024) *Guide to developing a data inventory*, ONDC website, accessed 25 September 2025.

Sax Institute (2025a) *SURE user fees*, Sax Institute website, accessed 25 September 2025.

Sax Institute (2025b) *What is SURE?*, Sax Institute website, accessed 25 September 2025.

UNSW (University of New South Wales) (2025) *ERICA – E-Research Institutional Cloud Architecture*, UNSW website, accessed 25 September 2025.

Legislation

Charities Act 2013 (Cth)

Corporations (Aboriginal and Torres Strait Islander) Act 2006 (Cth)

Data Availability and Transparency Act 2022 (Cth)

Data Availability and Transparency Code 2022 (Cth)

Data Availability and Transparency (Consequential Amendments) Transitional Rules 2022 (Cth)

Data Availability and Transparency (National Security Measures) Code 2022 (Cth)

Data Availability and Transparency Regulations 2022 (Cth)

Data (Use and Access) Act 2025 (UK)Digital Economy Act 2017 (UK)

Freedom of Information Act 1982 (Cth)

Privacy Act 1988 (Cth)

Privacy and Responsible Information Sharing Act 2024 (WA)

Public Governance, Performance and Accountability Act 2013

Public Governance, Performance and Accountability Rule 2014

Regulatory Powers (Standard Provisions) Act 2014 (Cth)

Appendices

Appendix A: Submissions, meetings and other engagements

Appendix A1: Submissions to the Issues Paper

Submission No.	Submission
1	ACT Government
2	ANDHealth
3	Anonymous 1
4	Anonymous 2
5	Association of Australian Medical Research Institutes
6	Attorney-General's Department
7	Australian Academy of Science
8	Australian Banking Association
9	Australian Bureau of Statistics
10	Australian Computer Society
11	Australian Curriculum Assessment and Reporting Authority
12	Australian Institute of Health and Welfare
13	Australian Research Data Commons
14	Business Council of Australia
15	David Kalisch
16	Department of Education
17	Department of Employment and Workplace Relations
18	Department of Health, Disability and Ageing
19	Department of Home Affairs
20	Department of Industry, Science and Resources
21	Department of Social Services
22	Digital Transformation Agency
23	Electronic Frontiers Australia Inc.
24	Flinders University
25	Geoscape Australia
26	Geoscience Australia
27	Indigenous Data Network
28	Information and Privacy Commission NSW
29	IoT Alliance Australia
30	James Cook University
31	Jobs and Skills Australia
32	KPMG
33	Medical Software Industry Association Ltd
34	Melbourne Disability Institute
35	Melbourne Institute of Applied Economic and Social Research

36	Monash University
37	National Archives of Australia
38	National Data Commissioner
39	National Emergency Management Agency
40	National Indigenous Australians Agency
41	Northern Territory Government
42	Office of the Australian Information Commissioner
43	Office of the Information Commissioner Queensland
44	Office of the Victorian Information Commissioner
45	Population Health Research Network
46	Professor Lyria Bennett Moses and Nicholas Hodgkinson
47	Prospection
48	Psithur
49	Queensland Cyber Infrastructure Foundation
50	Research Alliance for Youth Disability and Mental Health and the CRE in Achieving Health Equity for All People with Disabilities
51	Research Australia
52	Seer Data & Analytics, Greater Shepparton Lighthouse Project, and Maranguka Community Hub
53	Services Australia
54	Social Research Centre
55	South Australian Department for Health and Wellbeing
56	Universities Australia
57	University of Adelaide
58	University of Melbourne
59	University of Queensland
60	University of Sydney
61	University of Tasmania
62	University of Western Australia

Appendix A2: Submissions to the Draft Findings and Recommendations Paper

Submission No.	**Submission**
63	Australian Computer Society
64	Australian Institute of Health and Welfare
65	Australian Research Data Commons
66	Conexus Institute
67	Data Synergies
68	Department of Education
69	Department of Health, Disability and Ageing
70	Dr Phillip Gould (Acting Australian Statistician)
71	Equifax
72	Information and Privacy Commission NSW
73	Monash University
74	National Data Commissioner
75	National Emergency Management Agency

76	National Indigenous Australians Agency
77	Office of the Australian Information Commissioner
78	Office of the Information Commissioner (Qld)
79	Population Health Research Network
80	Professor Lyria Bennett Moses & Nicholas Hodgkinson
81	Seer Data and Analytics (and partners)
82	Services Australia
83	University of Melbourne
84	University of Queensland
85	University of Sydney
86	University of Tasmania
87	Western Australia Department of Premier and Cabinet

Appendix B: DAT Bill amendments

The Senate Standing Committee for the Scrutiny of Bills requested amendments to the DAT Bill to include a public interest test prioritising privacy interests in decision-making and to provide guidance about the circumstances in which it would be unreasonable or impracticable to seek an individual's consent for sharing their personal information (Scrutiny Committee 2021a).[210] The Scrutiny Committee further requested an addendum to the DAT Bill's Explanatory Memorandum be tabled in the Parliament explaining the breadth of the 'unreasonable or impractical' exception (Scrutiny Committee 2021b).

The Minister agreed to these requests and further advised (DAT Bill 2020a):

> The bill's approach to consent mirrors the approach in the Privacy Act, requiring consent be sought for the sharing of personal information, unless unreasonable or impracticable.
>
> The bill also includes other privacy-enhancing measures, such as data minimisation.
>
> Importantly, the bill will work with new regulations to exclude sharing of particularly sensitive data, such as the electoral roll, My Health Record and COVIDSafe app data.
>
> The National Data Commissioner will champion these safeguards and cooperate with other regulators, such as the Australian Information Commissioner, to ensure personal information is handled appropriately under the scheme.

The Senate referred the DAT Bill to the Senate Finance and Public Administration Committee. The Committee responded on 29 April 2021, and the majority of senators recommended that (Senate Legislation Committee 2021a):

- assurances be provided to Parliament regarding appropriate ongoing oversight by security agencies of data sharing agreements and potential security risks
- any relevant findings of the Parliamentary Joint Committee on Intelligence and Security inquiry into national security risks affecting the Australian higher education and research sector be taken into account as part of the development of any additional data codes and guidance material and inform continued engagement with the national security community
- consideration be given to amendments to the DAT Bill, or further clarification in the Explanatory Memorandum, to provide additional guidance regarding privacy protections, particularly in relation to the de-identifying of personal data that may be provided under the DAT Bill's data sharing scheme.

The Labor Party Senators (the then Opposition) on the Committee issued a dissenting report recommending that the DAT Bill not be passed. The Senators stated that they were of the view that (Senate Legislation Committee 2021a):

[210] The functions of the Scrutiny Committee are to assess all bills introduced into the Parliament against a set of accountability standards that focus on the effect of proposed legislation on individual rights, liberties and obligations, the rule of law and on parliamentary scrutiny (Scrutiny Committee n.d.).

> While there is a clear need for an effective scheme for the management and regulation of public data, and clear public benefits from using such data, the measures outlined in this bill do not represent a proportionate means of achieving that objective. If passed, the scheme outlined in the bill would undermine current privacy protections, most notably the *Privacy Act 1988*.

Following discussions between the then Government and the Opposition, the DAT Bill 2022 passed both Houses of Parliament on 30 March 2022 (DAT Bill 2022a). At that time, the then Opposition noted concerns that (DAT Bill 2022b):

> …the privacy protections were insufficient for data which ultimately is the Australian people's data, not the government's…there were a lack of safeguards were this new system of data sharing to go wrong… the scope of the data-sharing scheme was excessively broad, proposing opening public data to foreign, non-Australian organisations… it was also excessive and highly problematic that such an untested new scheme was proposed to involve private corporations that would be able to apply for access to public data under the bill.

Appendix C: Current state of public sector data sharing – additional background

Part 1: Legal frameworks

This part outlines key legal frameworks that enable Commonwealth data custodians to share public sector data.

Aside from the DAT Act, there is a myriad of Commonwealth legislation dictating when and how data can be shared. These range from rules of general application to agency specific frameworks. Examples are set out below.

- *Archives Act 1983* (Cth)
    - This Act governs the management and access to Commonwealth records, including their preservation, disposal, and public access. The Act establishes the National Archives of Australia as the agency responsible for these functions and outlines the processes for accessing records.
- *Australian Institute of Health and Welfare Act 1987* (Cth) (AIHW Act)
    - The AIHW Act enables the AIHW to share data in certain circumstances (AIHW 2024). This includes appointing an AIHW Ethics Committee to advise on ethical matters concerning the collection and production of health and welfare-related information and statistics. AIHW (2022, pg 45) states that:

> Section 29 of the AIHW Act imposes strict confidentiality requirements that prohibit the release of documents and/or 'information concerning a person' held by the AIHW unless one of the following apply:
>
> • express written permission has been provided by the relevant data supplier(s);
>
> • release has been approved by the AIHW Ethics Committee;
>
> • the data are in the form of publications containing de-identified statistics, information and conclusions.
>
> In the absence of express approval of the data supplier(s) or the AIHW Ethics Committee

- *Census and Statistics Act 1905* (Cth) (CSA)
    - The CSA authorises the Australian Statistician to conduct statistical collections, including the Census of Population and Housing, and direct a person to provide statistical information. The CSA requires the ABS to publish and disseminate compilations and analyses of statistical information and to maintain the confidentiality of information collected. The CSA is used in conjunction with other legislation to authorise the linkage of data and creation of data assets (ABS n.d. a).
    - The CSA also empowers the responsible Minister to make determinations providing for the disclosure of data, with the current determination specifying

how the ABS may determine and impose conditions on disclosures of specific types of information to particular users.

- *Data-matching Program (Assistance and Tax) Act 1990* (Cth)
    - This Act enables a multi-agency data-matching program for identifying and preventing fraud, overpayments, and non-compliance in income support and tax systems. It authorises the controlled use of TFNs, and other personal data, by agencies like the ATO and Services Australia. The Act contains rules relating to privacy, sharing, storage and use cases.
- FOI Act
    - This legislation enables the public to access documents held by the Australian Government, including ministers and agencies, unless specific exemptions apply. It aims to promote transparency and accountability by allowing individuals to request information and ensures that government information is treated as a national resource.
    - Documents that contain data shared under the DAT Act are excluded from the operation of the FOI Act.
- Privacy Act
    - The Privacy Act is the primary Australian law regulating the handling of personal information. The Act aims to protect individual privacy by setting out principles for the collection, use, storage, and disclosure of personal information. The Act also includes provisions for handling sensitive information and regulates areas like consumer credit reporting and health records.
    - The Act is supported by Australian Privacy Principles (APPs) that govern standards, rights and obligations on the collection, use and disclosure of personal information, an organisation or agency's governance and accountability, integrity and correction of personal information and the rights of individuals to access their personal information (OAIC n.d.).
    - The DAT Act operates in conjunction with the Privacy Act to safeguard personal information. The DAT Act provides general privacy protections that limit the sharing of personal data, prohibit the re-identification of de-identified information, and restrict the storage or access of personal information outside Australia. Sharing biometric data always requires express consent. Additionally, the DAT Act includes purpose-specific privacy safeguards that apply depending on the intended use of the shared data (ONDC 2023).
    - The DAT Act is not intended to 'override' the Privacy Act. It is intended to facilitate the sharing of data consistently with the Privacy Act.

- *Taxation Administration Act 1953* (Cth)
    - This Act governs the use of 'protected information' for tax law purposes. It makes it an offence to disclose data obtained under a tax law if it relates to the affairs of an entity and is reasonably capable of being used to identify the entity. The Act also prescribes the circumstances in which disclosures of protected information may be made. These exceptions include purposes relating to administration of specified laws or programs and includes certain compliance activities.
    - Other exceptions connect tax data with other agency's data sharing frameworks. For example, section 355-65 authorises tax data to be disclosed (with safeguards in place) to the Australian Statistician for the purpose of administering the CSA, which enables the ABS to publish statistical information using ATO data and include ATO data in its data sharing framework.

Part 2: Governance

This part summarises the governance in place to support data sharing by Commonwealth data custodians. It outlines key strategies, standards and groups that provide leadership over how government manages public sector data.

Commonwealth Government strategies and standards

The Commonwealth Government has implemented strategies, frameworks and standards to target and support greater data availability and use. The following are key examples.

