information and privacy commission new south wales

STATUTORY REVIEW OF THE DATA AVAILABILITY AND TRANSPARENCY ACT (2022)

Submission by the Information and Privacy Commission NSW

11 June 2025

Sonia Minutillo
Privacy Commissioner

The Commissioner's signature has not been included in this submission to facilitate public access to the submission, manage security risks and promote availability in accordance with the *Redacting signatures on public facing documents Practice Guide* published on the IPC website.

The Information and Privacy Commission NSW (IPC) welcomes the opportunity to provide a submission to the Statutory Review of the *Data Availability and Transparency Act 2022* (Cth).

About the IPC

The Information and Privacy Commission NSW (IPC) oversees the operation of privacy and information access laws in New South Wales.

The Privacy Commissioner has responsibility for overseeing and advising NSW public sector agencies on compliance with the *Privacy and Personal Information Protection Act 1998 (*NSW*)*(PPIP Act) and the *Health Records and Information Privacy Act* 2002 (NSW) (HRIP Act). The PPIP and HRIP acts establish the Information Protection Principles and the Health Privacy Principles which govern the collection, use and disclosure of personal and health information by NSW Government agencies.

The Information Commissioner has responsibility for overseeing the information access rights enshrined in the *Government Information (Public Access) Act 2009* (NSW) (GIPA Act) and exercises functions under the *Government Information (Information Commissioner) Act* 2009 (NSW) (GIIC Act). The Information Commissioner also holds the role of NSW Open Data Advocate, in which capacity she provides advice across the NSW Government on nonpersonal data that should be released to the public.

Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000 • GPO Box 7011, Sydney NSW 2001
T 1800 ipc nsw (1800 472 679) • **E** ipcinfo@ipc.nsw.gov.au • **W** www.ipc.nsw.gov.au

Submission

Governments increasingly produce and hold significant quantities of data, much of which involves personal, health and sensitive information. This data is often viewed for its potential as a resource that can be drawn upon for analysis to target programs, and for improved service delivery. Government data is both a strategic and valuable asset for researchers and commercial entities.

The Privacy Commissioner welcomes the opportunity to make this submission in response to some of the issues raised in the Statutory Review of the *Data Availability and Transparency Act 2022* – Issues Paper (the Issues Paper).

Law Enforcement Purposes

One of the principal themes of the Issues Paper is the consideration of several potentially substantial expansions of the DATA Scheme, including by:

- extending the scheme to allow for data sharing for purposes that have previously been excluded, including enforcement and compliance-related purposes (Issue Paper p. 12)
- expanding the scheme to include private and non-government entities (Issue Paper p. 12).

In its current form the DAT Act precludes data sharing for any enforcement related purposes, which includes for the purposes of detection, investigation and response to offences, the contravention of laws punishable by pecuniary penalties, and acts or practices detrimental to the public revenue. The use of data to identify individuals for compliance review or compliance activity is also an enforcement related purpose.

The IPC notes that prior consultation on the Bill in 2020 raised numerous concerns from stakeholders consistently expressing the view that data sharing should not be used for the purposes of compliance or assurance processes.

Extending the application of the DAT Act for precluded purposes of compliance or assurance processes would appear to be at odds with the intended objectives and represents a significant deviation from the original scope of the DAT Act. From a privacy perspective and to ensure procedural fairness, data sharing related to law enforcement and national security are best governed and managed under specific legislation that provides tailored protections and redress mechanisms to ensure procedural fairness. Extended use for law enforcement related purposes, such as for identification of individuals, raises significant privacy concerns. Any departure should be subject to broader public consultation, including a further privacy impact assessment.

Application to additional entities

The DAT Act includes several elements, which contribute to privacy protections. These include purpose limitation, data minimisation, accredited users, data sharing agreements and

Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000 • GPO Box 7011, Sydney NSW 2001
T 1800 ipc nsw (1800 472 679) • **E** ipcinfo@ipc.nsw.gov.au • **W** www.ipc.nsw.gov.au

restrictions to ‘on sharing”. The current framework for data sharing between known and trusted parties assists in lessening privacy risks.

Wider and broader release can lead to risks, which may be difficult to mitigate, such as on sharing or commercialisation. It may also be difficult to align the direct use of data for the public benefit and the three purposes provided for in the DAT Act. Adequacy of privacy policies and practices, data management governance and the adequacy of systems for protection of the data from unauthorised use, access or loss will need to be addressed.

Application to additional entities requires careful consideration be given to ensuring that the sharing objectives provide tangible value. Additionally, privacy risks, such as the possibility of re-identification of personal information, requires careful evaluation. The increasing use of emerging technologies, such as artificial intelligence, requires specific consideration.

Data Sharing principles in the DAT Act

The IPC considers the inclusion of data sharing principles in the DAT Act as important and necessary for framing and achieving the objects of the DAT Act. These principles are modelled on the “Five Safes” framework and provide a risk-based approach to making decisions about data sharing decisions. The inclusion of the principles provides assurance, confidence and trust for when and how data sharing can or will occur. The adoption of principles in the DAT Act is also consistent with the approach to privacy law, which is principles-based.

Inclusion of the data sharing principles strengthens the privacy settings underpinning the scheme. Removal of the principles may lead to unintended consequences that undermine the privacy protections and the public interest, both of which are central to the framework.

Culture of data sharing

Data sharing under the Scheme is currently limited to three potential purposes: delivery of government services, informing government policy or programs, or research and development. Whether those limited purposes remain or are expanded, each instance of data sharing under the Scheme should be accompanied by a considered justification of the need for the requested data and whether they are appropriate in the specific circumstances at issue. Careful consideration should be given to establishing an appropriate process to ensure that data sharing only occurs when it is aligned with clearly defined objectives and that the sharing is necessary to fulfill those objectives.

Thank you for your consideration of this submission.

For further information about the IPC visit www.ipc.nsw.gov.au.

Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000 • GPO Box 7011, Sydney NSW 2001
T 1800 ipc nsw (1800 472 679) • **E** ipcinfo@ipc.nsw.gov.au • **W** www.ipc.nsw.gov.au