Australian Government

Office of the Australian Information Commissioner

Senate Finance and Public Administration Legislation Committee – Inquiry into the Data Availability and Transparency Bill 2020

Submission by the Office of the Australian Information Commissioner

Angelene Falk

Australian Information Commissioner and Privacy Commissioner

12 March 2021

OAIC

Contents

Introduction

1. The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to make a submission to the Senate Finance and Public Administration Legislation Committee's inquiry into the Data Availability and Transparency Bill 2020 (the DAT Bill) and the Data Availability and Transparency (Consequential Amendments) Bill 2020 (the Consequential Amendments Bill).

2. The DAT Bill proposes to create the Data Availability and Transparency scheme (DAT scheme) to enable Australian Government agencies to share public sector data with particular entities for particular purposes, and under particular conditions.

3. The OAIC is an independent Commonwealth regulator, established to bring together three functions: privacy functions (protecting the privacy of individuals under the *Privacy Act 1988* (Cth) (Privacy Act) and other legislation), freedom of information functions (access to information held by the Commonwealth Government in accordance with the *Freedom of Information Act 1982* (FOI Act)), and information management functions (as set out in the *Information Commissioner Act 2010* (Cth)).

4. Upholding information access rights and supporting the proactive release of government-held information are therefore key strategic priorities for the OAIC.[1] This recognises that data held by the Australian Government is a national resource which can yield significant benefits for the Australian people when handled appropriately, and in the public interest. The DAT scheme is one of several current Australian Government initiatives that reflect this policy objective, including the proposed expansion of myGov and the Digital Identity scheme.

5. Nevertheless, proposals to share data containing personal information will necessarily carry certain privacy risks, including the loss of control by individuals and the potential for mishandling of personal information. Privacy risks can be heightened in relation to Government-held personal information, which is often collected on a compulsory basis to enable individuals to receive a service or benefit or is otherwise required by law. Such data is often sensitive or can become sensitive when it is linked with other government data sets.

6. Robust data protection and privacy safeguards are therefore central to successful data sharing initiatives. The *Privacy Act 1988* (Cth) provides a well-established framework to minimise the privacy risks posed by data sharing activities. The Government's review of the Privacy Act, which commenced on 30 October 2020, will consider whether the Privacy Act can be further enhanced to better empower consumers, protect their data and serve the Australian economy.[2]

7. Together, the Privacy Act and the DAT legislative framework will apply to protect the personal information of individuals that is shared within the DAT scheme. The DAT Bill invokes the 'required or authorised by law' exception to Australian Privacy Principles (APP) 3 and 6 in the Privacy Act, to permit personal information to be collected, used and disclosed under the DAT

[1] See Strategic Priorities 2 and 3 in the OAIC's Corporate Plan 2020-21.

[2] https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988.

scheme. In addition, the scheme would override a range of existing secrecy provisions that ordinarily prevent the sharing of data, including personal information.[3]

8. However, data scheme entities covered by the Privacy Act continue to have obligations under the APPs and in relation to the Notifiable Data Breaches scheme. These include obligations relate to governance, privacy policies, collection notices, data quality and security, access and correction. The Privacy (Australian Government Agencies – Governance) APP Code 2017 also continues to apply to Australian Government agencies operating under the DAT scheme, including the requirement for agencies to conduct a Privacy Impact Assessment (PIA) for all high privacy risk projects.

9. The OAIC has engaged with the Office of the National Data Commissioner (ONDC)[4] throughout the development of this legislative package to help ensure that privacy and security play a central role in the legislative framework. This is crucial to achieve the Bill's objectives of enabling 'consistent safeguards for sharing public sector data', enhancing 'integrity and transparency in sharing public sector data' and building 'confidence in the use of public sector data'.[5]

10. The OAIC supports the measures that have been included in the legislative package that are designed to build on the existing privacy framework to minimise the privacy impacts of the DAT scheme. These measures include:

- Requiring all data scheme entities to be covered by the Privacy Act or a law of a State or Territory that provides a commensurate level of privacy protection, monitoring of compliance with the law, and a means for an individual to seek recourse if their personal information is mishandled.
- Requiring consent to be obtained if the personal information of individuals is to be shared, unless it is unreasonable or impractical to seek their consent.
- Requiring entities to outline how the public interest is served by the sharing in a data sharing agreement.