- Data and Digital Government Strategy
    - This outlines common rules, processes, and accountabilities for Commonwealth Government entities to ensure data quality, privacy, authority, and innovation. Key aspects include establishing data governance principles, roles, responsibilities, and processes for data acquisition, storage, use, and disposal. The strategy aims to deliver world-class data and digital capabilities to improve public services and outcomes for all Australians by 2030.
      The strategy outlines five key missions to guide Commonwealth Government entities data and digital transformation:
        - delivering for all people and business, which focuses on inclusive and accessible services
        - simple and seamless services, which aims to make interactions with government easy and efficient
        - government for the future, which emphasises adaptability and innovation.
        - trusted and secure, which prioritises data security and privacy
        - data and digital foundations, which focuses on building the necessary infrastructure and capabilities.

- Framework for the Governance of Indigenous Data
    - This Framework aims to create greater awareness and support for Indigenous Data Sovereignty amongst APS agencies. Co-designed with Aboriginal and Torres Strait Islander partners, the Framework supports increased agency of First Nations Australians in government-held Indigenous data across the data lifecycle and supports the National Agreement on Closing the Gap, Priority Reform Three (Transforming Government Organisations) and Priority Reform Four (Shared Access to Data at a Regional Level). The Framework recognises that better outcomes are achieved when First Nations people are genuinely engaged on matters affecting them, including on the use of data for policymaking and government service delivery.
- Information Asset Management Standard
    - This outlines expectations for organisations to manage information as an asset. It sets standards and best practice to align information requirements with organisational needs, comply with data-driven legislation, share information and collaborate with non-government organisations and First Nations people (DTA n.d. a).
- Digital Health Standards Catalogue
    - This resource supports ongoing digital transformation of the healthcare sector and enable different systems and applications to communicate and exchange data securely and reliably across the Australian healthcare system (ADHA n.d.).
- Five Safes framework
    - This framework is an internationally recognised model enshrined in the DAT Act for assessing and managing data sharing appropriate to the intended data use. The Framework poses specific questions to help assess and describe each risk aspect (or safe) in a qualitative way (ABS 2021, UWE n.d.).

Commonwealth governance groups

The Commonwealth Government uses several whole-of-government data governance groups to support consistent and effective data management across Commonwealth agencies (Department of Finance 2024b). These groups focus on various aspects of data governance, including information sharing, best practices, and strategic guidance. There are three key forums:

- Secretaries Digital and Data Committee (SDDC) is constituted by the Secretary of the Department of Finance, and heads of departments and agencies with large scale data collection and holdings, or digital policy responsibilities. The SDDC provides strategic leadership to promote an APS enterprise approach to the planning, coordination, investment, assurance, and delivery of trusted and secure digital and data across government. Regarding data sharing, the SDDC drives the adoption of common patterns, platforms, and services to promote the sharing and re-use of digital and data capabilities across government, consistent with the Commonwealth Government Architecture policies and standards.
- Deputy Secretaries Data Group (DSDG) consists of senior officials from all government departments and agencies with large scale data collection and holdings, or digital policy responsibilities. It is responsible for shaping and driving collaboration on a whole-of-government data agenda and supporting data and relevant digital initiatives under the APS Reform Plan.
- Chief Data Officers Group (CDO Group) consists of Chief Data Officers from all government departments and agencies with large scale data collection and holdings, or digital policy responsibilities. It is a strategic decision-making group providing stewardship for data at a whole of APS level. The CDO Group supports DSDG, and implementation of data-related commitments in the Data and Digital Government Strategy.

There are also a variety of informal groups such as communities of practice that are used by departments to suit their needs.

National governance groups

In addition to Commonwealth Government governance groups, a number of cross-government groups also operate to support improved outcomes from using public sector data.

- The Data and Digital Ministers Meeting (DDMM) is constituted by the Commonwealth Minister for data and/or digital matters and one ministerial representative responsible for data and or digital matters from each Australian jurisdiction and from New Zealand. Its purpose is to achieve cross-government collaboration on data and digital transformation to ensure smarter service delivery and improved outcomes (Department of Finance 2024c). Ministers investigate barriers to digital integration and data sharing within and across Commonwealth, state and territory governments.
- The DDMM Senior Officials Group (DDMM SOG) is a sub-group of DDMM and supports the implementation of the IGA and the National Data Sharing Work Program. It consists of senior officials across jurisdictions with portfolio responsibility for data or digital matters.
- Data and Analytics Working Group (D&AWG) consists of up to two representatives from state and territory departments and/or entities with data and digital responsibilities, and two representatives from the Commonwealth Department of Finance. It supports DDMM SOG to oversee the National Data Sharing Work Program and collaborates on and promotes data policy reform, to uplift data maturity and improve data sharing across Commonwealth and State and Territory governments.

- ANDII Board provides coordinated senior oversight of the design, build and management of ANDII, oversees ANDII's role supporting the priority data development for the NDDA, and provides strategic oversight on the further design, build, and operation of ANDII.

Part 3: Examples of Commonwealth data assets and platforms that enable data sharing

This part outlines several key examples of Commonwealth data assets (highly valuable datasets that are formed by integrating multiple public sector datasets held by different data custodians) and summarises the key platforms currently used to support Commonwealth data sharing and requests for data.

Commonwealth data assets

Australian Government entities have added value to their public sector data holdings by contributing towards enduring linked data assets, which greatly enhance the insights that can be gained from Commonwealth, State and Territory, and private sector administrative data. Existing data assets include:

- BLADE, which combines tax, trade and intellectual property data with information from ABS surveys to provide a better understanding of the Australian economy and businesses performance over time (ABS n.d. b). Authorised researchers use BLADE to understand how businesses fare over time and the factors that drive performance, innovation, job creation, competitiveness, and productivity, and provide new insights into the development and evaluation of government policies, programs and services.
    - BLADE currently comprises 57 datasets from Commonwealth, state and territory agencies, having grown from 10 datasets from Commonwealth agencies in 2017.
- PLIDA, which combines data about health, education, government payments, income and taxation, employment, and population demographics (including the Census) over time (ABS n.d. c). It provides whole-of-life insights about various population groups in Australia, such as the interactions between their characteristics, use of services like healthcare and education, and outcomes like improved health and employment. PLIDA can also be leveraged to create new, focussed assets (e.g. the Vocational Education and Training National Data Asset (VNDA)).[211]
    - PLIDA currently comprises 35 datasets from Commonwealth, state and territory agencies, having grown from 9 datasets from Commonwealth agencies in 2017. This is expected to increase to 62 by the end of 2025, expanding to include administrative data from non-government organisations.[212]
    - Over 5,000 researchers have accessed PLIDA and/or BLADE data through almost 800 projects since 2017. The number of active analytical projects accessing PLIDA and/or BLADE has grown from approximately 20 in 2017

[211] The VNDA is a project between the ABS and Jobs and Skills Australia to track the employment, economic and further study outcomes of VET students (Jobs and Skills Australia n.d.).
[212] Submission 9, ABS.

to 445 in April 2025. The number of active researchers and analysts trained to access these integrated data assets in the ABS secure facility, the DataLab, has grown from 29 in 2020 to 2,200 in 2025, across governments, academia and policy institutes.[213]

- The NHDH, which combines health and welfare data. It a longitudinal, person-focussed health linkage system comprising data from Commonwealth, state and territory and non-government data sources. It is unique among similar linkage assets in that it brings together hospital data on admitted patient care services, emergency department services and outpatient services for all states and territories (except for Western Australia and the Northern Territory) (AIHW 2025).

Platforms supporting data sharing

A number of Commonwealth platforms support data sharing. Some were designed as whole-of-Government data platforms while others were created for specific initiatives and have evolved to expand their service offering. Platforms such as ANDII have been created at the national level to service all jurisdictions.

- Australian Government Data Catalogue (AGDC) is a single portal to connect users to Australian Government data assets including open-source data as well as assets that have conditional or restricted access requirements.
    - The AGDC contains records for over 36,000 datasets from 70 data custodians. Of these, 150 datasets have restrictions on access (for example, requiring a formal request to access), 150 datasets have conditions of use (such as fees to access) and the remaining datasets are available as open datasets.
    - The majority of these records are populated via APIs with Geoscience Australia (over 25,000) and data.gov.au (over 10,000) and 22 custodians have directly contributed records for 187 datasets.
    - There has been limited uptake by data users since the Catalogue's launch on 8 July 2024. As of September 2025, there have been 5,485 site visits and 10,242 metadata records viewed. This contrasts with an average 1,000 views per day for data.gov.au (which as discussed below has a larger catalogue from a broader range of government users) (DTA n.d. b).
- Dataplace is a digital platform to request Australian Government data, develop a data sharing agreement or apply for accreditation under the DAT Act. It hosts the AGDC and allows users to request data from data custodians, lodge data sharing agreements, and provide transparency on data sharing activities (Dataplace n.d.).
    - as at 30 September 2025, 125 organisations have been onboarded to Dataplace (ONDC 2025)
    - the ONDC attributes the low uptake of Dataplace and the AGDC to misconceptions that Dataplace is only for DAT Act data sharing activities, the complexity of how the system develops a data sharing agreement,

[213] Submission 9, ABS.

and cultural resistance impeding custodians from moving off their established processes.[214]

- Data.gov.au was introduced in 2011 and is the central repository for open data created by all levels of Australian governments. As at 31 August 2025, data.gov.au has an average 1,000 website visits every day, and the platform contains 80,197 datasets from 1,065 organisations. Most datasets are from state and local governments (data.gov.au n.d.).
- Digital Atlas of Australia is a central platform to connect, explore and visualise data across different jurisdictions and systems. It contains a catalogue of location-based datasets that can be explored using interactive maps. In 2023-24, there was an increase of 46,000 individual active users and 169 new or updated location data products available to access (GA 2024, pg 32).
- Secure access environments (also referred to as TREs) include established Commonwealth platforms such as the ABS DataLab and AIHW Research Only Network, enable users to access sensitive data in a controlled way (ABS n.d. c; AIHW 2022). Solutions for safely accessing data are not limited to government platforms. Department of Social Services data (through the AIHW) and ATO data are made available using the Sax Institute's Secure Unified Research Environment (AIHW n.d.; ATO n.d.; Sax Institute n.d.).

In the absence of ready-to-use platforms, data custodians may use ad hoc processes to facilitate data sharing. For example, in the absence of a central register of data sharing arrangements (both under and outside of the DAT Act), data custodians may administer data sharing using numerous Microsoft Word or Excel documents held in different parts of the organisation.

Part 4: Examples of state-based data sharing frameworks and assets

State data sharing frameworks

South Australia

South Australia does not have legislation for general privacy but instead applies a Cabinet Administrative Instruction to set personal information handling requirements for government agencies (Government of South Australia 2020). Data sharing within South Australia pairs legislation (to enable data sharing for policy making, program management and service planning and delivery) and non-legislative guidelines (to enable data sharing that is required on an immediate-needs basis).

The *Public Sector (Data Sharing) Act 2016* (SA) was introduced in response to the Child Protection Systems Royal Commission (SA) which identified that '[c]aution about information sharing between government departments and other non-government services has created administrative barriers to meeting the needs of children' (Child Protection Systems Royal Commission (SA) (2016):XVIII). The Act's first data sharing project ensured

[214] Sourced additional information provided by the ONDC to the Review.

the South Australian government could meet its commitments to the Child Protection Systems Royal Commission Report (SA Treasury n.d. a).

The legislation operates in a decentralised data sharing environment and does not prevent or discourage data sharing using other legislation. The Act authorises SA agencies to share public sector data with other agencies despite any other South Australian law, with few exceptions. The Act also establishes the Office for Data Analytics which can direct agencies to provide data.

Data sharing between SA agencies and service providers can be authorised by an approved data sharing agreement. The Minister can also approve sharing across jurisdictions, to the broader research community and to the private sector. De-identified data is the default setting but sharing identifiable data is authorised under certain circumstances, including under general privacy provisions and for public safety purposes.

The Act utilises the Five Safes framework to guide agency decision making. While not prescribed in the Act, two committees: the State Social Data Asset Committee and State Economic Data Asset Committee provide oversight of state datasets, and consider certain data sharing requests before they can be approved (SA Treasury n.d. c).

