Australian Government
Attorney-General's Department

June 2025

Statutory Review of the *Data Availability and Transparency Act 2022*

Attorney-General's Department submission

Introduction

The Attorney-General's Department (the department) welcomes the opportunity to contribute to the Statutory Review of the *Data Availability and Transparency Act 2022* (DAT Act).

Of particular relevance to this review, the department has responsibility for the *Privacy Act 1988* (Privacy Act), which regulates how Australian Government agencies and certain private sector and not-for-profit organisations handle personal information. The department also supports administration of the *Criminal Code Act 1995* (Cth), including the general secrecy offences in Part 5.6. The department also works with First Nations peoples to develop policies and programs to improve justice outcomes and progress the priority reforms under the National Agreement on Closing the Gap.

While most of the data subject to sharing arrangements under the DAT Act would not be (or need to be) personal information, the impact of the DATA Scheme on privacy was a central issue when the DAT Bill was being considered by the Parliament in 2022. While the department is a Data Custodian and Accredited User under the DATA Scheme it has not, to date, received a request or otherwise had cause to use the DATA Scheme.[1]

This submission considers the objects of the DAT Act in promoting better availability of Government data balanced with other relevant considerations including privacy, provides an update on current work to update the Privacy Act to ensure it is fit-for-purpose for the digital age and highlights potential privacy reforms which may be relevant in the context of the DAT Act's objectives and operation.

[1] The department has instead used data-sharing mechanisms built into specific research projects the department has commissioned. Using project-specific data-sharing mechanisms was preferred because, for example: they allowed access to data in accordance with the ethics approval and purpose of the specific research project and data users were bound by licence agreements and usage agreements managed by the Australian Data Archive (ADA).

Balancing privacy with beneficial uses of personal information

The department recognises the importance of allowing personal data to be used in ways that benefit individuals, society and the economy. The digital economy results in large amounts of information about people being generated, used, disclosed and stored. This information may be used beneficially to deliver better government services, innovate new commercial services and modes of delivery, market goods and services, provide consumers access to content or services for free or at a lower cost, generate public interest research and facilitate communication. Access to data can also enable First Nations people to drive their own development. Through hundreds of written submissions and meetings over the course of the Privacy Act Review process, stakeholders have told the department that there are a number of purposes for which they share personal information. At the same time, it is clear that Australians expect their personal information to be protected and respected.

The Privacy Act is designed to balance the protection of the privacy of individuals with the interests of entities in carrying out their functions and activities, including activities which serve the public interest. The Australian Privacy Principles (APPs) in the Privacy Act outline standards and obligations in relation to the handling of individuals' personal information originally derived from the OECD's *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*.[2] The APPs apply to Commonwealth government agencies and organisations with an annual turnover of more than $3 million, and some other organisations such as health service providers.[3]

APP 3 permits an entity to collect personal and sensitive information where it is reasonably necessary for (or for agencies, directly related to) its functions or activities. Entities must obtain an individual's consent (or satisfy an exception) to collect their sensitive information including health information and information about certain attributes such as racial origin and political opinion. APP 6 permits an entity to use or disclose personal and sensitive information for the purpose(s) for which it was collected, or for a secondary purpose if an exception applies. Exceptions include: (i) where the individual would reasonably expect the information to be used or disclosed for a secondary purpose related to the primary purpose for collection, (ii) where an individual has consented to the secondary use or disclosure, or (iii) where the secondary use or disclosure is required or authorised by or under an Australian law or court/tribunal order.[4]

The Privacy Act currently includes exceptions for research, noting the public interest. Subsection 95(4) permits agencies to derogate from the APPs in the course of medical research. Organisations are permitted to collect, use and disclose health information without consent for research that is relevant to public health or public safety or for the compilation or analysis of statistics relevant to public health or public safety where it

---

[2] Organisation for Economic Co-operation and Development Council, *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD/LEGAL/0188, adopted on 23 September 1980 and amended on 11 July 2013 <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188>. The OECD Guidelines were developed in recognition of the common interest in promoting and protecting both privacy and the free flow of information among OECD member countries. See OECD, *Report on the Implementation of the OECD Privacy Guidelines* (OECD Digital Economy Papers No 361, November 2023) p 7 < https://www.oecd.org/en/publications/report-on-the-implementation-of-the-oecd-privacy-guidelines_cf87ae8f-en.html>.

[3] *Privacy Act 1988* (Cth), s 6.

