information and privacy commission
new south wales

Enquiries: [redacted]
Telephone: [redacted]
Our reference: IPC21/A000090

25 March 2021

Office of the Secretary
Department of Customer Service
McKell Building, [redacted]
2-24 Rawson Place
Sydney NSW 2000

By email: data.sharing@customerservice.nsw.gov.au

Dear Sir/Madam

REVIEW OF THE *DATA SHARING (GOVERNMENT SECTOR) ACT 2015*

Thank you for the opportunity to make a submission to the review of the *Data Sharing (Government Sector) Act 2015* (Data Sharing Act). This submission provides general commentary and specific responses to the consultation questions published by the Department of Customer Service.

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* (PPIP Act) and the *Health Records and Information Privacy Act 2002* (HRIP Act).

The Information Commissioner has responsibility for overseeing the information access rights enshrined in the *Government Information (Public Access) Act 2009* (GIPA Act). These rights are realised by agencies authorising and encouraging proactive public release of government information; and by giving members of the public an enforceable right to access government information. The Information Commissioner also holds the role of NSW Open Data Advocate, in which capacity she provides advice across the NSW Government on non-personal data that should be released to the public.

While the IPC does not share data in the way that is envisaged by the Data Sharing Act, data sharing by government agencies has the potential to significantly impact both citizens' access to information and their privacy rights. Should the review of the Data Sharing Act lead to any substantial amendments, including any expansion of the scope of data sharing to include non-government entities, it is vital that the provisions of the Act continue to preserve extant rights, accountability and the principles of open government.

Privacy

Data sharing and privacy safeguards

Section 3(a) of the Data Sharing Act includes, as one of the Act's objects:

> "to promote, in a manner that recognises the protection of privacy as an integral component, the management and use of government sector data as a public resource that supports good Government policy making, program management and service planning and delivery".

Any sharing that occurs under the Data Sharing Act must be done in accordance with the PPIP Act, HRIP Act and any applicable Public Interest Direction or Privacy Code of Practice made under the privacy legislation (section 12).

A public sector agency can only share (disclose) personal information if one of the following exceptions under section 18 of the PPIP Act (or another exemption under the Act) applies:

- the disclosure is directly related to the purpose for which the information was originally collected and the agency has no reason to believe the individual whose information is to be shared would object to it being shared
- the individual is likely to be aware or has been made aware that information of that kind is usually shared
- the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual or another person.

It is important that the Data Sharing Act continues to include privacy safeguards that require agencies to comply with privacy legislation and, in particular, to consider the risk of re-identification when sharing and linking data.

Agencies may share de-identified data without breaching privacy laws. De-identification means that a person's identity is no longer apparent or cannot be reasonably ascertained from the information or data. Where multiple datasets are brought together, however, there is a heightened risk of re-identification. Circumstances where there is a risk of re-identification can include where:

- coded information will remain potentially re-identifiable to a person or body with the means to link the code back to other identifying details
- flaws or a weakness in the technique used to encrypt information in the dataset allows the encryption to be reversed
- highly detailed information in the dataset creates a significant risk that some individuals may be identified by linking with other sources
- unique or rare characteristics of the individual, or a combination of unique or remarkable characteristics, can enable identification
- machine identification is possible, despite the personal information being redacted and not able to be read by a human eye.

There can be significant value to government in using and sharing de-identified data to monitor events and to inform government decisions. A notable example of this has been the NSW Government's COVID-19 Data Program. The program, which the Privacy Commissioner was consulted on, was established to provide data and insights to improve coordination of the NSW Government's COVID-19 response and drew on data from across NSW, the Commonwealth and the private sector. COVID-19 data is published on Data.NSW as open data.

However, as the risk of re-identification can significantly increase when several de-identified datasets are brought together, a range of mitigation strategies and privacy safeguards have had to be adopted to reduce this risk, including limiting access to data to authorised individuals, maintaining audit logs of user access to the data and screening data for re-identification risk before publication.

The risks of re-identification of supposedly de-identified data were highlighted in the report of the investigation by the Office of the Victorian Information Commissioner (OVIC) into the disclosure of Myki travel information by the Victorian Department of Transport in 2018.[1]

Sharing personal data in emergencies

There is a strong public interest in allowing government agencies to share personal data in emergency situations. In the context of the COVID-19 pandemic, successive public health orders issued by the Minister for Health have authorised government sector agencies to exchange personal or health information with other government sector agencies, if considered necessary for the purposes of protecting the health or welfare of members of the public during the COVID-19 pandemic. This sharing of personal information would not have otherwise been authorised under the PPIP or HRIP Acts.