South Australia's Information Sharing Guidelines for Promoting Safety and Wellbeing (ISG) (SA DPC n.d) are policy-level requirements that operates in parallel with the *Public Sector (Data Sharing) Act 2016* (SA). The ISG assists state service providers to share data when it is believed a person is at risk of harm and service delivery is required to avoid an adverse outcome. Data sharing under the ISG must be applied in a manner consistent with the organisation's legal obligations.

Queensland

Queensland does not have specific data sharing legislation and relies on the *Information Privacy Act 2009* (Qld) and agency specific legislation to legally authorise the sharing of personal information.

A non-legislative Information sharing authorising framework (Queensland Government 2022) was finalised in 2018 to ensure data sharing decisions were better informed and balanced the risk of sharing with the intended outcome. It does not override or replace legislative provisions. The framework sets out how to establish data sharing agreements that authorise consistent and repeatable data sharing.

Western Australia

Western Australia recently introduced data sharing legislation which integrates its data sharing enablers alongside its privacy requirements.

The *Privacy and Responsible Information Sharing Act 2024* (WA) was developed in response to a range of issues that made state public data sharing 'complicated, and at times, unworkable'.[215] It combines privacy protections and data sharing into a single act. This design was intentional and informed by the barriers that other jurisdictions experienced when adopting a data sharing framework separate to their privacy framework. The Act also established the role of the Chief Data Officer to build capability and provide assistance on

[215] Western Australia Privacy and Responsible Information Sharing Bill 2024, second reading, Page 1.

the Act (including by issuing guidelines), conduct analysis and maintain a register of data sharing agreements.

The Act enables agencies to share public sector data for public interest purposes across government and to other trusted entities. The legislation permits agencies to share data using the Act, or through other legislation. Under the Act, an approved data sharing agreement enables agencies to share data despite any secrecy provision that may otherwise apply, with few exceptions. Data can be shared between state public entities and additional requirements and expectations apply to cross-border sharing and sharing with other entities such as research institutions and service providers.

Special consideration is established for the sharing of Indigenous data, with an Indigenous data assessment used as a requirement to ensure that use of the data is culturally appropriate.

Examples of state and national data assets

In addition to the Commonwealth based assets and systems that authorises the sharing, collection and use of public sector data, state and national assets are routinely constructed through data sharing including:

- South Australian Business Research Environment (SABRE), which was launched in 2021 and links state administrative data from across different custodians to improve decision making on business and economic trends at the sectoral level (SA Treasury n.d. b). Following a successful pilot, SABRE intends to link with BLADE to provide a more accurate picture of the Australian economy as well as within SA (ABS n.d. a.).
- PeopleWA, which contains linked information on life events of people in Western Australia from across several state departments to address the most complex social, health, environmental and economic issues facing the state (WA DPC 2025).
- the Criminal Justice Data Asset is a longitudinal national data asset under development. It will show how people move through the justice system nationally so that approved policy-makers and researchers can analyse patterns of offending and inform policies to reduce recidivism (ABS 2023).
- ANDII is a foundational infrastructure asset developed by the ABS and the AIHW. ANDII supports the NDDA by enabling the secure and streamlined linkage and analysis of data from various sources. This infrastructure is built with cloud-based technology, offering enhanced security and scalability for data sharing and analysis (DTA n.d. c).
- the NDDA, which will bring together de-identified information from different government agencies about all Australians. Australian, state and territory governments are working with people with disability and the wider disability community on the NDDA. This asset will help government entities and the wider disability community to better understand the experiences of people with disability. The NDDA will provide more information about programs and services that will help to better support people with disability, their families, and carers (NDDA 2025).

Part 5: Examples of legislative frameworks and platforms used in other countries

This section provides an overview of select countries' legislative frameworks to enable data sharing, as well as examples of assets and platforms that other countries have developed for sharing data.

In comparing other countries systems, it is important to note that a range of factors (such a different political systems and citizen expectations) can impact public sector data sharing. A domestic example is Australia's federal system, which divides responsibility between different levels of government.

Public sector data sharing in the United Kingdom

Sharing of public sector data in the UK is enabled under specific legislation that allows a public authority to share information, or under the *Digital Economy Act 2017* (UK) (DEA), which authorises the sharing of personal information for defined purposes between specified public authorities (ICO 2022).[216] All public sector data sharing, however authorised, must comply with the UK's data protection legislation (the UK General Data Protection Regulation (UK GDPR) and the *Data Protection Act 2018* (UK) (DPA)). This includes complying with the following 'data protection principles' (ICO 2023):

- lawfulness, fairness and transparency
- purpose limitation
- data minimisation
- accuracy
- storage limitation
- integrity and confidentiality (security)
- accountability.

The DEA is comparable to the DAT Act as it provides a generally applicable authorisation to share public data. As with the DAT Act, the DEA was introduced 'to reduce legal barriers to information sharing and enable public authorities to share information, including personal data, for specific purposes' (Department for Science, Innovation & Technology (UK) 2025: paragraph 1).

The DEA includes specific 'powers' to share data (personal information) for particular purposes, including for public service delivery, debt, fraud, and research (DEA Part 5).[217] Codes of practice provide guidance for sharing data under each power, and must be consistent with the Data Sharing Code of Practice issued by the UK's Information Commissioner under the DPA (DEA subsections 43(2), 52(2), 60(2), and 70(2)). Codes of practice are generally issued by the relevant Minister, but the code of practice covering the research data sharing power is issued by the UK's Statistics Authority (DEA,

[216] The terms 'personal information' in the DEA and 'personal data' in the data protection legislation have slightly different meanings. Public sector bodies sharing data are required to apply both definitions and comply with both frameworks when sharing data (Code of Practice for public authorities disclosing information under chapters 1, 3 and 4 (Public Service Delivery, Debt and Fraud) of Part 5 of the Digital Economy Act 2017 (DEA Code of Practice, paragraphs 8-10).

[217] Sharing for other purposes, such as civil registration, is also enabled by the DEA, but will not be explored in this report. The DEA does not authorise a public authority which has functions relating to health services or adult social care to share such data for research purposes (DEA s 64(4)).

subsection 70(1); Research Code of Practice and Accreditation Criteria (Research Code of Practice)).

The DEA was recently amended by the *Data (Use and Access) Act 2025* (UK), which included reforms to some aspects of the data protection legislation and replaced the statutory office of the Information Commissioner with the new Information Commission.

Sharing data for service delivery

The DEA authorises a range of bodies to share and access data, including government agencies, local councils, and service providers.

The public service delivery powers in the DEA allow the sharing of information to support the well-being of individuals and households. Examples of purposes (referred to as 'objectives') for which personal information can be shared are enabling the targeting of public services to households that face multiple disadvantages and alleviation of fuel and/or water poverty. Objectives are set by regulations, and new objectives can be added (DEA subsections 35(7) to (12); *Digital Government (Disclosure of Information) Regulations 2018* (UK)). An example of a new objective set by regulations is sharing for the purposes of identity verification services (*Digital Government (Disclosure of Information) (Identity Verification Services) Regulations 2024* (UK)). Proposals to expand the objectives are submitted to the Public Service Delivery Review Board which provides advice to relevant Ministers on making regulations (DEA Code of Practice, paragraphs 75-82; UK Government n.d.).

Public sector data sharing generally involves the undertaking of a privacy impact assessment or data protection impact assessment, and arrangements must be captured on the publicly available register (DEA Code of Practice, part 2.5).[218]

The person to whom the data is disclosed must not use the shared data for other purposes (DEA, subsection 40(1)), except in specific circumstances, including for the prevention or detection of a crime (DEA, subsection 40(2)). On-disclosure of personal information is also restricted to specified circumstances, including where the person to whom the information relates consents to the on-disclosure (DEA, section 41).[219]

The debt and fraud powers

The DEA enables data to be shared by and with specified persons 'to reduce debt owed to the public sector' (DEA, section 48) or to 'take action in connection with fraud against a public authority' (DEA, section 56).

For both powers, information sharing proposals must be 'piloted' before they can be established as 'business as usual' information sharing activities. Information sharing proposals must be submitted to the Debt and Fraud Information Sharing Review Board, which will provide advice to the Minister for the Cabinet Office on whether the proposal should be implemented (DEA Code of Practice, paragraphs 94-105; UK Cabinet Office 2025).

Specific 'Fairness Principles' apply to data sharing using the debt power, under which public authorities must consider impacts that debt collection practices may have on vulnerable people and those experiencing hardship (DEA Code of Practice, paragraphs 107-109).

---

[218] The public register is available here: https://www.digital-economy-act-register.data.gov.uk/powers.
[219] There are specific provisions related to personal information disclosed by His Majesty's Revenue and Customs.

Information sharing agreements making use of the debt and fraud powers in the DEA are captured on the public register.

Research power

The 'research power' in the DEA allows public authorities to share data with researchers, for the purpose of research that is 'in the public interest', provided certain conditions are met (Research Code of Practice, paragraph 2.3).

Personal information must be de-identified by the public authority or by another party, and anyone involved in the de-identification process must be accredited. The DEA also requires that the research project and researchers (individuals and entities) are accredited (subsections 64(8) to (9)).[220] Accreditation is carried out by the UK Statistics Authority, according to conditions established by the UK Statistics Authority (see further at Appendix G). One of the conditions must be that the research is in the public interest.

There are seven specific principles that apply to sharing data for research (Research Code of Practice):

- confidentiality: the risks of compromising confidentiality of personal information must be minimised to the extent possible
- transparency: this includes complying with the UK GDPR's principle of lawfulness and transparency
- ethics and the law: the research must be both lawful and ethical
- public interest: the primary purpose of the research must be in the public interest, e.g. to provide an evidence base for public policy decision-making, service delivery, or reviewing existing research
- proportionality: the burdens and costs of the data sharing are proportionate to the anticipated benefits of the proposed research
- accreditation: all required accreditations must be in place for the duration of the project
- retention and onward disclosure: retention periods must be defined for identifiable data held by third party data processors, and any disclosure of the data to other researchers must meet approval and accreditation requirements.

The UK Statistics Authority maintains downloadable registers of accredited projects and accredited researchers, and a public register of 'accredited processing environments' or accredited processors.

The DEA also provides the UK Statistics Authority, by amending the *Statistics and Registration Service Act 2007* (UK) (Statistics Act), with a power to access administrative data for UKSA's purposes (section 79). The UK Statistics Authority has the power to access data upon request, or, in some cases, may require the disclosure (Statistics Act, section 45A-F).

[220] Any peer reviewers for the relevant research must also be accredited (Research Code of Practice, paragraph 24.1).

Public sector data sharing in New Zealand

Sharing of public sector data in New Zealand is enabled under specific legislation that allows a government agency to share information, or under the *Privacy Act 2020* (NZ) (Privacy Act NZ), which governs disclosure of personal information. The *Data and Statistics Act 2022* (NZ) (DSA) enables the sharing of government data for research purposes. There is no general data sharing legislation analogous to the DAT Act in the New Zealand context.

Sharing data for research

The DSA repealed and replaced the *Statistics Act 1975* (NZ) (1975 Act). The DSA was introduced to address key gaps in the 1975 Act, and modernise, improve and strengthen New Zealand's government data system and the collection and production of official statistics (Explanatory Note to the Data and Statistics Bill, p.1-5). The DSA and Statistics New Zealand (Stats NZ) play central roles in New Zealand's government data ecosystem (Stats NZ 2023), including to enable access to government data for research purposes (DSA, part 5).

The DSA enables New Zealand's Government Statistician to collect data from, and share data with, other public sector agencies (DSA, section 24). There is an obligation to comply with requests from the Government Statistician, except where the Statistician specifies that compliance is voluntary (DSA, section 29). The Government Statistician also has oversight and enforcement powers, and offences can be applied where a person fails to provide requested data (DSA, sections 76 to 89).

The DSA includes mandatory requirements for engaging, consulting and considering impacts on Māori people. These requirements give effect to the principles of te Tiriti o Waitangi/the Treaty of Waitangi (DSA, section 4).[221]

Under the DSA, the Government Statistician may provide access to data held by Stats NZ for research purposes. Access can be provided to an individual, public sector agency or organisation if certain conditions are met (Part 5). These include that

- the research is in the public interest
- the person or entity seeking access is an 'appropriate researcher'
    - specific matters are prescribed which the Statistician must take into account when determining whether a person or entity is an 'appropriate researcher'
- appropriate protective measures are in place
- the individual researcher has provided a 'certificate of confidentiality' to Stats NZ.