[4] Ibid APPs 6.1 and 6.2.

is impracticable to obtain an individual's consent.[5] To rely on one of these exceptions, entities must adhere to guidelines issued by the CEO of the National Health and Medical Research Council and approved by the Information Commissioner.

In another instance of balancing public interest factors, Part VIA of the Privacy Act makes special provision for the collection, use and disclosure of personal information in emergencies and disasters. If certain conditions are met, the Prime Minister or the Attorney-General may make a declaration permitting personal information sharing which would otherwise not be consistent with the APPs. The conditions include that an emergency or disaster has occurred affecting Australian citizens or permanent residents, and that it is necessary for information to be shared to facilitate the Commonwealth's response to the emergency or disaster in a manner which would otherwise not be permitted under the Privacy Act and secrecy provisions in Commonwealth legislation. A similar provision permits sharing of personal information where needed to prevent further harm following a notifiable data breach under the Privacy Act.

The Productivity Commission's *Inquiry Report into Data Availability and Use (2017)* (DAU report), which led to the introduction of the DAT Act, identified that 'the primary legal impediment to more effective data use is typically *not* the Privacy Act but regulations and guidelines specific to the field in which the data is collected'.[6] The DAU report also found that individuals are likely to be more willing to allow data about themselves to be used by private and public organisations, provided they understand why and how the data is being used, can see tangible benefits, and have control over who the data is shared with.[7]

The department supports the objects of the DAT Act, which include enabling the sharing of public sector data consistently with the Privacy Act and appropriate security safeguards. Ensuring that appropriately calibrated privacy protections apply to the sharing of personal information held by Government agencies for purposes other than the purpose for which it was collected is essential to safeguard Australians' autonomy and manage risk of serious harms which may flow from misuse of, or unauthorised access to, the information. Such harms can include, for example, suffering worsened impacts of data breaches, profiling and excessive surveillance. Failure to do so will have broader impacts for trust in Government as a safe and responsible custodian of data.

Privacy reform

Following recommendations in the Australian Competition and Consumer Commission's 2019 Digital Platforms Inquiry Report, the department's comprehensive review of the Privacy Act was published in early 2023.[8] The Government published its Response to the Privacy Act Review report in September 2023.[9] The Response agreed or agreed in principle to 106 of the 116 proposals, recognising the need to strengthen

---

[5] Other conditions apply, including that the relevant research or compilation or analysis of statistics cannot be served by collection of de-identified information: *Privacy Act 1988* (Cth) s 16B(2)-(3).
[6] Productivity Commission, *Data Availability and Use* (Inquiry Report No 82, 31 March 2017) 121 < https://www.pc.gov.au/inquiries/completed/data-access/report>.
[7] Ibid 125.
[8] Attorney-General's Department, *Privacy Act Review Report 2022* (2023) <https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report>.
[9] Attorney-General's Department, *Government Response Privacy Act Review Report* (28 September 2023) < https://www.ag.gov.au/rights-and-protections/publications/government-response-privacy-act-review-report>.

privacy protections for Australians in the digital age while balancing this with the regulatory impacts on entities.

The *Privacy and Other Legislation Amendment Act 2024 (Cth)* (Amendment Act) passed the Parliament in November 2024, representing a first tranche of privacy reform. The Government has committed to progressing a second tranche of reform, with targeted consultation on draft provisions to occur over coming months. Further privacy reform provides the opportunity to establish a single uplifted standard of personal data protection applying to organisations and entities, reducing the need for separate, bespoke privacy regimes. The final content and details of any further legislative reform package will be a matter for Government.

Privacy reform is popular and expected. Deloitte's 2024 Privacy Index showed that consumers have little trust in the way any industry, including government, handles their personal information, with key drivers for this result including data security, privacy, data collection and transparency.[10] According to the Office of the Australian Information Commissioner's 2023 Australian Community Attitudes to Privacy Survey, 89% of Australians would like government agencies to do more to protect personal information, and would like the government to pass legislation that protects personal information.[11]

Potential privacy reforms relevant to the DATA Scheme context

A number of potential privacy reforms being considered by Government as part of implementing the Government Response to the Privacy Act Review report could support the objects of the DAT Act.

Research

As outlined above, the Privacy Act currently provides exceptions to requirements in the Act for certain types of research. The Government response to the Privacy Act Review report agreed to further consultation on combining and expanding the scope of these exceptions. If this reform proceeds, there is an opportunity to streamline the privacy protections which currently apply under the DAT Act for research which falls within an expanded research exception to the Privacy Act. For example, if research using biometric data comes within an expanded research exception to the Privacy Act, it may be appropriate to reconsider the application of subsection 16A(1) of the DAT Act, which currently requires an individual's express consent to share biometric data, to such research.