By contrast, the Commonwealth *Privacy Act 1998* does include special privacy provisions in Part VIA, which take effect if the Prime Minister or the Minister responsible for the Privacy Act declares an emergency or disaster. When a declaration is in force, Part VIA allows for and regulates the collection, use and disclosure of personal information between Australian Government agencies and State and Territory authorities, private sector organisations, non-government organisations and others for broad permitted purposes, including:

- identifying those who are, or may be, injured, missing or dead, or involved in the emergency or disaster
- helping individuals to access services including repatriation, medical or other treatment, health services and financial or other humanitarian assistance
- helping law enforcement with the emergency or disaster
- coordinating or managing the emergency or disaster
- ensuring that people who are responsible for individuals are kept appropriately informed about those individuals and the emergency response to those individuals.[2]

Data sharing and privacy: models in other jurisdictions

Victoria

The *Victorian Data Sharing Act 2017* authorises the use and disclosure of identifiable data for the purpose of data integration, enabling the sharing of such data between public sector bodies and the Chief Data Officer. Under the Victorian Act, data must only be handled for the purpose of informing government policy making, service planning and design. Sections 18 and 19 of the Act also set out restrictions on the use of identifiable data, requiring reasonable steps to be taken to mitigate the risk of re-identification.

[1] https://ovic.vic.gov.au/wp-content/uploads/2019/08/Report-of-investigation_disclosure-of-myki-travel-information.pdf
[2] *Privacy Act 1998* (Cth), section 80H

Commonwealth

In 2020, the Data Availability and Transparency Bill 2020 was introduced to the Australian Parliament, to establish a framework for sharing public sector data. Section 16 of the Bill sets out data sharing principles. These are modelled on the "Five Safes" framework and provide a risk-based approach to making decisions about data sharing. Each principle established under section 16 provides non-exhaustive illustrative examples of matters that should be considered when deciding to share data.

United Kingdom

In the United Kingdom, the UK General Data Protection Regulation (GDPR) and the *Data Protection Act 2018* do not apply to anonymised data. Anonymous information is defined as information which does not relate to an identified or identifiable natural person or to personal data "rendered anonymous in such a manner that the data subject is not or no longer identifiable" (Recital 26, UK GDPR). Anonymised data can therefore be processed for statistical or research purposes. However, data protection laws continue to apply to personal data that has been pseudonymised; that is, data which could be attributed to a natural person by the use of additional information. The UK Information Commissioner's Office has published extensive guidance on the difference between anonymisation and pseudonymisation, which may also be useful in the NSW context as it sets out factors that will be relevant to consider in the context of sharing and linking data from different sources.[3]

Sharing personal data outside of the NSW Government

Any proposal to allow for the sharing of personal data by NSW Government agencies with non-government organisations and other jurisdictions would require appropriate privacy governance arrangements, to ensure that citizens' personal information will continue to be handled securely and in accordance with privacy laws. Currently, sections 12 and 14 of the Data Sharing Act provide important privacy safeguards and data custody and control safeguards with oversight by the Privacy Commissioner and the Information Commissioner. If personal information were to be shared outside of the NSW Government, sections 12 and 14 would need to be amended to clarify the obligations of non-government entities in relation to NSW privacy legislation.

Information access

The Data Sharing Act and the GIPA Act

The Data Sharing Act can operate to enhance the object of the GIPA Act, which is to open government information to the public and in doing so, maintain and advance a system of responsible and effective representative democratic government that is open, accountable, fair and effective. This object is to be realised by agencies authorising and encouraging proactive public release of government information (section 3(1)(a)); and by giving members of the public an enforceable right to access to government information (section 3(1)(b)). Subsection (1)(c) under section 3 of the GIPA Act provides that access to government information is restricted only when there is an overriding public interest against disclosure.

As Open Data Advocate, the Information Commissioner encourages the proactive public release of government information by agencies in ways that are respectful of data sharing safeguards, as well as providing information, advice and assistance to agencies and members of the public on access to government information.