The Government Statistician may also authorise other public sector agencies, at their request, to provide access to the data they hold for research purposes (DSA, section 55). Data providers can impose conditions on the data they provide to Stats NZ for research purposes in certain circumstances (DSA, section 33).

[221] Recognising the Crown's obligations under to Tiriti o Waitangi/the Treaty of Waitangi was a reason for the repeal and replacement of the 1975 Act with the DSA (Data and Statistics Bill 2021 (81-1) (explanatory note)).

Sharing for service delivery

The Privacy Act NZ governs the sharing of personal information in New Zealand. The definition of personal information is the same as the definition under the Privacy Act. Approved Information Sharing Agreements (AISAs) are a key information sharing mechanism under the Privacy Act NZ.

AISAs allow personal information to be shared between or within agencies for service delivery, including for service delivery improvement and enforcement and compliance activities. This mechanism was introduced to overcome the hesitation to share data for service delivery attributed to the Privacy Act NZ's restrictions (Privacy Commissioner / Te Mana Mātāpono Matatapu (n.d.)).

Agencies are not required to use AISAs if the information sharing is allowed by another law or is permitted under the Information Privacy Principles (IPPs) (Privacy Commissioner / Te Mana Mātāpono Matatapu 2015). [222] AISAs must be made by the Governor-General by an Order in Council (Privacy Act NZ, sections 138 and 145).[223] This mechanism can be used to modify or grant an exemption from the application of most of the IPPs (Privacy Act NZ, paragraph 145(2)(a)). There are specific requirements specified in the Privacy Act NZ both for the Order in Council and for the AISA (Privacy Act NZ, sections 144, 146 and 147).

The Privacy Commissioner has the power to review the operation of an AISA, and provide a report and make recommendations about the AISA – including that the relevant Order in Council be revoked (Privacy Act NZ, sections 158 and 159).

Public sector data sharing in Singapore

Sharing for service delivery

Singapore's national digital identity and government data sharing frameworks are generally considered to be effective examples of public sector data use to support service delivery (Cooper et al 2022: xiii). Enablers of Singapore's framework are its:

- digital identity system (Singpass and Myinfo) which enables individuals to consent to their personal information being shared, and
- APEX, 'an application programming interface (API) gateway for government agencies to share and re-use data'.

A key legislative enabler of Singapore's framework is its *Public Sector (Governance) Act 2018* (Singapore). Under that Act, a Minister can direct (and authorise) a public sector agency to share information it controls with other public sector agencies (sections 4 and 6). There are also whole-of-government policies that support the management and sharing of data (Cooper et al 2022). Non-legislative enablers that support Singapore's framework are (Cooper et al 2022:42-43):

- identifying authoritative data (a 'single source of truth')
- a unified approach to data standards and formats to support interoperability.

---

[222] IPPs are very similar to the APPs under the Commonwealth Privacy Act. IPP 11 deals with disclosure of personal information.

[223] An Order in Council is secondary legislation subject to parliamentary scrutiny and disallowance, similar to legislative instruments in Australia: *Legislation Act 2019* (NZ). An Order in Council also requires policy approval by a Minister and a Cabinet Committee (Privacy Commissioner / Te Mana Mātāpono Matatapu 2015).

Sharing for research

The Department of Statistics Singapore facilitates access to public sector data for research purposes. This is enabled under the *Statistics Act 1973* (Singapore) (Singapore Statistics Act). Under the Singapore Statistics Act, the Department of Statistics and specified research and statistics units (see the Second Schedule) can collect and process data for statistical purposes (subsection 3(1)). 'Statistical purposes' include the preparation of anonymised microdata that relate to a set of specific subject matters (Singapore Statistics Act, section 2), including, for example, education, finance, health and social services, and housing (see the First Schedule).[224]

Singapore's Chief Statistician has a similar central, coordinative role to New Zealand's Government Statistician (Singapore Statistics Act, section 4). Under section 6 of the Singapore Statistics Act, the Chief Statistician can direct public agencies to share data with the Chief Statistician, for statistical purposes.[225] Section 7 enables the Chief Statistician and research and statistics units to disclose anonymised microdata to public agencies and specified universities. The Department of Statistics uses the Five Safes framework to manage the risks and ensure the safety and security of sharing microdata (Department of Statistics Singapore n.d.).

Comparisons with data platforms and infrastructure used overseas

Globally, countries have adopted different systems to support their data sharing frameworks and deliver improved service delivery or access for research or policy purposes. A comparison of several countries reveals variances and similarities in the platforms and infrastructure used to improve data sharing outcomes. This demonstrates the importance of having established systems to accompany data sharing frameworks.

Denmark's Datafordeler system is the national open data portal and data distribution platform for delivering information about individuals, businesses, properties, addresses and geography (Agency for Data Supply and Infrastructure 2024; Datafordeler n.d.; European Commission 2019; UNECE 2024). It supports data re-use and datasets can include unique identifiers to link information across different registers and sources. Sensitive datasets on Datafordeler may have access restricted to whitelisted organisations and require additional information in a data request.

Datafordeler's purpose broadly aligns with Australia's data.gov.au open data platform. However, Datafordeler's use of unique identifiers provides a higher level of infrastructure standards. For example, data.gov.au does not have any metadata requirements for a common address format, whereas Datafordeler datasets can include common address identifiers to link information together based on location.

Estonia and Finland use X-Road as an open-source data exchange layer solution developed by the Nordic Institute for Interoperability Solutions (NIIS), which is jointly founded by Estonia and Finland. It enables real time interoperability of data held across multiple public and private organisations to enable e-services to be delivered to its citizens. X-Road is aided by every resident having a secure digital ID to join services together. It was first implemented in

[224] Under the Singapore Statistics Act (section 2), 'anonymised microdata' means (relevantly) information pertaining to any person in a form that conceals or protects the identity of that person so that the person's identity cannot be 'readily discovered or ascertained from… information'.

[225] The Chief Statistician and statistics and research units also have powers to issue a requisition for information to any person for the purpose of obtaining data for statistical purposes (Singapore Statistics Act, section 5).

the Estonian government and then expanded to interoperate with Finland and enable cross-border services accessible to citizens of both countries. Available services include checking address registration and health insurance details, validating driver licenses and lodging taxes. This is essential for a mobile society, especially in cross-border regions like Finland and Estonia where citizens live and work on both side of the borders (NIIS n.d.).

There are some similarities in intent with individual Australian state government platforms and infrastructure (for example, the NSW government's Service NSW provides a platform for horizontal government and greater interoperability in government service functions (Dominello 2025)), but there is no comparable national platform for Australia that spans all Commonwealth, state and territory services.

X-Road's primary purpose is to enable the delivery of services. Broader use of Estonia's public sector data outside of government is enabled via an open data portal (ISA n.d.). This is the only platform that supports data access for purposes other than the delivery of services. No platforms exist for requesting or accessing more sensitive datasets for research purposes.

Canada uses a mix of federal and jurisdictional/provincial legislation to govern how it shares data. It operates an Open Government Portal for datasets published by federal government agencies (Government of Canada n.d. a). There is no national platform for sharing sensitive data but some organisations have established pathways to access sensitive datasets. For example, Statistics Canada operates the Virtual Data Lab and Virtual Research Data Centre secure access environments which permit approved users to access sensitive data from certain authorised locations (Government of Canada n.d. b).

Canadian provinces also operate their own frameworks and platforms. For example, in Ontario the ICES is an independent, non-profit organisation that holds coded and linkable public sector health datasets in a repository (ICES n.d.). Public and private sector researchers can apply to access datasets for research purposes through either the ICES Data & Analytic Virtual Environment or the Data Safe Haven depending on researcher's analytical requirements. Applications are reviewed to establish whether the use of data aligns with various requirements including alignment with ICES' mission, vision and values, evidence of scientific merit to the intended use, and ethics board considerations.

New Zealand operates data.gov.nz for open data and the Statistics NZ secure virtual environment (Data Lab) for controlled access by approved researchers to integrated datasets (Stats NZ 2022). The New Zealand government also uses the Data Exchange platform for securely transmitting data between Government and certain service providers (Social Investment Agency 2025; Social Investment Agency n.d.).

Part 6: Related initiatives and reviews

Productivity Commission 5-year Productivity Inquiry

In 2022 the then Treasurer requested the Productivity Commission undertake an inquiry into the Australia's productivity performance and provide recommendations on productivity-enhancing reform. This inquiry was the second of a regular series, undertaken at five-yearly intervals, to provide an overarching analysis of where Australia stands in terms of its productivity performance. The inquiry consisted of nine volumes of which Volume 4 is focussed on Australia's data and digital dividend (PC 2023b).

On Commonwealth Government data sharing, the Productivity Commission found that data sharing between public and private sectors has productivity benefits (PC 2023a, Finding 4.12):

> Collaboration between government and the private sector can lead to new opportunities for digitisation and data sharing, and derive more value from data provided to government agencies. Enabling government data sharing can benefit businesses and consumers by streamlining processes and improving service delivery, but only if data safety and security are maintained. The Data Availability and Transparency Act 2022 (Cth) does not currently allow government data sharing with the private sector, which could prevent some high-value data uses.

Based on this finding the Productivity Commission recommended private sector access to government data (PC 2023a: Recommendation 4.3):

> The Australian Government should enable government data to be securely shared with the private sector, so that not-for-profit organisations and businesses can undertake research and develop improved products and services for Australians.
>
> This could be enabled by extending the *Data Availability and Transparency Act 2022* (Cth). Extension could be gradual, starting with accredited private organisations using the data for policy and research purposes to achieve social objectives, before being opened for accredited businesses to use the data commercially. Appropriate safeguards should be employed to ensure security and privacy concerns are addressed, and the government could consider utilising advances in technology for individual privacy preservation.

Productivity Commission Investing in cheaper, cleaner energy and the net zero transformation Inquiry

In December 2024 the Treasurer requested the Productivity Commission undertake five inquiries to identify priority reforms under each of the five pillars of the Commonwealth Government's productivity growth agenda and make recommendations to assist governments implement productivity-enhancing reforms.

The interim report for Investing in cheaper, cleaner energy and the net zero transformation identified gaps in environmental and cultural heritage data delaying approval processes and increasing costs (PC 2025b). This was despite regulators holding significant data.
The Productivity Commission recommended the Australian Government provide the environmental data with appropriate protections for culturally and commercially sensitive information.

Productivity Commission Harnessing data and digital technology Inquiry

The Harnessing data and digital technology interim report of the five productivity pillars mentioned above considered the following reform areas:

- support innovation through an outcomes-based approach to privacy
- unlock the benefits of data through consumer access rights
- enhance reporting efficiency, transparency and accuracy through digital financial reporting
- enable the productivity potential of artificial intelligence (AI) (PC 2025a).

While this inquiry predominately focussed on improving private sector and consumer data flows, it also included themes and messages around the Australian Government's role in improving data sharing.

Government response to the Privacy Act Review Report

The Privacy Act Review was undertaken by the Commonwealth Attorney-General's Department. The Report concluded that an overhaul of Australia's privacy laws was required to ensure they remain fit-for-purpose in the digital age (Australian Government 2023).

Feedback following the release of the Report reiterated an expectation that the Australian Government strengthen privacy laws to ensure the collection, use and disclosure of people's personal information is reasonable, reflects community expectations and is adequately protected from unauthorised access and misuse.

National Data Sharing Work Program

The National Data Sharing Work Program implements the IGA by embedding it in data sharing practices (Department of Finance n.d). The Work Program also aims to; build trust and relationships, uplift capacity, and capability in the Australian data ecosystem; and develop robust, reusable data products. The Work Program seeks to uplift the national data sharing system by focusing national effort on specific time-limited priority policy areas to deliver collaborative, inter-jurisdictional projects, and driving broader data sharing system reforms.

The DDMM of 7 February 2025 agreed the fourth Work Program will include projects to:

- produce national guidance to enable best-practice family and domestic violence information sharing
- define 'trusted entities' for the purposes of national data sharing
- create foundational infrastructure for a national location spine (Department of Finance 2025c).