Definitions – including deidentification

Consultation during the Privacy Act Review indicated that a number of key definitions central to determining the Act's coverage are presently unclear, largely due to developments in the ways data is now being created and handled in the digital era. The Privacy Act Review report recommended these definitions be updated to ensure new ways of identifying individuals are covered by the protections in the Act. It also proposed that the

[10] Deloitte, *A Transparent Tomorrow Deloitte Australia Privacy Index 2024* (10th edition, 21 November 2024) 8 < https://www.deloitte.com/au/en/services/risk-advisory/analysis/deloitte-australian-privacy-index.html>.
[11] Office of the Australian Information Commissioner, *Australian Community Attitudes to Privacy Survey August 2023* (8 August 2023) 42 <https://www.oaic.gov.au/engage-with-us/research-and-training-resources/research/australian-community-attitudes-to-privacy-survey/australian-community-attitudes-to-privacy-survey-2023>.

definition of 'de-identified' be updated to make it clear that personal information is de-identified where a process is applied to it such that it does not relate to an individual who is identified or reasonably identifiable in the current context (i.e. it is not absolute).

These reforms, along with updated guidance from the privacy regulator, the OAIC, could support the ability of Accredited Data Service Providers performing data de-identification services to make personal information held by Government agencies able to be utilised for the data sharing purposes under the DAT Act on a de-identified basis.

High-risk practices

Facial biometric data raises particular privacy risks due to its use to identify individuals and infer sensitive information, such as race, demographic and health information, raising risks of misidentification, inaccuracy, bias and discrimination. The department is considering how the privacy reforms could address the specific risks of facial recognition technology and other uses of biometric information without compromising its technology-neutral approach. The results of this process could impact whether the general privacy protection for biometric data under the DAT Act continues to align with best practice.[12]

Strengthening responses to data breaches

With their increasing scale and prevalence, the Australian community expects better responses to data breaches. The Government Response agreed to a number of proposals to better facilitate reporting processes under the Notifiable Data Breaches (NDB) Scheme. These include an obligation to notify the OAIC within 72 hours and requiring entities to take steps to mitigate harm to affected individuals. Noting the DAT Act preserves the Information Commissioner's oversight of data breaches involving personal information through the NDB Scheme, these reforms would have a flow-on effect for data custodians and accredited entities under the DATA Scheme and would also contribute to whole-of-government efforts to enhance cyber security and identity protection.[13]

Privacy safeguards proportionate to risk

As noted above, personal and sensitive information which is collected for a primary purpose may be used or disclosed for a secondary purpose which is related (or directly related, for sensitive information) to the primary purpose for collection and which an individual would reasonably expect. In all other cases, use or disclosure for a secondary purpose must be with the consent of the individual or for an authorised secondary purpose under the Privacy Act (for example, law enforcement purposes) or as authorised by or under another law (for example, health and safety laws). Authorised secondary purposes are purposes recognised as serving the public interest. Disclosure of personal information by a government agency for a project under the DAT Act is an authorised secondary purpose disclosure.

As part of its work towards a further tranche of privacy reform, the department is considering feedback on the scope of various authorised secondary purposes contained in the Privacy Act. If this Statutory Review

[12] *Data Availability and Transparency Act 2022* (Cth) s 16A(1).
[13] Ibid s 37.

finds that consideration should be given to the calibration of the current privacy protections in Part 2.4 of the DAT Act to ensure their application to a project is proportionate to risk to enhance the scheme's effectiveness, the department would be happy to engage further on how this might be achieved.

Conclusion

The proliferation of data in the digital economy has created significant benefits and opportunities, including benefits that extend to individuals and the public at large. However, it also exposes individuals and entities to significant risks, including through data breaches. The department recognises the importance of the DAT Act as an effective mechanism for enabling access to public sector data for projects that serve the public interest, whilst also safeguarding people's privacy.

Uplifting the Privacy Act is crucial to achieving the productivity benefits associated with data sharing, and more broadly to protect trust in Government. The department is keen to participate in a constructive conversation to strike the right balance between giving individuals transparency, and appropriate choice and control over how their personal information is used, while ensuring that the benefits of data to support productivity and innovation are realised.

The department considers the DATA Scheme has meritorious objectives and should continue, potentially with modifications, and looks forward to contributing to the discussion on opportunities to achieve the DAT Act's objectives.