Australian Government

Office of the Australian Information Commissioner

Data Availability and Transparency Bill 2020: exposure draft consultation

Submission by the Office of the Australian Information Commissioner

Angelene Falk

Australian Information Commissioner and Privacy Commissioner

6 November 2020

OAIC

Introduction

1. The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to comment on the legislative package for the Data Availability and Transparency (DAT) Bill 2020, which includes the exposure draft (the draft Bill), explanatory materials, and a Discussion Paper on the draft Accreditation Framework. A privacy impact assessment (PIA) on the draft Bill accompanies the legislative package.

2. The OAIC has had engagement with the Office of the National Data Commissioner (ONDC) throughout the development of this legislative package, including through two submissions to previous consultations.[1] In addition, the Australian Information Commissioner is a member of the National Data Advisory Council.

3. The legislative framework for the DAT scheme will comprise the draft Bill, explanatory materials and any regulations, rules and/or data codes made by the Minister or the National Data Commissioner. The framework will enable Australian Government agencies to share public sector data with particular entities for particular purposes, and under particular conditions.

4. The release of the DAT legislative package coincides with the Government's plans to expand myGov and the Digital Identity scheme and follows the commencement of the Consumer Data Right (CDR). These initiatives are intended to improve service delivery, increase competition between service providers, enable more evidence-based policy development and research, and provide individuals with greater choice and control over their personal information.

5. The OAIC recognises that data held by the Australian Government is a valuable national resource that can yield significant benefits for the Australian people when handled appropriately, and in the public interest.

6. Nonetheless, proposals to share data that contains personal information attract privacy risks, including loss of control by individuals and the mishandling of personal information. These risks are heightened in relation to Government-held personal information, as much of the personal information held by Government is 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.

7. Robust privacy safeguards are therefore central to the success of data sharing initiatives. The *Privacy Act 1988* (Cth) provides a well-established framework to minimise the privacy risks posed by data sharing activities. Successful data initiatives will build on the strengths of that framework to achieve the trust and confidence of the community, which is vital to the success of these projects. 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]

---

[1] 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.

Office of the Australian Information Commissioner 2019, Data Sharing and Release legislative reforms discussion paper — submission to Prime Minister and Cabinet, OAIC, Sydney.

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

8. The OAIC's 2020 Australian Community Attitudes to Privacy survey indicates that the Australian Government is generally more trusted than businesses with the protection of personal information, with 51% of respondents indicating that Australian Government agencies are trustworthy with personal information. The results also demonstrate the importance of maintaining that trust, showing that Australians are more likely to be comfortable (36%) with government agencies sharing information with other government agencies now, compared with 2017 (30%). Similarly, the proportion of people who are uncomfortable with this practice (40% in 2020) has decreased since 2017 (45%).

9. 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. 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.

10. The OAIC notes that the effectiveness of the privacy protections in the draft Bill will depend on their successful implementation by the National Data Commissioner and data scheme entities. Appropriate levels of resourcing will be necessary to ensure that the National Data Commissioner is supported to provide guidance on the operation of the scheme, implement a robust accreditation framework, and undertakes an appropriate level of oversight and assurance.

11. The OAIC supports the objects of the draft Bill, which include 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' (cl 3). To achieve these objectives, the privacy and security of data must continue to play a central role in both the legislative framework and the implementation of the DAT scheme.

Privacy protections in the draft Bill

12. 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 draft 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 scheme. Data scheme entities covered by the Privacy Act continue to have obligations under the APPs and in relation to the Notifiable Data Breaches (NDB) scheme. These include obligations relating 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 PIA for all high privacy risk projects.[3]

13. Given the ongoing application of a number of Privacy Act obligations to data custodians and many accredited entities that will collect, use and disclose personal information under the DAT scheme, it is vital that there is consistency between the privacy protections in the Privacy Act

[3] Under s 12(2) of the Privacy (Australian Government Agencies – Governance) APP Code 2017, a project may be a high privacy risk project if the agency reasonably considers that the project involves any new or changed ways of handling personal information that are likely to have a significant impact on the privacy of individuals.

and draft Bill to facilitate the compliance of entities operating under both frameworks. It is important to ensure that the amount of personal information shared under the DAT framework is minimised, and that there is transparency about the operation of the scheme.