Trusted Entities

The DDMM Work Program Four: 'Defining 'trusted entities' for the purposes of national data sharing' (Trusted Entities), co-led by Services Australia and the Queensland Government, has produced a list of attributes of a 'trusted entity' for the purposes of building confidence in the national data sharing system. The trusted entity attributes were endorsed at the DDMM in August 2025, with the Program expected to be finalised at the next DDMM in late 2025.

Appendix D: Examples of legislative complexity and inflexibility in the DAT Act

This appendix outlines in greater detail examples of legislative complexity in the DAT Act. Many of the common drivers and measures of legislative complexity feature in the DAT Act's authorising framework.

Drivers of complexity are factors external to legislation itself which can impact on the degree of complexity in the legislation (ALRC 2021). These drivers include complexity of the field being regulated and the underlying policy, stakeholder demands, and legislative design preferences (ALRC 2021; OPC 2016; AGD 2014). Drivers of complexity relevant to the DAT Act include:

- the complexity of the data sharing ecosystem generally
    - For example, the substantial variation in the characteristics, requirements, and scale of data sharing projects, ranging from one-off, self-contained projects to large-scale enduring linkage initiatives; the rate of technological change affecting data sharing and privacy; interdependencies across a number of different legislative frameworks, depending on the type of data (i.e., the overlaps and distinctions between secrecy provisions and privacy law); the constitutional delineation of responsibility between Commonwealth, state and territory governments; and wide discrepancies and lack of transparency in processes and decision-making across different data custodians.
- the range of stakeholders and interests which the DAT Act aims to recognise and account for
    - While the Data Availability and Transparency Bill was already comprehensive in this regard, this driver was compounded by amendments made after its introduction in Parliament.[226] The provisions added during this amendment process are some of the more complex in the DAT Act (discussed further below).
- the preference for including comprehensive, detailed rules in the primary law
    - Many of the instrument-making powers in the original Bill were removed and the relevant subject matter prescribed in the primary legislation. An example of this is the removal of the power to prescribe the authorised officer for particular types of entity, which has materially affected the ability of some Commonwealth bodies to effectively participate in the Scheme.[227] Another example is the ability to transfer accreditation to accommodate Machinery of Government changes.[228]

The DAT Act also has many of the (internal) measures of complexity identified by the ALRC (2021) and others, which negatively impact participants' ability to understand the legislation (see e.g. AGD 2014.; OPC 2016; Burton Crawford et al. 2022). This report highlights only some of the most significant examples of complexity in the DAT Act.

---

[226] OPC (2016) also identifies changes made to Bills in Parliament or late changes to drafts of Bills can contribute to legislative complexity.
[227] Submission 31, Jobs and Skills Australia.
[228] Submission 1, ACT Government.

Length

The DAT Act is not necessarily a long piece of legislation in terms of word count relative to other Acts (Burton Crawford et al. 2022). However, it is long compared to other legislative and non-legislative frameworks that data custodians rely on to share public sector data.

For example, South Australia's *Public Sector (Data Sharing) Act 2016* is 4889 words in length, and the Census and Statistics (Information Release and Access) Determination 2018 (Cth) contains 2362 words.[229] The DAT Act, by contrast, has a word count of 34608 – approximately 7 times the length of South Australia's legislation, and 14 times the length of the ABS's data sharing framework.[230] While a one-to-one comparison between the length of the DAT Act and these other frameworks is not necessarily determinative, it does indicate that the task of understanding the DAT Act will be more onerous for participants compared to other frameworks.

The length of the DAT Act's key provisions relevant to its authorising framework is another metric of the DAT Act's complexity. The parts of the DAT Act relevant to the authorisation of sharing, collection and use of data are the longest and most dense in the DAT Act.
For example:

- The relevant concepts and definitions for understanding data sharing under the DAT Act are set out in Chapter 1, including 7 pages of definitions and an additional 4 pages setting out key concepts relevant to data sharing ('access to data', 'entity definitions' and the 'data sharing project').
- The data sharing authorisation requirements are set out in Chapter 2, which comprises 8 distinct parts.
- There are additional requirements and considerations for data sharing set out in the two existing data codes.

There is a significant volume of detail for participants to digest and understand in order to understand what is required for data sharing activities to be authorised. The relevant material would be even longer if the provisions about 'authorised officers', the extension of the authorisations to 'designated individuals', and relevant data breach responsibilities were included in this count.

Prescription: data sharing agreements

The issue of the length or volume is exacerbated by excessive prescription. Greater prescription in legislation is often intended to ensure the legislation is comprehensive in covering all possible activities and considerations. While often intended to improve clarity, excessive prescription or specificity can have the opposite effect (ALRC 2021).

An example commonly raised by stakeholders,[231] and reported in the ONDC's Working Group (ONDC 2024), is the significant number of requirements that must be met by a data

[229] For the *Public Sector (Data Sharing) Act 2016* (SA), this includes the words starting from the long title but does not include the endnotes. For the Census and Statistics (Information Release and Access) Determination 2018, this includes all the words starting from the 'Contents' section.
[230] This includes all the words starting from the long title of the Act but does not include the endnotes or subordinate legislation.
[231] Numerous Commonwealth entities mentioned the degree of prescription in the DAT Act as an issue (see, e.g. Submission 9, ABS; Submission 12, AIHW; Submission 21, Department of Social Services), as did a number of other entities, including Submission 1, ACT Government and Submission13, Australian Research Data Commons.

sharing agreement. Data sharing agreements – and their registration by the National Data Commissioner – are the key authorising mechanism in the DAT Act (paragraphs 13(c), 13A(a), 13B(a) and section 13C).

There is a total of just under 70 requirements for data sharing agreements set out in the DAT Act and the two data codes. Many of these are conditional, and so only apply when a data sharing project has certain features (for example, when the project involves personal information).

Data sharing agreement requirements are also spread across a variety of different parts of the legislation: most are contained in section 19 (which has a total of 17 subsections), but others are contained in Parts 2.4 and 2.7 in Chapter 2, and in both data codes. Some data sharing agreement requirements duplicate other aspects of the authorisation provisions. For example, the data sharing principles and mandatory considerations are set out in the legislation (section 16 of the DAT Act and sections 6 to 15 of the DAT Code), but parties are also required to set out the actions that will be undertaken to give effect to the data sharing principles (paragraph 19(7)(b)).[232]

Participants must also understand concepts and obligations in other parts of the Act to understand whether a particular requirement applies. An example of this is the requirement to specify whether subsections 37(2) and (3) apply to the sharing, which set out responsibilities for notifiable data breaches under the Privacy Act. Specifying whether the subsections apply or do not apply will change which of the parties is responsible for notifications. A separate provision (subsection 37(4)) is the actual provision that allows the responsibility to be shifted from a data custodian to an accredited entity. Whether responsibility can be given to a party other than the data custodian depends on whether the accredited entity is an 'APP entity', meaning that participants must also understand the relevant responsibilities under the Privacy Act to meet their obligations under the agreement.

Part of the reason for the significant volume of data sharing agreement requirements is the number of core obligations that are given effect through agreements, rather than through the DAT Act in its own right. For example, the authorisation provisions are not direct in requiring the sharing, collection or use of data to only be for one of the data sharing purposes, or conversely not be for a precluded purpose. Instead, the DAT Act requires:

- the data sharing purpose/s of the project to be specified in a data sharing agreement, and
- a term be specified in the data sharing agreement that 'prohibits' the accredited user from collecting or using the output of the project for any purpose that is not specified or for any precluded purpose (except in relation to a use of specified allowed output).

The restriction of the purposes for which data can be shared and used under the DAT Act is a core safeguard of the authorising framework. As OPC (2016) notes, obscuring important concepts in procedural detail can lead to 'overly complex' provisions.[233]

The ONDC has taken several steps to reduce the burden imposed on participants in navigating the degree of prescription and complexity of data sharing agreements, including:

[232] Sometimes, no distinct action may be required in order to satisfy the principle. This could either be because there are no particular risks to mitigate, or because many of the DAT Act's requirements directly address the data sharing principles: for example, the use of an ADSP to provide secure access services may address the setting principle, and the accreditation process may, to a significant extent, address the people principle for a particular project.

[233] Also cited in the ALRC's Background Paper (2021).

- publishing guidance on data sharing agreement requirements and registration processes
- integrating and automating the generation of template data sharing agreements in Dataplace based on the specification of project requirements
- developing a 'short form' data sharing agreement template
- delivering webinars on establishing data sharing agreements, and
- providing targeted resources to assist participants to establish agreements for high-priority data sharing projects.

The fact that these efforts have not dispelled the view that data sharing agreements are too burdensome is a significant indicator of the complexity resulting from the prescriptiveness of the DAT Act. This further indicates that the complexity is unnecessary, and the degree of prescription is excessive.

Data sharing agreements are one of a significant number of requirements for the sharing, collection and use of data to be authorised under the DAT Act. There are also more requirements for data custodians (or 'sharers' of data) than for other types of scheme entities (section 13 spans almost two and a half pages, compared to half a page each for users and intermediaries). It is understandable, then, when faced with this degree of complexity and burden – and the related risk – that data custodians would choose to use other available frameworks to share data.

Other structural legislative features

Other significant structural legislative features contributing to the DAT Act's complexity include the number of conditional statements and cross references.

Conditional statements

Many of the conditional statements in the DAT Act relate to whether a data sharing project will involve personal information (see for example paragraph 13(1)(g), and subsections 16A(2) and (3)). However, the volume and structure of the privacy protections in particular may contribute to the view that the DAT Act takes an overly burdensome approach to protecting personal information.

For example, section 16B sets out privacy protections for certain data sharing projects. Subsection 16B(3) sets out protections for projects which are for the purpose of informing government policy and programs or research and development. Personal information can be shared for these purposes in two alternative circumstances (paragraph 16B(3)(a) or (b)). The second alternative deals with sharing without individuals' consent, and has four requirements. One of those requirements (subparagraph (iv)) can be satisfied in one of six ways if the purpose is informing government policy and programs (paragraphs 4(a) to (f)), but only in four ways (paragraph (a) to (d)) if the purpose is research and development (subsection 16B(5)).

If the first option for satisfying the requirement in subparagraph 16B(3)(b)(iv) is chosen (that it is unreasonable or impracticable to seek consent), there are an additional two requirements that apply, and which must be included in the data sharing agreement for that project (subsection 16B(7)). This is set out in a conditional statement in which the first word

'If' and the applicable requirements are separated by 48 words. There are also additional considerations to which data custodians must have regard when meeting this requirement, which are set out in section 21 of the DAT Code.

There is also an additional requirement, which is set out in subsection 16B(8), which applies if a project relies on paragraph 16B(3)(b) to share personal information without consent, and which must be included in a data sharing agreement. There are 30 words between the word 'If' at the beginning of the subsection and the operative requirement. There are additional mandatory considerations set out section 23 of the DAT Code which will apply if personal information is being shared without consent, and further applicable considerations in section 22 of the DAT Code if subsection 16B(3) applies to the project at all.

The purpose of outlining how these provisions interact is to demonstrate the difficulties of navigating the Act. This is more likely to dissuade participants from using the DAT Act than to use it to ensure personal information is shared with the appropriate protections. Section16B is a provision that was added by amendments made to the Bill before its passage through Parliament (as indicated by the inconsistent alphanumeric numbering of the provision – which is also an indicator of complexity (ALRC 2021; OPC 2016)).

Interdependency and cross-referencing

The significant degree of cross-referencing in the DAT Act and the interdependency between the DAT Act and other legislation also contribute significantly to complexity.

Interdependency with other legislation undermines the overarching objective of the DAT Act to reduce the number of different legislative frameworks that need to be navigated to share public sector data, as envisioned by the PC Inquiry.

One key example of this is the difficulty participants have had in understanding the relationship between the DAT Act and the Privacy Act. This issue was raised in the ONDC's Working Group (cited as a concern in Submissions 13 and 46). It was also mentioned explicitly by the Department of Health, Disability and Ageing in their submission to the Review.

