8 August 2025

Department of Finance
Australian Government

By email: DATActReview@finance.gov.au

Submission to Statutory Review of the *Data Availability and Transparency Act 2022* (Cth) (DAT Act) – Draft Findings and Recommendations

This submission is prepared by Lyria Bennett Moses, relevantly a Professor in the School of Law, Society and Criminology in the Faculty of Law and Justice at UNSW and a researcher with the UNSW-UTS Trustworthy Digital Society Hub and Nicholas Hodgkinson, relevantly a Research Assistant with the UNSW-UTS Trustworthy Digital Society Hub. The UNSW-UTS Trustworthy Digital Society Hub has funded a seed project, in collaboration with the Australian Research Data Commons (**ARDC**), exploring the feasibility and implications of Australian "dataspaces".

In summary, we agree that the DAT Act and other legislation and policies need substantial reform, but:

- **We believe that the draft recommendations are inadequate; and**
- **We remain concerned about some of the proposed solutions, given the current operation of the DAT Act as an "override" mechanism rather than an integrated data policy.**

We want to emphasise that most of the DAT Act's issues are due to its conceptual structure. Our submission is otherwise organised around selected focus questions for each Recommendation in the Draft Findings and Recommendations Paper.

1. The DAT Act should not be treated as an "override" mechanism

Consider the following findings in the Draft Findings and Recommendations Paper:

- 'Some features (such as its framing as a secrecy override) indicate it is to be as an authorising pathway of 'last resort'. Others indicate that it is intended to provide a comprehensive system for all Commonwealth data sharing.' (page 7)
- 'Many of the protective settings imposed by the DAT Act are disproportionate for lower-risk instances of data sharing.' (page 9)
- DAT Act 'accreditation is viewed as one-size-fits-all'. (page 11)

UNSW SYDNEY NSW 2052 AUSTRALIA
T [redacted] | F [redacted] | ABN 57 195 873 179 | CRICOS Provider Code 00098G

Each of these issues relates to the conceptual structure of the DAT Act.

Substantive regulations as to the circumstances in which data of different kinds can be shared, the reasons for which it can be shared, and the persons with whom it can be shared, already exist.[1] It makes no sense at all, at least from a policy-making perspective, for there to be careful, context-specific regulation of data governance on one hand,[2] but then a single override in the DAT Act that is context-agnostic.

The layering of legislation also creates transparency issues, evident in government agency privacy policies. For instance, the Department of Education's policy mentions sharing data with other Commonwealth agencies, but omits DATA Scheme sharing. Similarly, Department of Home Affairs' policy lists legislation under which data may be disclosed—the DAT Act is not on it. Assuming this isn't deliberate obfuscation, it appears disclosures under the DATA Scheme are considered are outside the scope of legislation—namely, the *Privacy Act*—that mandates privacy policies. However, if the DATA Scheme were to facilitate meaningful levels of data sharing, this omission could mislead data subjects

What is needed here is coherence. That is more work than simply updating the DAT Act, but it is the only sustainable mechanism for coherent data policy in Australia.

However, assuming this structure is to be retained, our more specific responses are below.

2. Recommendation 2

Recommendation 2 proposes that 'highly detailed data sharing agreements should not be the primary mechanism to authorise sharing' and that the requirements for such agreements should be 'scaled back'. At a general level, we would argue against that, particularly given the need for robust data governance and the current absence of other comprehensive legislative means by which that might be effectively achieved.[3] Unless obligations that would ordinarily appear in a data sharing agreement—such as to destroy data at the conclusion of the project—are formally embedded within the proposed rules or other binding instruments, contractual agreements are required to ensure enforceability of such requirements.

3. Recommendation 3

It makes sense to keep the DAT Act 'high level', 'principles-based' and 'outcomes-focused' with detail and guidance in subordinate legislation. In line with our earlier submission, we would suggest a sufficient level of flexibility in the DAT Act to leave open the possibility of sharing within dataspaces.

We also note on Recommendation 3 that data protection rules are not limited to the *Privacy Act* but can be found in different legislation with adjusted requirements.

---

[1] See, eg, *Privacy Act 1988* (Cth); see also portfolio legislation like the *My Health Records Act 2012* (Cth) (and related legislation like the *Health Insurance Act 1973* (Cth)); the *National Health Act 1953* (Cth) (and the *National Health (Privacy) Rules 2018* (Cth); the *Migration Act 1958* (Cth) (and *Australian Border Force Act 2015* (Cth) and *Australian Citizenship Act 2007* (Cth) and *Customs Act 1901* (Cth)).

[2] Which we note, incidentally, needlessly adopts different definitions of key concepts and terms.

[3] See generally Shiri Krebs and Lyria Bennett Moses, 'Data Sharing Agreements: Contracting Personal Information in the Digital Age' (2024) 48(1) Melbourne University Law Review 95, <https://www.austlii.edu.au/cgi-bin/viewdoc/au/journals/MelbULawRw/2024/3.html>.

4. Recommendation 5

We would strongly argue against the proposal for a Ministerial power to authorise data sharing in the national interest. While the Draft Findings and Recommendations contemplates that this power will be reserved for 'exceptional circumstances' and constrained by 'appropriate safeguards', it introduces a political dimension to decisions that should be grounded in consistently applied and transparent criteria.

As per our earlier point, the DAT Act's conceptual structure being an "override" mechanism—rather than an integrated data policy—is already problematic. Introducing a political override only exacerbates this. Such a power risks undermining the integrity and perceived objectivity of the entire data sharing framework:

1. Agencies might be incentivised to lean on the Ministerial power to secure funding or avoid a perceived personal risk associated with administrative decision-making;
2. Agencies might view the framework as being politically driven, rather than a collaborative effort geared towards achieving public interest outcomes through established data governance principles.
3. Such a Ministerial power would accentuate rather than resolve the existing lack of clarity as to whether the DATA Scheme a pathway "of last resort" or more than that.

4. Recommendation 6

The functions of the Commissioner are confused in the DAT Act, and the proposed solutions risk compounding this confusion.

We reiterate the point in our initial submission that a national strategy for data protection and sharing needs to be developed. This function could be a role for an independent statutory office. Similarly, if the DATA scheme continues in its present form as an "override" mechanism, rather than integrated data policy, a regulator may still be needed to oversee its operation. But the roles of policy developer and regulator should be kept separate—to avoid conflicts of interest and inefficiency, amongst other things.

5. Recommendation 8

Recommendation 8 proposes the introduction of explicit accreditation 'tiers' to simplify standards and align with data sharing use-cases. We understand the argument for that based on differential risk in different contexts. However, as we have argued above, the underlying "alignment problem" is not simply a question of updating the DAT Act. Different kinds of data are currently dealt with haphazardly through distinct and unconnected regulatory interventions. So the underlying 'rules' for data processing differ from 'personal information' in the *Privacy Act* to specific kinds of data that have their own separate rules (for example, CDR data). If we are to truly simplify the system as a whole, we need to think about tiering not only for levels of accreditation but for specific features of data that warrant distinct treatment and bring the underlying data rules together in a coherent way. In other words 'tiering' is not only an issue for accreditation (brought together under a revised DAT Act) but an issue for processing rules (currently sprinkled over numerous separate context-specific pieces of legislation). Ideally, the tiering for both could align (in other words, more extensive

accreditation requirements would apply to data that, under a coherent data governance law, would was classified as higher risk in one or more dimensions.

Yours sincerely,

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

Nicholas Hodgkinson
Research Assistant
[redacted]