Section 23 of the GIPA Act may have particular application to government policies relevant to the management and exchange of data. Section 23 provides:

[3] See https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/#pd4

An agency's policy documents are such of the following documents as are used by the agency in connection with the exercise of those functions of the agency that affect or are likely to affect rights, privileges or other benefits, or obligations, penalties or other detriments, to which members of the public are or may become entitled, eligible, liable or subject (but does not include a legislative instrument)—

(a) a document containing interpretations, rules, guidelines, statements of policy, practices or precedents,

(b) a document containing particulars of any administrative scheme,

(c) a document containing a statement of the manner, or intended manner, of administration of any legislative instrument or administrative scheme,

(d) a document describing the procedures to be followed in investigating any contravention or possible contravention of any legislative instrument or administrative scheme,

(e) any other document of a similar kind.

Public awareness and public trust will be enhanced by transparency of government policies that impact citizens who share their information with government. Government data holdings will exponentially increase, and visibility of those data holdings will ensure that government has appropriate governance structures to support sound management of this significant government asset.

Section 20 of the GIPA Act places a positive obligation upon agencies to publicly report this significant asset:

20 Agencies must have agency information guide

*(1) An agency (other than a Minister) must have a guide (its **agency information guide**) that—*

(a) describes the structure and functions of the agency, and

(b) describes the ways in which the functions (including, in particular, the decision-making functions) of the agency affect members of the public, and

(c) specifies any arrangements that exist to enable members of the public to participate in the formulation of the agency's policy and the exercise of the agency's functions, and

(d) identifies the various kinds of government information held by the agency, and

(e) identifies the kinds of government information held by the agency that the agency makes (or will make) publicly available, and

(f) specifies the manner in which the agency makes (or will make) government information publicly available, and

(g) identifies the kinds of information that are (or will be) made publicly available free of charge and those kinds for which a charge is (or will be) imposed.

Any review of the Data Sharing Act should be informed by the operation of other relevant statutes including the GIPA Act and the *State Records Act 1998*. Likewise, consideration is required in respect of the definitions and the exceptions provided under the Data Sharing Act to extant legislation, particularly rights-based legislation, to ensure that the Data Sharing Act is fit for purpose. Factors including:

- the uses of data e.g. to inform decision making, service delivery, research
- distinctions between data and statistical information
- the primacy of other statutes
- jurisdictional remit
- application to information held by third parties

should all be examined.

Data sharing outside of the NSW Government

The sharing of government information outside of NSW and with non-government entities has the potential to create uncertainty around who holds information and how access will be provided to citizens. Information is held by an agency when it is:

- information contained in record held by an agency
- information contained in a record held by a private sector entity to which the agency has an immediate right of access
- information contained in a record in the possession or custody of the State Archives and Records Authority to which the agency has an immediate right of access
- information contained in a record that is in the possession or under the control of a person in his or her capacity as an officer or member of staff of an agency.

Under the GIPA Act an agency must have an agency information guide which identifies the various kinds of information held by the agency (section 20(1)(d)). The guide must be made publicly available, together with an agency's policy documents (sections 6, 18(a) and 18(c)). What constitutes an agency's policy documents is set out in section 23 of the GIPA Act (see above).

Government information held by third parties

The Information Commissioner expects agencies to have regard to the application of section 121 of the GIPA Act when entering into contracts with private sector persons to ensure that certain information held by contractors is designated as government information and subject to the GIPA Act.

Section 121 of the GIPA Act applies in circumstances where an agency enters into a contract with a private sector entity to provide services to the public on behalf of the agency. Subject to certain exceptions, section 121 requires government agencies to ensure that their contracts provide them with an immediate right of access to information:

- relating directly to the performance of services by the contractor
- that is collected by the contractor from members of the public to whom it provides, or offers to provide, the services, and

- that is received by the contractor from the agency to enable the contractor to provide the services. Section 121 mandates the inclusion of a clause to permit access to information held by the contractor.

Despite the mandatory requirements of section 121, where there are no contractual arrangements in place and no immediate right of access to information, information in the possession of a contractor may not be government information held by an agency for the purposes of the GIPA Act.

If the scope of the Data Sharing Act were to expand to include data sharing with non-government entities, section 14 of the Act would need to be amended, to clarify the obligations of non-government entities in relation to the GIPA Act. This approach would ensure that rights are not diminished in circumstances of government outsourcing/partnership arrangements to deliver government services and, importantly, inform government decision making.

We hope that these comments are of assistance to you. Please do not hesitate to contact us if you have any questions. Alternatively, your officers may contact [redacted], Senior Project Officer, on [redacted] or by email at [redacted].

Yours sincerely

[redacted]

Elizabeth Tydd
CEO, Information and Privacy Commission NSW
Information Commissioner
NSW Open Data Advocate

[redacted]

Samantha Gavel
Privacy Commissioner