11. This submission recommends the inclusion of additional privacy measures that will provide further protections for individuals and clarity for data scheme entities about their privacy obligations. The OAIC considers that these additional measures are necessary to ensure the

[3] Clause 23, Data Availability and Transparency Bill 2020.

[4] Office of the Australian Information Commissioner 2018, New Australian Government Data Sharing and Release Legislation – Submission to the Department of Prime Minister and Cabinet, OAIC, Sydney: https://www.oaic.gov.au/engage-with-us/submissions/new-australian-government-data-sharing-and-release-legislation-submission-to-department-of-prime-minister-and-cabinet/

Office of the Australian Information Commissioner 2019, Data Sharing and Release legislative reforms discussion paper — submission to the Department of Prime Minister and Cabinet, OAIC, Sydney: https://www.oaic.gov.au/engage-with-us/submissions/data-sharing-and-release-legislative-reforms-discussion-paper-submission-to-prime-minister-and-cabinet/

Office of the Australian Information Commissioner 2020, Data Availability and Transparency Bill 2020: exposure draft consultation – submission to the Department of Prime Minister and Cabinet, OAIC, Sydney: https://www.oaic.gov.au/engage-with-us/submissions/data-availability-and-transparency-bill-2020-exposure-draft-consultation/

In addition, the Australian Information Commissioner is a member of the National Data Advisory Council.

[5] Clause 3, Data Availability and Transparency Bill 2020.

proportionality of the scheme and to achieve the trust and confidence of the community, which is vital to the success of the DAT scheme.

12. Additionally, the OAIC is concerned about the proposed exemption of scheme data from the FOI Act, which the OAIC considers runs counter to the objects of both the FOI Act and the DAT Bill.

Proposal to exempt agencies from the FOI Act

13. The Consequential Amendments Bill proposes to amend the FOI Act to exempt agencies from the operation of the FOI Act in relation to specified documents, including documents that were shared with or through agencies under cl 13(1) of the DAT Bill, and data that has been enhanced (for example, integrated or cleaned) by an Accredited Data Service Provider.

14. The OAIC notes that this proposed amendment would effectively exempt any data that government agencies share with each other through the scheme. This exemption does not extend to documents that are outputs within the meaning of the DAT Bill. The Explanatory Memorandum to the Consequential Amendments Bill notes that agencies may still grant access to copies of datasets that are held outside of the DAT scheme.

15. The OAIC is concerned that the proposal is unnecessarily broad and risks misalignment with the objects of the FOI Act to provide a fundamental legal right to access to documents. The OAIC is also concerned that this proposal reduces the information access rights of individuals, impacting on their ability to seek access to their own personal information and understand how agencies are using this information.

16. The EM justifies this exemption from the FOI Act as necessary to preserve protections for data under the DAT Bill, which has created 'a controlled environment for sharing … For example, data shared under the scheme may include personal, commercial, and highly sensitive Commonwealth data… Allowing open access to this data under the FOI Act could undermine the scheme's protections and uptake.'

17. However the OAIC notes that data that is subject to the FOI Act may be exempt from disclosure under existing exemptions in the FOI Act which could be applied by the relevant agency should an FOI request for data shared under the scheme be received. Personal information may be exempt from disclosure under s 47F (personal privacy) if disclosure would be contrary to the public interest, commercial data may be exempt from disclosure under ss 47 (trade secrets or commercially valuable information) or 47G (business). Sensitive government data may be exempt from disclosure under s 33 (national security, defence or international relations), s 37 (enforcement of law and protection of public safety), s 38 (secrecy provisions of enactments), s 45 (material obtained in confidence), s 47B (Commonwealth-State Relations), s 47D (financial or property interests of the Commonwealth, s 47H (research) and s 47J (the economy).

18. The OAIC recommends that consideration is given to this proposed consequential amendment to the FOI Act being removed, and that data that is shared by agencies under the scheme remains subject to the usual FOI processes and potential exemptions under the FOI Act. Building on existing transfer mechanisms in the FOI Act, Data Custodians and Accredited Users could be supported to deal with such FOI requests through the inclusion of specific provisions in the FOI Act that:

- Allowed for the transfer of data back to the Data Custodian in the event an FOI request is received by the agency with which the data was shared as an Accredited User, or
- Required the Accredited User to consult with the original Data Custodian if data that had been shared with them under the DAT scheme is requested through the FOI Act.

Recommendations for additional privacy safeguards

19. While the OAIC acknowledges the important privacy safeguards that have been included in the DAT Bill, there are other key privacy protective measures that should be included to further mitigate the risks posed by sharing personal information.