The DAT Act's authorisation to share data does not 'override' the Privacy Act (subsection 17(5)). However, sharing that is authorised under the DAT Act is an 'authorised secondary purpose disclosure' under APP 6.[234] So, while the DAT Act can authorise sharing consistently with APP 6, it does not displace the obligations entities may have under the Privacy Act (for example, the requirement to undertake a Privacy Impact Assessment). Further, it may be that activity that would be permitted under the Privacy Act is nevertheless not permitted by (and may be subject to penalties under) the DAT Act. Therefore, not only is the DAT Act interdependent with the Privacy Act, it can be unclear to participants how the two regimes interact or how to navigate the relevant interdependency.

The DAT Act also requires data custodians to consider and navigate the secrecy provisions that would apply to the data sharing 'but for' the statutory override in section 23 of the DAT Act. There is a requirement to specify any such laws in the data sharing agreement (subsection 19(5)), which may be particularly difficult when the data being shared is an integrated data set comprising data drawn from multiple different Commonwealth sources. It also poses a barrier to minimising the burden of repurposing existing data for sharing

[234] Submission 6, Attorney-General's Department, pg 5.

under the DAT Act. Further, where output is proposed to 'exit' the DAT Act's authorising environment, the DAT Act requires that the provision of access to the data, or the publication of the data, must not 'contravene any other law of the Commonwealth, or a law of a State or Territory (disregarding section 23 of [the DAT Act])' (paragraphs 20C(1)(a); 20F(3)(a)).

Though the ONDC has provided guidance that this requirement would be met if the output was considered '"safe" for exit from the Scheme' (ONDC 2025), it is understandable that this requirement reinforces the impression that the DAT Act is overly complex (and restrictive; this is expanded upon in the next section on inflexibility).

This difficulty could be mitigated by the fact that the output created under a DAT Act project can be shared in subsequent DAT Act projects. This allows the data to remain subject to the DAT Act's protections (as pointed out in PHRN's second submission). However, this data can only subsequently be shared by a Commonwealth body (which may be a concern for accredited users or original data providers that are state or territory bodies). Further, doing so requires navigating the provision which permits the appointment of a data custodian of the output of a project and its corresponding data sharing agreement requirements (subsection 20F(2)). This is another of the DAT Act's more complex provisions due to intricate cross-referencing.

Under subsection 20F(2), an accredited user can be appointed a data custodian of project output if three requirements are met, the last of which (paragraph (c)) has two alternatives. One alternative (subparagraph (i)) cross references two provisions (section 20C and 20D), either of which can be satisfied to meet the sub-requirement). Section 20D is the provision that allows an accredited user to share data as the data custodian in a subsequent DAT Act project. It has two requirements which must be satisfied, one of which is a cross reference back to subsection 20F(2). The alternative option, section 20C, has three requirements – involving the 'exit' of output, referenced above. If neither section 20C or 20D is relied upon, then the other option to satisfy paragraph 20F(2)(c) (i.e., subparagraph (ii)) is to satisfy subsection 20F(3), which has three requirements. Subsection 20F(3) largely mirrors section 20C.

There are also a number of defined terms that are relevant to this subsection, including 'data custodian', 'Commonwealth body', 'output', and 'public sector data'. The ALRC (2021:18) notes that '[d]efinitions are a form of cross-referencing, because each use of a defined term requires a reader to have regard to the definition of that term'. As an example of the additional complexity involved in this particular provision, the term 'output' is defined in paragraph 11A(1)(b) as: (i) the copy of the data collected by the user,[235] and (ii) the data that is the result or product of the user's use of the shared data. However, one of the conditions in subsection 20F(2) is that the relevant output is 'public sector data and *not* a copy of the shared data collected by the user' (emphasis added). So in addition to the complexity caused by cross-referencing, complexity also arises as a result of overly intricate and unclear terms.

The combination of structural complexity and excessive prescription in the DAT Act is a clear and significant barrier to the degree of difficulty data custodians face when considering whether to use the DAT Act. These issues are compounded by the fact that, as will be

[235] There is no explanation in the legislation or the Revised EM as to what the purpose of this part of the definition is. It is only referred to in the legislation in s 20F – presumably to avoid the possibility of custodianship of the original data being transferred to another Commonwealth body.

explored in the next section, the complexity and degree of prescription has resulted in a common and legitimate view that the DAT Act is an inflexible framework.

Inflexibility

In addition to creating inhibitive complexity, the degree of prescription and specificity in the DAT Act has limited the flexibility of its authorising framework. It can therefore be difficult for participants to work out how or whether a particular data sharing activity can be authorised by, and undertaken consistently with, the DAT Act. This has contributed to the view that the DAT Act's requirements are too burdensome or that the bar of assurance which participants must clear is disproportionately high in cases other than those which are the most high-risk.

Limiting the activities that can be undertaken

Numerous stakeholders have highlighted the problem with the DAT Act's limiting conception of the data sharing 'project'.[236] Specifically, there is a perception that the DAT Act can only authorise simple, defined instances of a data custodian sharing, on a one-off basis, very specific data with a user for very restricted purposes, and that each instance must be authorised separately. This is a common view even though the DAT Act seems able to accommodate – to some extent and on a close reading – a programmatic approach to data sharing, and some more complex data flows. For example, the DAT Act allows for:

- multiple entities to play the same role in a data sharing project (i.e., there may be more than one sharer or accredited user)[237]
- multiple projects to be considered as a single project, if the parties and purposes are the same (subsection 11A(5))[238]
- data to be created as the output of a project for sharing under a subsequent project, even if the specific purpose of the next project(s) are not known (subsections 11A(6), 15(5) and 15(6))
- different output to be created for distinct uses by the accredited user[239]
- data sharing agreements to be ongoing rather than being only for a defined period (subsection 19(14))
- parties other than the data custodian, ADSP or accredited user to be party to data sharing agreements (Revised EM, paragraph 189)
- a program of work to be established, rather than a highly confined 'project' (subsection 16(1)).[240]

However, the DAT Act does limit the data sharing activities that can be undertaken. This includes the inability to authorise sharing data with an ADSP to prepare data for future use by (as yet undetermined) accredited users. It is also unclear on the face of the legislation

---

[236] E.g. Submission 9 (ABS); Submission 38 (National Data Commissioner).

[237] Note 2 below s 11A(1) expressly addresses multiple sharers. The ability for a project to involve multiple accredited users is not expressly stated in the legislation, but is implied in the Revised EM (paragraphs 63 and 182), and stated in the ONDC's guidance (see e.g. https://www.datacommissioner.gov.au/data-sharing-agreements).

[238] Though presumably intended to afford some flexibility, it is not clear what purpose this permission serves, or what benefit it might provide to participants, and the Revised EM does not elaborate on the text of the provision.

[239] E.g. the user can be permitted to publish 'specified' output (s 20C), as distinct from the 'final' output (s 16(9) and 19(3)(b)).

[240] The project principle in the DAT Act expressly requires consideration of whether the 'project is an appropriate project or *program* of work' (s 16(1)) (emphasis added).

how or whether the DAT Act can authorise 'multi-way' or 'two-way' data sharing. This is particularly significant with respect to state and/or territory data.

This is in large part an issue of inflexibility brought on by over-specification. The DAT Act defines a data sharing project in a largely linear way: a data custodian shares data with an ADSP who then shares the data with an accredited user on the data custodian's behalf for the user to create output to be used for a defined purpose. There may be work undertaken on data prior to sharing occurring (which is part of a project, but not specifically authorised under the DAT Act) (subsection 11A(2)), and the data created during the project may be shared back to the data custodian (but only for the data custodian to check the ADSP-enhanced data or output) (subsection 11A(4) and section 13C). But the DAT Act, in prescribing these specific data flows, appears to exclude the ability for:

- data to flow back and forth between participants during a project
- different subsets of the created data to flow in different ways to different parties, or
- for data that is not public sector data to be used or shared in a DAT Act project.

This is not to say that the DAT Act does not or cannot accommodate these data flows, but understanding how such flows fit into the specific formulation envisaged by the DAT Act requires both participants and the regulator to invest significant resources to determine whether and how such activities can be carried out consistently with the Act's requirements.

The highly prescribed, technical and linear way the DAT Act describes and authorises the data sharing limits its flexibility and, consequently, the scope and types of activity participants can undertake. Even if those activities can in fact be undertaken, the resources required to navigate the legal pathway to assure custodians that the activities would be authorised have proven to be prohibitive. In these circumstances, it may ultimately be easier and less costly for participants in a project to navigate multiple legislative frameworks to authorise the project than to use the DAT Act alone.[241] While this outcome is understandable from participants' – particularly data custodians' – perspective, this also results in a missed opportunity to standardise data sharing across the Commonwealth and, consequently, achieve broader system efficiency.

Disproportionate protections and burden

As the DAT Act appears to authorise only (or at least most clearly) simple data sharing projects, the protections in the DAT Act may appear to be disproportionate and unreasonably burdensome. This may be largely because of the degree of prescription and complexity in the legislation, but there are instances in the DAT Act where the protections appear to be excessive.

For example, where the purpose of a project is service delivery, personal information can be shared without an individual's consent if the relevant service is being delivered to that individual – but only where the subset of service being delivered is either providing information, or providing services other than those relating to a payment, entitlement or benefit (paragraph 16B(1)(i)). It is not clear why it would not be permissible to share personal information without consent if the purpose of doing so was to determine eligibility for, or to

[241] This is an issue in particular faced in establishing the NDDA. Further, in the case of state and territory data being shared into the Commonwealth's custody, the DAT Act does not eliminate the necessity of navigating relevant state and territory legislation (see e.g. Submission 1, ACT Government and Submission 12, AIHW).

pay, a payment, entitlement or a benefit to the person whose personal information was being shared (paragraphs 15(1A)(c) and (d)).

As another example, the DAT Act prohibits any project which involves the sharing of personal data from allowing storage of or access to ADSP-enhanced data or output outside Australia. This is excessive in a number of ways. First, it is possible to generate output from personal information which is comprehensively de-identified – for example, if it is highly aggregated data.[242] This also seems to conflict with the ability to create ADSP-enhanced data using a de-identification data service – which, presumably, would result in de-identified data which the user could access (see subsection 16C(3)). Second, this prohibition seems to be incongruous with the ability to publish the output of a project (if 'safe' to do so). Publishing output on the internet, for example as part of a report, would be accessible from outside Australia. Publication – i.e. 'release' – is a 'provision of access' for the purposes of the DAT Act (paragraph 10(1)(b)). And finally, the prohibition is inconsistent with the approach taken to overseas disclosure under APP 8 (both in its current form and prior to the recent amendments to the Privacy Act). A blanket, absolute prohibition on accessing *any* data from overseas where a project may only involve personal information before any treatments have been applied therefore seems unreasonably restrictive.[243]

It is important to note that this is not to say there should be no protections and safeguards for sharing personal information. Rather, the above is intended to illustrate that views about the DAT Act being unduly burdensome are justified given the lack of clarity in the legislation (which has numerous dimensions), particularly compared to other available frameworks. Also relevant is the fact that entities wanting to use the DAT Act's authorisation to access data first need to obtain accreditation under the Act, which itself is potentially very costly. To put this colloquially, this undermines the 'bang for buck' for entities to get accredited.

[242] Noting that there is a view that it is not possible to fully de-identify unit record data (Adams et al 2025).

[243] The Attorney-General's Department has similarly suggested in their submission that the blanket prohibition on sharing biometric data should be revisited, subject to any changes made in that respect to the Privacy Act.

Appendix E: Non-data accreditation frameworks in Australia

In Australia, all levels of government play a critical role in the development, implementation, and coordination of accreditation frameworks to support critical sectors including health services (hospital and health care facilities), health professions, disability services, aged care, construction, education, environmental management, food safety, and transport.[244] Accreditation frameworks among these sectors share some common goals and characteristics despite differing operating contexts. All frameworks aim to protect consumers and the public by establishing baseline sector quality and safety standards, and maintain standards and an external assessment regime to support compliance and continuous improvement. To support the Reviews findings and recommendations, it is important to present and analyse the function of other government-administered accreditation frameworks in Australia with respect to standard management, framework design (including assessment processes), and accreditation incentives.