14. The draft Bill includes privacy protective measures that are designed to address these issues and protect the personal information that is shared under 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 (cl 27).
- Outlining three permitted purposes for data sharing, as well as data sharing purposes that are precluded or excluded from the scheme, which will limit the use of data within the scheme (cl 15).
- 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 (cl 16(1)(b)).
- Requiring entities to outline how the public interest is served by the sharing in a data sharing agreement (cl 16(1)(c)).
- Requiring data custodians to only share data with accredited entities who have met standards for security and privacy of data (cl 13(1) and cl 74(2)(a)).

15. Given the potential richness of the datasets or other outputs that may be created under the DAT scheme, the OAIC considers it is appropriate that the draft Bill contain these specific privacy protective measures that apply in parallel to the Privacy Act requirements, to assist in restricting the scope of data sharing under the scheme.

Further privacy safeguards required

16. While the OAIC acknowledges the important privacy safeguards that have been included in the draft Bill, there are other key privacy protective measures that should be included to further mitigate the risks posed by sharing personal information and provide clarity about the privacy obligations of data scheme entities.

Sharing personal information – minimisation and transparency

17. The draft Bill adopts a 'data minimisation' approach, requiring data custodians to only share the data that is reasonably necessary to contribute to the data sharing purpose (cl13(1)(a)). The Explanatory Memorandum (EM) clarifies that this requirement applies 'to the total amount of data shared as well as the type of data involved'.

18. The OAIC strongly recommends that the data minimisation requirement is strengthened by including an explicit requirement in the draft Bill that data custodians must not share personal information where the data sharing purpose can reasonably be met without sharing personal information. Framed another way a requirement that data custodians must not share personal

information where the data sharing purpose can reasonably be met by sharing de-identified information, as defined in the Privacy Act.[4]

19. This is consistent with the OAIC's position throughout the development of the DAT framework that the data shared under the scheme should be de-identified where possible, to minimise the privacy impacts of the scheme for individuals.

20. Explicitly requiring data custodians to consider whether personal information is required for their data sharing project will necessitate a specific consideration of the risks involved in sharing this personal information, and an assessment of whether the benefits of the data sharing project outweigh these risks.

21. As an additional transparency and accountability requirement that supports the data minimisation approach, item 3 of the table at cl 18 of the draft Bill should be amended to explicitly require data sharing agreements to outline when personal information is being shared as part of a project.

22. The data minimisation requirements in the draft Bill should be reinforced with clear guidance and monitoring by the National Data Commissioner.

Exit mechanism

23. The draft Bill includes an 'exit mechanism', which will allow an output to exit the data sharing scheme in two circumstances (cl 20). Output is defined in cl 10 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 subsection 13(1)'.

24. Under cl 20(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.

25. The exit mechanism in cl 20 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 20(3)). 'Release' is defined in cl 9 of the draft Bill as 'provide open access'. This is distinct from 'sharing' data, which means providing controlled access to that data.

26. The EM notes that cl 20(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

[4] Section 6 of the Privacy Act says that 'personal information is ***de-identified*** if the information is no longer about an identifiable individual or an individual who is reasonably identifiable.'

mechanism is designed to facilitate release of outputs from the scheme, such as highly aggregated research outputs.

27. 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.

28. The proposed exit mechanism is a significant change to the framework that has previously been consulted. The ONDC's 2019 Data Sharing and Release Discussion Paper focused on data sharing to enable government agencies to 'share information with the right users for the right purpose', and noted that the National Data Commissioner would work with relevant entities to improve guidance on using existing mechanisms to release open data. Following consultation on this paper, the name of the framework was changed from Data Sharing and Release to Data Availability and Transparency, in recognition of the fact that data release was not envisaged under the framework.

29. The draft Bill sets up a framework that includes specific privacy protective measures, in recognition of the fact that there are risks involved in data sharing, and particularly in combining datasets to create an output that may form a richer picture of an individual than those datasets considered separately. A decision to remove these specific protections and restrictions in relation to such output should only be made if it is reasonably, necessary and proportionate to achieving a specific policy objective.

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 draft 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 20(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 draft 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 20(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.

32. In addition, there is a strong need for guidance to be provided to data scheme entities to explain what is permitted under the exit mechanism, where the authorisations under the DAT framework end and what protections apply once the outputs have exited the system. The OAIC would be pleased to work with the ONDC to develop guidance about how the Privacy Act obligations apply in relation to personal information that has exited the DAT scheme.