De-identification

20. The data principle in cl 16(8) of the DAT Bill states that 'only the data reasonably necessary to achieve the applicable data sharing purpose' should be shared; and 'the sharing of personal information [should be] minimised as far as possible without compromising the data sharing purpose.' The Explanatory Memorandum (EM) notes that the data principle requires data custodians to consider 'whether to provide an entire dataset or a customised extract of particular variables, and the level of detail of (and any treatments applied to) that data.' Examples of appropriate treatments in the EM include the removal of records that could directly identify a person, for example, through de-identification.

21. The OAIC supports the elevation of the requirement to minimise the amount of personal information shared from guidance into primary legislation, following consultation on the Exposure Draft of the DAT Bill. However, the OAIC shares the concerns of the Standing Committee for the Scrutiny of Bills (the Committee) that, 'while the data principles contemplate minimising the sharing of personal information as far as possible and sharing only the data reasonably necessary to achieve an applicable purpose, there are no requirements for sharing only de-identified data in the principles or elsewhere in the bill.'[6]

22. This is consistent with the OAIC's position throughout the development of the DAT scheme, that the data sharing should occur on a de-identified basis where possible, to minimise the privacy impacts of the scheme for individuals. The OAIC recommends that the Bill include a requirement that data custodians must not share personal information where the data sharing purpose can reasonably be met by sharing de-identified information.

23. Any definition of 'de-identified' used in the DAT Bill should align with the definition in the Privacy Act: personal information is 'de-identified' if the information is no longer about an identifiable individual or an individual who is reasonably identifiable.[7] Such an approach is technology neutral and would enable the data custodian to apply the most appropriate de-identification technique to the data to ensure that personal information is protected and that the information will still be useful for its intended purpose after the de-identification process.[8]

[6] Senate Standing Committee for the Scrutiny of Bills, Scrutiny Digest 1 of 2021, 29 January 2021.

[7] Section 6(1) of Privacy Act.

[8] See https://www.oaic.gov.au/privacy/guidance-and-advice/de-identification-and-the-privacy-act/

24. As an additional transparency and accountability requirement that supports a data minimisation approach, cl 19 of the DAT Bill should be amended to require data sharing agreements to outline when personal information is being shared as part of a project.

Exit Mechanism

25. The DAT Bill includes an 'exit mechanism', which will allow an output to exit the data sharing scheme in two circumstances (cl 21). Output is defined in cl 10(4) as 'data that is the result or product of the use, by an accredited user, of public sector data shared with the accredited user under cl 13(1)'.

26. Under cl 21(1), an accredited user may provide individuals and businesses with outputs containing data about themselves to check the data is accurate by validating or correcting it. The data exits the scheme at the point at which the individual or business validates or corrects the data. The EM explains that the purpose of this exit mechanism is to support the use of outputs created for the data sharing purposes, particularly government service delivery for which accurate, up-to-date information is essential.' The OAIC notes that this data is likely to contain personal information.

27. The exit mechanism in cl 21 also allows an accredited user to release output in circumstances that are specified in the data sharing agreement for the project, as long as the release does not contravene a law of the Commonwealth or a State or Territory (cl 21(3)). 'Release' is defined in cl 9 of the DAT Bill as 'provide open access'. This is distinct from 'sharing' data, which means providing controlled access to that data.

28. The EM notes that cl 21(3) does not create an authorisation to release data (that is, it will not invoke the 'required or authorised by law' exception to APPs 3 and 6 in the Privacy Act), but instead serves to permit the output to exit the scheme if it is permitted by other legislation. Therefore, if that output contains personal information, it could only be disclosed by an accredited user if that disclosure is permitted by the Privacy Act. The EM notes that this exit mechanism is designed to facilitate release of outputs from the scheme, such as highly aggregated research outputs.

29. Once the output has exited the scheme, it is no longer 'scheme data', and therefore no longer regulated by the DAT legislation. The protections and obligations of other laws will apply to the data after it has exited the scheme, including the Privacy Act, where that data includes personal information.

30. The OAIC acknowledges that to maximise the benefits and utility of the DAT framework, it may be necessary for outputs to exit the scheme in certain circumstances. For example, sharing data to improve service delivery is likely to necessitate providing that data to individuals and businesses.