Health services

The Australian Commission on Safety and Quality in Health Care, which administers the *National Health Reform Act 2011* (Cth), provides quality assurance of health services (hospitals and other healthcare facilities) delivered in Australia through the administration of the National Safety and Quality Health Service (NSQHS) Standards under the Australian Health Service Safety and Quality Accreditation Scheme (Greenfield et al 2015). It is a requirement for all public and most private hospitals to be accredited against the NSQHS standards, and since 2013, it is for all intents and purposes, mandatory given accreditation is required for hospitals to receive both Medicare and other financial support from government. To obtain and maintain accreditation, hospitals must demonstrate compliance against criteria relevant to patient safety and care quality including clinical governance, infection control, medication management, comprehensive care, blood management, and management of acute deterioration. Accreditation assessments are completed on three-year cycles which includes a review of policies, inspection of hospital practices, and staff/patient interviews. Given accreditation against the NSQHS standards is required for government funding, this strategy produces strong economic incentives for hospitals to obtain and maintain accreditation.

Health professions

The National Registration and Accreditation Scheme (NRAS), established by the Council of Australian Governments in 2010, is jointly administered by the Australian Health Practitioner Regulation Agency (AHPRA) and the national boards for identified health professions. The separation of the AHPRA (providing government oversight) from national education standard-setting boards supports the dual function of an accreditation scheme which both maintains professional standards and is accountable to the public. The NRAS accredits 16 professions, including doctors, nurses, pharmacists, physiotherapists, and psychologists. The NRAS accreditation framework assesses and accredits university and clinical programs based on a set of criteria including faculty qualifications, student support, facilities, curriculum content and examination processes; ensuring graduates meet minimum levels of competency before entering their profession. Graduates from accredited programs can then

[244] For brevity, this section discusses a sample of government-administered accreditation frameworks relevant to the provision of critical services (health services, health professions, disability, and aged care).

apply for professional registration with AHPRA, making accreditation a barrier to entry into identified health professions. Through collaboration with state-based professional boards, NRAS has developed as a national accreditation system which integrates education, accreditation, and registration of health practice across Australia (Kruk 2023).

Disability services

The NDIS Quality and Safeguards Commission is the national regulatory body (established in 2018) which provides oversight of service quality to recipients of NDIS participants. Providers are required to meet NDIS Practice Standards and undergo independent audits to be registered and deliver services under the NDIS. The NDIS Practice Standards include person-centred support, rights and empowerment of participants, health and well-being, provider governance and operational management, and provision of a supportive environment (NDIS Quality and Safeguards Commission 2025a). NDIS registration requires renewal every three years which are bolstered by mid-term independent audits. Importantly, without NDIS registration, a disability services provider is unable to present as holding a NDIS registration, significantly limiting its ability to compete in the disability services market and preventing it from claiming payments under the NDIS (NDIS Quality and Safeguards Commission 2025b). Similar to the NRAS, the NDIS Quality and Safeguards Commission unified previously state-based standards and certification systems to support the provision of disability services.

Aged care

All residential aged care facilities in Australia which receive government subsidies require accreditation through the Aged Care Quality and Safety Commission (established by the *Aged Care Quality and Safety Commission Act 2018* (Cth)). Accreditation assessments of applicants are made against the Aged Care Quality Standards which consider consumer dignity and choice, ongoing assessment and planning, personal and clinical care, services and support for daily living, the physical service environment, feedback and complaints, human resources, and organisational governance (Aged Care Quality and Safety Commission 2025).

Appendix F: Digital identity accreditation frameworks

Digital accreditation frameworks have been established to address the growing need for effective management and regulation of transactions and interactions in the digital economy. These activities frequently require individuals to verify their identities digitally. Numerous countries have established digital identity legislation and corresponding frameworks to ensure that providers of digital identity services adhere to specific standards for data security, privacy, and service quality. The following discusses digital identity accreditation frameworks in the United Kingdom, European Union, Canada and Australia.

United Kingdom

The United Kingdom is in the process of transitioning from the non-statutory 'Digital Identity & Attributes Trust Framework', established in 2021, to a legislated digital identity regime under the *Data (Use and Access) Act 2025* (UK). The legislation:

- formalises the trust framework through regulations
- introduces an official 'trust mark' which signifies 'trusted providers' which have been certified (accredited) and registered with the government to provide digital identity services
- includes a public register of certified 'trusted providers'
- provides oversight powers to the government to suspend or remove providers from the register if they fall out of compliance, and to set conditions or requirements, and
- enables an information sharing gateway which allows 'trusted providers' to verify records against government held data (CMS Law, 2025).

With respect to accreditation, the trust framework defines standards across the identity process, including confidence level requirements for the verification of identities, secure user authentication mechanisms, including, for example, the use of multi-factor authentication, attribute validation including qualification verification, and privacy and consent management. Independent audits are performed to certify applicant providers against the trust standards; with the independent auditors themselves accredited for competency and impartiality as Conforming Assessment Bodies through the United Kingdom Accreditation Service (Department for Science, Innovation and Technology 2025).[245]

European Union

The accreditation of digital identity services in the European Union is implemented through the Electronic Identification, Authentication and Trust Services (eIDAS) Regulation (No. 910/2014), and is therefore binding for all European Union member states (Rauh, 2025). The eIDAS requires the mutual recognition of certified identification services between member states. A supervisory authority is instituted in each member state, and which regulates Qualified Trust Service Providers (QTSPs) under their respective national identity scheme.[246] For the purposes of maintaining consistency and interoperability among member states, the

[245] It is important to note that, as at 26 June 2025, the certification process is operating as an unaccredited pilot, with the expectation that it will be operational from mid-2025 (Department for Science, Innovation and Technology 2025).

[246] QTSPs can be accredited to provide one or more of the following 'electronic signatures, electronic seals, time stamping, registered electronic delivery and website authentication' (European Commission 2014).

European Commission establishes the technical, procedural, and operational standards for the provision of digital identity services, with national supervisory authorities responsible for accrediting and auditing QTSPs against these standards (European Commission 2025).

Canada

Digital identity services in Canada are administered by the Digital ID and Authentication Council of Canada (DIACC) who maintain the Pan-Canadian Trust Framework (PCTF). The PCTF establishes standard criteria for digital identity services in Canada, and is recognised at both provincial and federal levels (Digital ID & Authentication Council of Canada 2025a).[247] The PCTF is not mandated by law, as is the case with the United Kingdom and European Union, but instead, acts as reference model for the implementation and delivery of digital identity services in Canada. DIACC maintains a certification program where digital identity solutions are independently audited for compliance against the PCTF (Digital ID & Authentication Council of Canada 2025b).

Australia

Australia maintains a government-led framework for accrediting digital identity services, which has evolved from a pilot framework (the Trusted Digital Identity Framework (TDIF)) into the legislated Australian Government Digital ID System (AGDIS) established under the *Digital ID Act 2024* (Cth). Accreditation is managed by the Australian Competition and Consumer Commission as the Digital ID regulator, with assessment involving the review of written applications made against the standards for accreditation. Accreditation is mandatory for providers operating within the Australian Government Digital ID System and requires providers to demonstrate that their services meet government standards of trust, privacy, and security (Department of Finance 2024b).

[247] The Digital ID and Authentication Council of Canada is a non-profit coalition composed of leaders from both the public and private sectors. Its mission is to develop a Canadian framework for digital identification and authentication that enables secure, inclusive, and privacy-enhancing participation in the digital economy (Decentralized ID 2025).

Appendix G: Public sector data sharing accreditation frameworks

Public sector data sharing accreditation schemes assess organisations on their ability to meet standards for sharing, using, or providing services related to public sector data. The following discusses data sharing accreditation in the United Kingdom, European Union, and Canada.

United Kingdom

Chapter 5 of Part 5 of the DEA establishes a legal gateway to share data held by public authorities in the United Kingdom for research purposes. The accreditation framework established under the Act is administered by the UK Statistics Authority. To support data sharing, the Act establishes an accreditation framework administered by the United Kingdom Statistics Authority. Researchers, research projects, and processing facilities must be accredited before they can access de-identified public sector data for research, the standards of which are published in the Research Code of Practice and Accreditation Criteria (UK Statistics Authority 2020). Data intermediaries must be accredited as 'processors', and projects must be approved by an independent panel for public benefit and disclosure risk. Similarly, accredited researchers (peer reviewers) are required to undertake training on data handling, have their identity published on a public register of accredited researchers, and sign a declaration which confirms they agree to abide by the conditions of accreditation imposed on them. Data is then accessed through secure portals like the Office for National Statistics (ONS) Secure Research Service, which acts as an accredited safe setting (UK Statistics Authority 2020).

European Union

Regulation (EU) 2022/868 (Data Governance Act) facilitates general data sharing within the European Union. The Data Governance Act mandates the registration of organisations providing 'data intermediation services' with the relevant member state national authority, and which are required to maintain standards of neutrality, transparency, and data security.[248] Although accreditation is not mandatory, data intermediation service providers may seek formal compliance confirmation from their respective national authority. If the national authority considers the provider compliant, this permits the provider to publicly display an EU-wide 'trust mark' confirming its compliance with the standards of the European Union (Bange et al (2023). In lieu of an accreditation framework enabling the *use* of public sector data, the Data Governance Act allows public sector data to be shared with third parties provided relevant safeguards or treatments are applied in certain circumstances including, for example the requirement for data to be de-identified, or for data flows to be managed using data intermediation services.

[248] Data intermediation services are identified in Article 10 of the Data Governance Act and include acting as a channel or exchange between data custodians and users which facilities the exchange of data, and the creation and administration of data platforms.

Canada

To support the use of public sector data for research in Canada, Statistics Canada authorise access under the *Statistics Act 1985* (CA). Specifically, Statistics Canada maintain Research Data Centres (RDCs) which allow approved researchers to access public sector-held microdata. To authorise access, researchers must apply to be considered as 'deemed employees' of Statistics Canada for the purposes of the *Statistics Act 1985* (CA).
This requires applicant researchers to undergo a security clearance process and sign confidentiality agreements (Statistics Canada 2019). This is effectively an accreditation of individuals and projects, whereby only vetted researchers working on approved, public-interest projects are permitted to access and use public sector-held microdata within secure access environments managed by Statistics Canada.

Appendix references

AGD (Attorney-General's Department) (2014) *Clearer Commonwealth Laws: causes of complex legislation and strategies to address these*, Attorney-General's Department, Australian Government, accessed 22 September 2025.

Agency for Data Supply and Infrastructure (2024) *Linking data across domains and sources – Danish Basic Data Programme & Data, Distributor Platform*, Conference of European Statisticians, 72nd plenary session, accessed 29 September 2025.

Aged Care Quality and Safety Commission (2025) *Aged Care Quality Standards*, Aged Care Quality and Safety Commission website, accessed 25 August 2025.

ALRC (Australian Law Reform Commission) (2021) *Background Paper FSL2 Legislative Framework for Corporations and Financial Services Regulation: Complexity and Legislative Design*, Australian Law Reform Commission, Australian Government, accessed 22 September 2025.

ALRC (2022) *Measuring Legislative Complexity*, ALRC website, accessed 22 September 2025.

ALRC (2023) *Confronting Complexity: Reforming Corporations and Financial Services Legislation*, ALRC Report 141, Australian Government, accessed 22 September 2025.

ABS (Australian Bureau of Statistics) (2021) *Five Safes framework*, ABS website, accessed 30 September 2025.

ABS (2023) *Annual Report 2022-23, Case Study 4 – Criminal Justice Data Asset*, Australian Government Transparency Portal website, accessed 30 September 2025.

ABS (n.d. a) *PLIDA data and legislation*, ABS website, accessed 30 September 2025.

ABS (n.d. b) *Business Longitudinal Analysis Data Environment (BLADE),* ABS website, accessed 30 September 2025.

ABS (n.d. c) *DataLab,* ABS website, accessed 30 September 2025.

ABS (n.d. d) *BLADE case studies*, ABS website, accessed 30 September 2025.

ADHA (Australian Digital Health Agency) (n.d.) *Digital Health Standards Catalogue*, ADHA website, accessed 30 September 2025.

AIHW (Australian Institute of Health and Welfare) (2022) *AIHW Data Governance Framework 2022 (Public Edition)*, AIHW website, accessed 30 September 2025.

AIHW (2024) *Governance protocols for National Health Data Hub (NHDH),* AIHW website, accessed 30 September 2025.

AIHW (2025) *National Health Data Hub*, AIHW website, accessed 30 September 2025.

AIHW (n.d.) *Data available from the Department of Social Services*, AIHW website, accessed 30 September 2025.

