Australian Government

Services Australia

Submission

Review of the

Data Transparency and Availability Act (2022)

May 2025

Data and Analytics Division/Services Australia

Contents

Executive Summary

Services Australia (the agency) welcomes the opportunity to provide input into the review of the *Data Availability and Transparency Act* (DAT Act). The agency is supportive of the intent of the DAT Act, which aims to improve access to government data and establish a structured accreditation scheme overseen by the National Data Commissioner (ONDC). The DATA Scheme (the Scheme) is designed to balance increased data sharing with appropriate privacy and security provisions.

Since the inception of the Scheme in 2022, Services Australia has received only two requests for data via DataPlace, with most data requests being released under existing mechanisms such as Public Interest Certificates (PIC). Although the agency is not an Accredited Data Service Provider (ADSP) under the DAT Act, it collects and stores a significant amount of sensitive data through, and in support of, the delivery of a range of government services.

Based on our experience engaging with the Scheme, we provide the following comments:

1. **Legal Framework Uncertainty**: The DAT Act needs to adequately account for privacy and secrecy provisions. While the Act intended to simplify data sharing, operationalising it has proven complex due to legal, ethical, and consent considerations. The lack of clarity on the interaction between the DAT Act and existing legislation has created uncertainties.
2. **Custodianship**: The DAT Act needs to provide clear guidance on joint custodianship. Determining the data custodian ensures the appropriate entity authorises the disclosure. However, joint custodianship requires multiple entities to make determinations of public interest, which can lead to complexity through both conflicting policy and legal advice.
3. **Accreditation**: Accreditation processes under the DAT Act are complex and there is not sufficient regulation to ensure that accreditation is an appropriate risk mitigation for sharing sensitive datasets. Services Australia is co-leading the Trusted Entity Project with the Queensland Government to streamline the current approach to accreditation and develop guidance material to define what it means to be a 'trusted entity'.
4. **Interoperability**: Investment is required to operationalise government systems and processes to enable effective and efficient data sharing. Disparate data systems make standardised data sharing difficult and resource intensive.

Collectively these issues add to the administrative burden on the agency and impact seamless data sharing which the DAT Act was designed to deliver. Services Australia remains committed to supporting the intent of the DAT Act and looks forward to working collaboratively to address these challenges and improve the Scheme's effectiveness.

Legal Framework Uncertainty

The DAT Act needs to adequately account for privacy and secrecy provisions.

While the DAT Act intended to simplify data sharing, this has not been the agency's experience in operation. For example, to share the Medicare Consumer Directory (MCD) for the purposes of the National Disability Data Asset, the agency explored the use of the DAT Act extensively. Due to the complexity of legal, ethical, and consent considerations and accreditation processes, a PIC was utilised instead.

Services Australia is uniquely positioned as a custodian of personal, sensitive, and protected information from almost every Australian. This means that a considerable amount of data we hold is protected under the *Privacy Act 1988* as well as other legislation. The DAT Act was intended to be complementary and overarching to these existing legal frameworks, however, operationally the interaction between the application of the DAT Act and existing legislation (Australian Privacy Principles, secrecy provisions, and state laws) has created compliance uncertainties.

To share personal information under the DAT Act, we need consent of the person or we need for the Commissioner to determine it is unreasonable or impracticable to obtain consent. Where personal information is involved, then the Privacy Act provisions remain in place. We always require consent to share biometric data.

One example where the agency cannot share relates to My Health Record. The Regulations bar sharing data of entities acting in a capacity under the *My Health Records Act 2012*. These include the System Operator, Data

Custodian within the meaning of the *My Health Records Act 2012*, Chief Executive Medicare, and any other entity that is a participant in the My Health Records system.

Data agreements are long and complex when considering all requirements must be articulated within. These are difficult for the agency to navigate and create an administrative burden as we strive to balance data sharing goals against legal and ethical requirements, creating a tension for implementation.

Risks increase for non-government entities as it is harder to define public interest. Additionally, there are also ongoing risks with onward sharing, for example, universities. Non-government entities may not have the same level of understanding or commitment to privacy and security as government agencies, which can lead to potential misuse or unauthorised disclosure of sensitive data.

Furthermore, the complexity of data agreements and the administrative burden they create can result in delays and inefficiencies in data sharing processes. This can hinder the agency's ability to achieve its data sharing goals while maintaining compliance with the requirements of the DAT Act.