Ensuring clarity about data breach notification obligations

33. The draft Bill includes responsibilities for data scheme entities in the event of a data breach involving scheme data. 'Data breach' is defined in cl 34. This definition is modelled on the definition of 'data breach' under the Privacy Act, however terms have been changed to reflect the terminology used in the DAT scheme, for example 'unauthorised disclosure' has been changed to 'unauthorised release' in the draft Bill.

34. If a data scheme entity reasonably suspects or becomes aware that a data breach has occurred, the entity must take reasonable steps to mitigate the risk of harm resulting from the breach (cl 35). If the data breach involves non-personal data, the data scheme entity must notify the National Data Commissioner of the breach in certain circumstances (cl 37).

35. The OAIC's general position is that when a new data breach reporting scheme is created, to the extent possible, the tests and obligations on entities should align with the requirements of the NDB scheme under the Privacy Act. This will reduce regulatory fragmentation and increase certainty for regulated entities. There should only be a divergence in requirements if there is a critical policy reason for doing so.

36. The OAIC recommends that further information is included in the EM that specifically draws attention to the differences that exist between the data breach reporting schemes under the DAT legislation and the Privacy Act, particularly in relation to the differences in the definition of 'data breach' under both laws. This will ensure that data scheme entities have clarity in relation to their differing obligations under each.

37. If a data breach involves personal information that has been shared under the DAT scheme, the Notifiable Data Breach (NDB) scheme obligations under Part IIIC of the Privacy Act continue to apply. Under cl 36(1) of the draft Bill, default responsibility for notification under the NDB scheme rests with the data custodian, which will be an Australian Government agency and therefore have existing notification obligations under the Privacy Act. This provision recognises that some accredited entities will not be covered by the Commonwealth Privacy Act, and that State/Territory privacy laws do not currently have mandatory notification requirements.

38. The OAIC welcomes this approach to ensure that data custodians remain responsible for notifying breaches involving personal information, regardless of whether the breach was experienced by the data custodian or the accredited entity that the data was shared with.

39. In order to strengthen these requirements, the OAIC recommends that the draft Bill includes an explicit requirement that accredited entities must immediately notify the data custodian of any actual or suspected data breaches, unless the accredited entity is an APP entity, and the accredited entity and data custodian have agreed in their data sharing agreement that the accredited entity will remain responsible for notifying under Part IIIC of the Privacy Act (as permitted by cl 36(2)). This requirement could be inserted in cl 36, or as a mandatory term for data sharing agreements at cl 18.

40. Including this as an explicit requirement in the draft Bill would provide data scheme entities with clarity and certainty about their obligations in relation to data breaches, enabling them to take swift action in relation to suspected or actual breaches and notify in a timely and expeditious manner. The OAIC's experience regulating the NDB scheme indicates that prompt notification is essential to enable individuals to take action to mitigate the risk of harm in the event of a data breach involving their personal information. Prompt notification of a breach from an accredited entity to a data custodian would enable the data custodian to take steps to mitigate the breach and meet its notification obligations, if required.

Draft Accreditation Framework

41. In addition to the draft legislative package for the DAT scheme, the ONDC is seeking comments on the proposed accreditation framework.

42. Data custodians are only permitted to share data with entities that are accredited, and the draft Bill makes provision for rules to be developed to provide criteria for accreditation that cover governance and administrative frameworks, privacy and security of data, and technical skills and capabilities. The Accreditation Framework Discussion Paper notes that 'accreditation will ensure entities are identifiable and capable of handling data in accordance with the legislation's requirements.' The accreditation framework is another important assurance mechanism that is intended to facilitate safe data sharing.

43. The OAIC supports embedding further privacy safeguards in the system through the accreditation mechanism, and recognises the role that accreditation can play in ensuring that entities have appropriate processes, systems and procedures in place to support safe personal information handling practices. However, the effectiveness of an accreditation framework rests on the accreditation criteria being set at an appropriate level, rigor in accreditation processes, and effective regulation of the scheme.

Accreditation criteria

44. The OAIC is supportive of the proposal set out in the Discussion Paper to leverage the use of existing standards or processes to streamline the DAT accreditation framework. To that end, 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.