ATO (Australian Taxation Office) (n.d.) *[beta] The ATO Longitudinal Information Files,* Alife website, accessed 30 September 2025.

Bange V, Glass P, Nwosu C, and Uzoukwu A (2023) *The Data Governance Act: Common Logos and Other Requirements Introduced for Data Sharing in the EU*, Baker McKenzie website, accessed 25 August 2025.

Burton Crawford L, Akand E, Contractor S, and Scott Sisson (2022) 'Legislative complexity: what is it, how do we measure it, and why does it matter?' *AUSPUBLAW* website.

Child Protection Systems Royal Commission (SA) (2016) *The life they deserve, Child Protection Systems Royal Commission Report, Volume 1: Summary and Report,* South Australian Department for Child Protection website, accessed 3 October 2025.

CMS Law (2025) *Digital identity in the UK: A new legislative framework under the DUA Bill*, CMS Law-Now website, accessed 01 August 2025.

Cooper A, Marskell J, and Chan C H (2022) *National Digital Identity and Government Data Sharing in Singapore: A Case Study of Singpass and APEX (English)*, World Bank, accessed 30 September 2025.

Data Availability and Transparency Bill 2020 (DAT Bill 2020a) Second Reading. Robert, Stuart (LNP) 9 December 2020, accessed 14 July 2025.

Data Availability and Transparency Bill 2020 (DAT Bill 2020b), Second Reading, Shorten, Bill MP (ALP) 30 March 2022, accessed 14 July 2024.

Data Availability and Transparency Bill 2022, accessed 15 July 2025.

Datafordeler (n.d.) *Datafordeler*, Datafordeler website, accessed 25 September 2025.

Data.gov.au (n.d.) *data.gov.au [beta]*, Australian Government website, accessed 30 September 2025.

Dataplace (n.d.) *Welcome to Dataplace,* Australian Government website, accessed 30 September 2025.

Department of Finance (2024a) *Chief Data Officer Information Pack,* Department of Finance website, accessed 30 September 2025.

Department of Finance (2024b) *Digital ID Accreditation*, Department of Finance website, accessed 4 August 2025.

Department of Finance (2024c) *Data and Digital Ministers Meeting - Terms of Reference,* Department of Finance website, accessed 30 September 2025.

Department for Science, Innovation & Technology (UK) (2025) *Information sharing for public service delivery: expanding the information sharing powers in Part 5 (chapter one) of the Digital Economy Act 2017 to support passported benefits and reduce fuel poverty*, Gov.UK website, accessed 29 September 2025.

Department of Statistics Singapore (n.d.) *Anonymised Microdata Access Program (AMAP)*, Department of Statistics Singapore website, accessed 17 September 2025.

Digital ID & Authentication Council of Canada (2025a) *PCTF & Certification*, Digital ID & Authentication Council of Canada website, accessed 4 August 2025.

Digital ID & Authentication Council of Canada (2025b) *Trust Framework*, Digital ID & Authentication Council of Canada website, accessed 4 August 2025.

DTA (Digital Transformation Agency) (n.d. a) *Australian Government data catalogue*, DTA website, accessed 30 September 2025.

DTA (n.d. b) *Australian National Data Integration Infrastructure (ANDII)*, DTA website, accessed 30 September 2025.

DTA (n.d. c) *Information asset management standard*, DTA website, accessed 30 September 2025.

Dominello, V (2025) *The art of horizontal government*, Heywood Quarterly, Fourth Edition, accessed 30 September 2025.

European Commission (2014) *Q&A: Electronic Identification and Trust Services (eIDAS) Regulation*, European Commission website, accessed 4 August 2025.

European Commission (2019) *Open Data Maturity Report 2019*, European Data Portal, European Commission, accessed 25 September 2025.

European Commission (2025) *eIDAS Regulation*, European Commission website, accessed 4 August 2025.

GA (Geoscience Australia) (2024) *Annual Report 2023-24*, GA website, accessed 30 September 2025.

Government of Canada (n.d. a) *Open Government Portal*, Government of Canada website, accessed 30 September 2025.

Government of Canada (n.d. b) *Access to microdata*, Government of Canada website, accessed 30 September 2025.

Government of South Australia (2020) *PC 012 – Information Privacy Principles (IPPS) Instruction*, Premier and Cabinet Circular, Department of Premier and Cabinet (South Australia) website, accessed 3 October 2025.

Greenfield D, Hinchcliff R, Banks M, Mumford V, Hogden A, Debono D, Pawsey M, Westbrook J, and Braithwaite J (2015) 'Analysing 'big picture' policy reform mechanisms: the Australian health service safety and quality accreditation scheme', *Health expectations: an international journal of public participation in health care and health policy*, 18(6):3110-3122, doi: 10.1111/hex.12300.

ICES (Institute for Clinical Evaluative Sciences) (n.d.) About ICES Data, ICES website, accessed 30 September 2025.

ICO (Information Commissioner's Office) (2020) *Code of Practice for public authorities disclosing information under chapters 1, 3 and 4 (Public Service Delivery, Debt and Fraud) of Part 5 of the Digital Economy Act 2017* (DEA Code of Practice), accessed 29 September 2025.

ICO (2022) 'Lawfulness', *Data sharing: a code of practice*, UK Government, accessed 29 September 2025.

ICO (2023) *A guide to the data protection principles*, ICO website, accessed 29 September 2025.

Information System Authority (ISA) (n.d.) *Estonian open data portal*https://www.ria.ee/en/state-information-system/data-based-governance-and-reuse-data/estonian-open-data-portal, Information System Authority, Republic of Estonia website, accessed 29 September 2025.

Jobs and Skills Australia (n.d.) *VET National Data Asset (VDNA)*, Jobs and Skills Australia website, accessed 8 October 2025.

Kruk R (2023) *Independent review of Australia's regulatory settings relating to overseas health practitioners*, COAG Health Council, accessed 25 August 2025.

NDDA (National Disability Data Asset) (2025) *About the National Disability Data Asset,* NDDA website, accessed 30 September 2025.

NIAA (National Indigenous Australians Agency) (2025) *Framework for Governance of Indigenous Data (GID)*, NIAA website, accessed 30 September 2025.

NDIS Quality and Safeguards Commission (2025a) *Rules and standards*, NDIS Quality and Safeguards Commission website, accessed 25 August 2025.

NDIS Quality and Safeguards Commission (2025b) *About registration*, NDIS Quality and Safeguards Commission website, accessed 25 August 2025.

NIIS (Nordic Institute for Interoperability Solutions) (n.d.) *X-Road – The Free and Open Source Data Exchange Layer*, API Conference, accessed 29 September 2025.

OAIC (Office of the Australian Information Commissioner) (n.d.) *Australian Privacy Principles,* OAIC website, accessed 30 September 2025.

ONDC (Office of the National Data Commissioner) (2023) *DATA Scheme Safeguards*, ONDC website, accessed 30 September 2025.

ONDC (2024) *Data Scheme Working Group Findings and Actions*, ONDC website, accessed 30 September 2025.

ONDC (2025) *DataPoints: August 2025 Edition* ONDC website, accessed 30 September 2025.

OPC (Office of Parliamentary Counsel) (2016) *OPC's Guide to Reducing Complexity in Legislation*, Office of Parliamentary Counsel, Australian Government website, accessed 22 September 2025.

Privacy Commissioner / Te Mana Mātāpono Matatapu (2015) *An A to Z of Approved Information Sharing Agreements (AISAs),* New Zealand Government website, accessed 29 September 2025.

Privacy Commissioner / Te Mana Mātāpono Matatapu (n.d.) *Background to AISAs*, Office of the Privacy Commissioner website, accessed 29 September 2025.

Queensland Government (2022) *Information sharing authorising framework (ISAF),* Queensland government website, accessed 3 October 2025.

Rauh I (2025) *eIDAS: 4 key challenges that remain*, Swisscom Trust Services website, accessed 4 August 2025.

Sax Institute (n.d.) *Secure Unified Research Environment – Australia's most trusted research platform*, Sax Institute website, accessed 30 September 2025.

Senate Finance and Public Administration Legislation Committee (Senate Legislation Committee 2021a) *Data Availability and Transparency Bill 2020*, Australian Government website, accessed 15 July 2025.

Senate Finance and Public Administration Legislation Committee (Senate Legislation Committee 2021b) *Data Availability and Transparency Bill 2020, Labor Senators' Dissenting Report*, Australian Government website, accessed 15 July 2025.

Senate Standing Committee for the Scrutiny of Bills (Scrutiny Committee 2021a), *Scrutiny Digest, 1, 29 January 2021*, Australian Government website, accessed 14 July 2025.

Senate Standing Committee for the Scrutiny of Bills (Scrutiny Committee 2021b), *Scrutiny Digest, 3, 2021, 17 February 2021*, Australian Government website, accessed 15 July 2025.

Senate Standing Committee for the Scrutiny of Bills (n.d.), Australian Government website, accessed 14 July 2025.

SA DPC (South Australia Department of the Premier and Cabinet) (n.d.) *Information Sharing Guidelines for promoting safety and wellbeing,* SA Treasury website, accessed 3 October 2025.

SA Treasury (South Australia Department of Treasury and Finance) (n.d. a) *Data analytics and Information sharing – Completed projects,* SA Treasury website, accessed 3 October 2025.

SA Treasury (n.d. b) *Data analytics and Information sharing – Current projects,* SA Treasury website, accessed 3 October 2025.

SA Treasury (n.d. c) *South Australia's Data Governance,* SA Treasury website, accessed 3 October 2025.

Statistics Canada (2019) *Statistics Act and Research Data Centre program (guidelines for deemed employees)*, Statistics Canada website, accessed 4 August 2025.

Stats NZ / Tatauranga Aotearoa (2022) *How we keep integrated data safe*, Stats NZ website, accessed 30 September 2025.

Stats NZ / Tatauranga Aotearoa (2023) *Data leadership*, Stats NZ website, accessed 30 September 2025.

Social Investment Agency / Toi Hau Tangata (2025) *SIA and the Data Exchange*, Digital.gov.nz website, accessed 30 September 2025.

Social Investment Agency / Toi Hau Tangata (n.d.) *Data Exchange*, Social Investment Agency website, accessed 30 September 2025.

UK Cabinet Office (2025) *The Digital Economy Act 2017 – Debt and Fraud Information Sharing Review Board*, Gov.UK website, accessed 29 September 2025.

UK Government (n.d.) *Digital Economy Act 2017: Public Service Delivery Review Board*, Gov.UK website, accessed 29 September 2025.

UKSA (UK Statistics Authority) (2020) *Research Code of Practice and Accreditation Criteria*, accessed 29 September 2025.

UWE (University of the West of England) (n.d.) *The Five Safes*, Five Safes website, accessed 30 September 2025.

WA DPC (Western Australia Department of the Premier and Cabinet) (2025), *PeopleWA*, wa.gov.au website, accessed 30 September 2025.

Legislation

Aged Care Quality and Safety Commission Act 2018 (Cth)

Archives Act 1983 (Cth)

Australian Institute of Health and Welfare Act 1987 (Cth)

Census and Statistics Act 1905 (Cth)

Census and Statistics (Information Release and Access) Determination 2018

Data and Statistics Act 2022 (NZ)

Data Availability and Transparency Act 2022 (Cth)

Data Protection Act 2018 (UK)

Data (Use and Access) Act 2025 (UK)

Data-matching Program (Assistance and Tax) Act 1990 (Cth)

Digital Economy Act 2017 (UK)

Digital Government (Disclosure of Information) Regulations 2018 (UK)

Digital Government (Disclosure of Information) (Identity Verification Services) Regulations 2024 (UK)

Digital ID Act 2024 (Cth)

Freedom of Information Act 1982 (Cth)

Information Privacy Act 2009 (Qld)

National Health Reform Act 2011 (Cth)

Privacy Act 1988 (Cth)

Privacy Act 2020 (NZ)

Privacy and Responsible Information Sharing Act 2024 (WA)

Public Sector (Data Sharing) Act 2016 (SA)

Public Sector (Governance) Act 2018 (Singapore)

Statistics Act 1973 (Singapore)

Statistics Act 1975 (NZ)

Statistics Act 1985 (CA)

Statistics and Registration Service Act 2007 (UK)

Taxation Administration Act 1953 (Cth)