The agency must also consider the potential impact on public trust and the need to manage data breach processes for actions of other entities that are outside of its control. The Robodebt Royal Commission has highlighted the importance of clear accountability for agencies that collect data, ensuring they are held responsible for downstream misuse or unauthorised disclosure, which is not consistent with current legal interpretations of the responsibilities associated with data sharing.

Recommendations for consideration:

- Improve guidance to manage legal ambiguity, transparency, and consent arrangements.
- Build greater awareness amongst non-data decision makers, particularly in legal areas, about the Scheme and what it means to be an ADSP. This would reduce administrative effort by creating a more efficient and standardised process for handling data sharing requests.
- A tiered approach based on risk should be taken to manage expectations around timeframes, requirements for legal advice and ethic assessments for highly sensitive personally identifiable information vs non-sensitive government data. The data Services Australia holds could have customer safety implications if not shared carefully.

Custodianship

The DAT Act needs to provide clear guidance on joint custodianship.

Joint custodianship is difficult to operationalise as realistically, there can only be one true data custodian. To be considered a data custodian, the entity must be the holder of the relevant data and be responsible for managing its use, disclosure, and protection. In the context of our agency, we are the primary collector of the data, which means we carry all the risk and administrative and technical burden associated with sharing it.

Determining the data custodian ensures the appropriate entity and delegate authorise the disclosure. However, joint custodianship under the DAT Act requires multiple entities to make determinations and authorise the release of the data, which can lead to conflicting legal advice.

Under the current arrangements, the agency ends up carrying all the risk associated with data sharing that has been authorised by another entity, as seen in the case of releasing the MCD data. In this circumstance, the agency will be held accountable for public trust concerns and managing data breach processes for actions of other entities that are outside of our control. An outcome of the Robodebt Royal Commission is a diminished risk appetite and a very clear signal that agencies who collect the data will be held accountable for downstream misuse or unauthorised disclosure.

Recommendations for consideration:

- Strengthen the definition around accountability requirements for joint custodianship, and ideally nominate which custodian is the decision maker and risk owner. Without clear accountabilities, it is difficult to ensure customer data is protected.

Accreditation

Accreditation is not well understood, especially by those providing legal assurance over requests.

As a custodian of all Australians' personal data, Services Australia needs to be assured that an entity can be trusted when sharing data. The current accreditation processes under the DAT Act are complex, with many entities utilising alternative established accreditation mechanisms to receive and share data instead.

Services Australia is co-leading the Trusted Entity Project with the Queensland Government. The project aims to develop a shared understanding of opportunities for improvement, streamline the current approach to accreditation under the DAT Act, and create guidance material to define what it means to be a 'trusted entity.' The project is working closely with the Department of Finance and will submit the final report in August 2025 for consideration as part of the DAT Act review.

An ideal state is where the role, responsibilities, accountabilities, and accreditation requirements for trusted entities are detailed in the legislation to create efficiencies for data custodians. Additionally, the ONDC should be required by legislation to regulate the DATA Scheme to ensure that ADSPs are handling the data the way they should.

Recommendations for consideration:

- Define in the legislation the role, responsibilities, accountabilities and accreditation requirements for ADSPs to create efficiencies for data custodians.
- The ONDC should be required by legislation to regulate the DATA Scheme to ensure that ADSPs are handling the data the way they should.
- Create clearer guidelines and processes for sharing data with non-government entities, such as universities, to foster research while maintaining security and trust.

Interoperability

Investment is required to operationalise government systems and processes to enable effective and efficient data sharing.

Disparate data systems with varying levels of sophistication make standardised data sharing difficult and resource intensive, as seen with the MCD. In the context of Services Australia, where requests for data are large in both volume and scale, the process of curating data and establishing secure transfer pipelines is costly.

The exclusion of certain organisations under the DAT Act due to accreditation requirements restricts the agency’s ability to comply with other mandatory frameworks, such as The Framework for the Governance of Indigenous Data.

Recommendations for consideration:

- Mandate a minimum viable system requirement for system-to-system data sharing when disclosure is requested under the DAT Act.
- Government to lead the investment in data sharing infrastructure.
- Facilitate non-government collaboration and participation (e.g. enabling Aboriginal and Torres Strait Islander community groups to participate in the DATA Scheme).

servicesaustralia.gov.au