45. The accreditation criteria should be informed by the APPs and associated guidance from the OAIC, for example, the governance requirements in APP 1 and security requirements in APP 11. The important assurance mechanism that the accreditation framework provides could be undermined if the accreditation standards are less than the requirements of the APPs. This is particularly important in the context of the interaction between the accreditation framework and any regulatory action taken by the Australian Information Commissioner in relation to an accredited entity. The OAIC also notes that the PIA on the draft Bill specifically recommends that the accreditation requirements are aligned with APP 1 and that the ONDC gives regard to the OAIC's guidance on privacy governance and management. The OAIC is supportive of this recommendation.

46. There are a number of other privacy-related accreditation frameworks that should be leveraged to ensure standardisation of expectations across data initiatives. In particular, the CDR accreditation model and security requirements for CDR data recipients should be considered and applied in the DAT accreditation scheme where possible. In addition, Australia has committed to implementing APEC's Cross Border Privacy Rules system, which is an enforceable certification scheme to facilitate the flow of personal information across borders, and may provide a useful model for the privacy criteria in the DAT accreditation framework. The Government's review of the Privacy Act will also consider the desirability and feasibility of an independent certification scheme to monitor and demonstrate compliance with Australian privacy laws.

Accreditation process – assess, decide, maintain

47. The Discussion Paper sets out the steps in the accreditation process, which include the National Data Commissioner assessing the applicant's claims against the accreditation criteria and reviewing the supporting documents, deciding whether to grant or reject the application for accreditation, and monitoring and regulating the activities of accredited entities to ensure compliance with the requirements to maintain accreditation.

48. The Discussion Paper indicates that accreditation is an important assurance mechanism for the draft Bill, as it is the entry point for participation in the data sharing scheme and a safeguard to prevent participants from entering the data sharing scheme who have not been or should not be accredited.

49. It is therefore critical that the accreditation process is robust and a strong trust mark for the scheme. The Discussion Paper does not provide detail about how the National Data Commissioner will assure themselves that the accreditation criteria have been met, but the OAIC recommends that this process includes an interrogation of the claims made by the applicant and the quality of its supporting documentation. A light touch approach to accreditation risks undermining the level of assurance that the framework is designed to provide.

Regulation

50. The Discussion Paper notes that to regulate accreditation, the National Data Commissioner will maintain oversight of all accredited entities and can conduct assessments or initiate investigations about an accredited entity in response to a complaint or a suspected breach of the legislation or commence their own investigation. The National Data Commissioner will also have the power to suspend or cancel accreditation.

51. In determining when an accredited entity's accreditation should be suspended or cancelled, the ONDC should consider whether a finding that an accredited entity has interfered with the privacy of an individual under s 13 of the Privacy Act will impact on an entity's accreditation status. There is precedent for this approach in the Consumer Data Right (CDR) scheme, where a finding of a breach under the Privacy Act can impact a CDR participant's accreditation status.[5]

[5] The Data Recipient Accreditor may suspend or revoke a CDR participant's accreditation where satisfied that the participant (or an associated person of the participant) has been found to have contravened a law relevant to the management of CDR data, including the Privacy Act: Competition and Consumer (Consumer Data Right) Rules 2020, Rule 5.17.

The OAIC also considers that it is important that there is transparency about an entity's accreditation status, and as such, parties to a relevant data sharing agreement should be notified if an entity's accreditation is suspended or cancelled.

52. Finally, the OAIC supports the approach suggested in the Discussion Paper that accreditation may be suspended if there is *suspected* non-compliance. The OAIC suggests that the rules should include a positive obligation on the National Data Commissioner to take action in relation to an entity's accreditation once an issue is raised with the Commissioner.

Registers

53. The draft Bill specifies that the National Data Commissioner must maintain public registers of accredited entities, which contain the accredited entity's name and contact details.

54. The OAIC considers that it is important to ensure that relevant documentation provided by accredited entities to support their accreditation application is made available to data custodians on request, for example, details of the entities' privacy training programs, privacy policies and security arrangements (subject to necessary redactions). This will enable data custodians to make informed decisions about the most appropriate accredited entity to engage for their specific project, based on that entity's skills and experience with data, and their particular privacy risk profile.

55. The Discussion Paper notes that the National Data Commissioner will develop guidance on how data custodians can use accreditation when considering a data sharing request and/or agreement, which will provide a valuable support for data custodians in considering the above issues.