31. However, the OAIC recommends that additional protections are included in the DAT Bill to ensure that this exit mechanism minimises the risk to individuals' privacy and is only used in specific and confined circumstances:

- Only output that has been shared for the purpose of delivery of government services should be permitted to exit the scheme for validation or correction under cl 21(1), unless the ONDC can

identify a clear use case prior to the introduction of the legislation that reasonably necessitates data exiting the scheme for broader purposes.

- The DAT Bill should explicitly require the accredited user to take reasonable steps to ensure that the output is being shared with the entity or individual (or the individual's responsible person) that the output is about.
- Outputs that include personal information should not be permitted to be released from the data sharing scheme under cl 21(3). An accredited user will have collected the personal information from a data custodian and not directly from an individual. The individual will therefore have had no ability to consent to the information being disclosed outside the DAT scheme (which could include publication), or to decide to withhold their consent. Given the most likely scenario for data release under cl 21(3) will be sharing research or policy outcomes, it seems unlikely that personal information will be required to meet this purpose and should therefore be explicitly prohibited from release.

Automatic accreditation of Commonwealth Entities

32. Clause 74(3) of the DAT Bill requires the National Data Commissioner to automatically accredit certain Commonwealth bodies if they apply for accreditation as an accredited user under cl 76. This applies to non-corporate Commonwealth bodies and other Commonwealth bodies prescribed in the rules.

33. The OAIC notes that this is a significant change to the accreditation framework for the scheme, which has not been previously consulted on. Accreditation plays an important role in ensuring that entities have appropriate processes, systems and procedures in place to support safe personal information handling practices. The effectiveness of an accreditation framework rests on the accreditation criteria being set at an appropriate level and accreditation standards and processes being applied consistently across the scheme. A light touch or inconsistent approach to accreditation risks undermining the level of assurance that the framework is designed to provide. A robust accreditation process would provide a strong trust mark for the scheme.

34. The accreditation criteria in cl 77 of the DAT Bill includes requirements that the entity is able to manage scheme data accountably and responsibly, that the entity has designated an appropriately qualified individual to be responsible for overseeing the management of scheme data and that the entity is committed to continuous improvement in ensuring the privacy and security of scheme data.

35. The EM notes that non-corporate Commonwealth bodies already meet these accreditation criteria 'as they are subject to relevant Australian Government policies and frameworks, and to ongoing oversight by Ministers. Relevant measures… include… the Australian Government's Protective Security Policy Framework (PSPF) [and] the Privacy Act…. These measures ensure non-corporate Commonwealth bodies protect, manage, and use public sector data appropriately.'

36. As noted above, Commonwealth bodies are also required to comply with the Privacy (Australian Government Agencies – Governance) APP Code 2017, which, along with Australian Privacy Principle 1 in the Privacy Act, requires Commonwealth bodies to take a best practice approach to privacy governance to help build a consistent, high standard of personal information management across all Australian Government agencies. In particular, the Code requires

agencies to appoint a privacy officer and privacy champion, to have a privacy management plan and to provide appropriate privacy education and training to staff.

37. The OAIC recognises that these existing obligations are relevant to an entity's ability to handle data appropriately under the DAT scheme, and supports existing standards and processes being drawn on to streamline the accreditation framework. It is important that the privacy and security criteria are consistent with the Privacy Act and other existing privacy-related accreditation or certification schemes to ensure consistency and avoid fragmentation.

38. However, the OAIC considers that it is important that the accreditation framework include an upfront assessment of each entity that wishes to be accredited under the DAT scheme, and that the assessment is undertaken consistently in relation to all potential accredited entities. An upfront assessment component is an important safeguard in any accreditation framework to verify that an entity is compliant with regulatory and accreditation requirements and build accountability and transparency. For example, the initial assessment of entities that wish to receive consumer data under the Consumer Data Right (CDR) regime is one of the key assurance mechanisms in that framework, and has assisted in building trust and confidence in the CDR.

39. Compliance with the DAT scheme accreditation criteria could be demonstrated by drawing on the policies and processes, governance arrangements, training programs and data management protocols that an entity already has in place to comply with its existing obligations under other frameworks. However, an individual assessment of each application for accreditation by the National Data Commissioner would enable important oversight of how these obligations will be applied in the context of the DAT scheme. The OAIC considers that this should be the case even for Commonwealth bodies, who should still be subject to the same rigorous accreditation process, regardless of their broader privacy and security obligations.

40. Accordingly, the OAIC recommends that all accredited users are subject to the same accreditation processes and criteria as other entities seeking to become accredited under the DAT scheme.