Review of the Data Sharing (Government Sector) Act 2015

Department of Customer Service

August 2021

Review of the Data Sharing Act 2015

Table of Contents

1. Executive Summary

The *Data Sharing (Government Sector) Act 2015* (the **Act**) enables data sharing between NSW government sector agencies, including the NSW Data Analytics Centre (**DAC**). It aims to remove barriers that impede the sharing of data between agencies and to expedite data sharing to support evidence-driven policy and program management, service planning and delivery. The Act also maintains privacy protections under existing NSW privacy legislation.

The Minister for Customer Service and Minister for Digital (the **Minister**) administers the Act, which commenced in November 2015. Section 20 of the Act requires that the Act be reviewed five years after the date of assent to determine whether its policy objectives remain valid and whether the terms of the Act remain appropriate for securing those objectives.

This review has been conducted by the Department of Customer Service (the **Department**) on behalf of the Minister. Consultation was held from February to March 2021, including a total of 31 stakeholder interviews, 81 responses to online surveys and five written submissions. All submissions were considered as part of the statutory review.

The review found that the Act's policy objectives remain valid. Data sharing and analysis is more important than ever across all endeavours of life, and governments are becoming more adept at using data insights to inform and shape better policy, programs and services. Linked datasets and the data insights derived from them are increasingly viewed as critical government assets and digital infrastructure. The power of sharing and analysing datasets within government to deliver better social outcomes for citizens has been demonstrated through a number initiatives since the Act commenced:

- The Human Services Data Set has been established as an enduring de-identified linked dataset to improve the long-term outcomes for vulnerable populations.
- Compulsory Third-Party insurance reform involved data sharing between key agencies. Data insights revealed $10 million worth of fraud, resulting in numerous prosecutions and the cost of green slips was reduced by nearly $200 for customers.
- The Active Kids program used data insights gathered from analysing data around voucher uptake across NSW to adjust service delivery to encourage increased participation in sport by children and young people.
- The NSW Government's data-driven response to COVID-19 forged strong collaboration across clusters, supported by a centrally coordinated data program that resulted in unprecedented levels of data sharing across NSW Government as well as with the Commonwealth Government and other jurisdictions. The development of the COVID-19 Dashboard Portal brought insights together for key decision makers, enabling the NSW Government to respond effectively and efficiently to the pandemic. Using government data, the DAC also developed and published heatmaps to keep the community safe and informed throughout the pandemic.

The current data sharing context has matured in the last five years since the development of the Act, and so too has the demand for data and the need for data sharing within NSW to develop evidence based policy and effective and tailored services for NSW citizens.

Overall, this Review has found that there is general support for Act's role facilitating whole of government data sharing and that its objectives remain valid. However, further clarification about the Act and updates to how it operates are needed to fully deliver on the Act's underling policy objectives, address stakeholder needs and enhance data sharing capabilities across the sector.

Several stakeholders highlighted operational challenges which they felt have been barriers to the timely and effective sharing of data under the Act, especially where data analysis and insights have required individual determinations under NSW privacy legislation. This has at times frustrated objective 3(c) of the Act - to facilitate the expeditious sharing of government sector data with the DAC or between other government sector agencies. The Review found a complex interdependency between the Act and the NSW privacy legislation, with opportunities to streamline how the Act intersects with privacy legislation needed as part of a pragmatic and balanced data protection regime.

The Act and supporting materials, such as policy guidelines and data safeguards could be strengthened and updated with more detail on how to share data safely, which will give greater confidence in the data sharing process so the Act can be applied more effectively. The implementation of data safeguards that protect privacy and security should support attainment of emerging benefits such as from linked data assets that provide deeper insights and value to policy makers and program and service designers which inform the delivery of better outcomes for the community.

The report makes 14 recommendations to update and improve the Act and privacy legislation to better support the data sharing needs of agencies and encourage more effective policy and program design. Several of the recommendations are interrelated.

The Review recommendations are outcomes focused. Apart from Recommendations 1-3, the recommendations identify the issues that need to be solved rather than how we should go about solving them. Considerable work will need to be undertaken in consultation with the Privacy Commissioner to develop the detail as to how the recommendations will be implemented. This may require amendments to the Act and/or privacy legislation in order to support the Act achieving its objectives.

This Review has consolidated the views of all NSW Government clusters, public submissions and reflects the data sharing learnings of other Australian jurisdictions. The NSW Information and Privacy Commission (IPC) was consulted as part of this review.

2. Recommendations

Recommendation 1: Support on-sharing of data insights

a. Amend section 9 of the Act to enable de-identified data insights to be on-shared by the agency that performs the analytics function, on the condition that the agency or agencies that provided the source data have been consulted on the decision to share and:
   - had the opportunity to verify the accuracy of the data insights,
   - have visibility over the current and future use of the data insights, and
   - have access to the data insights.

b. Agencies should support sharing the data insights unless there is an overriding public interest against the data being shared.

This recommendation will promote data sharing collaboration across agencies while minimising the risk of misuse and misinterpretation. This recommendation should be read in conjunction with the recommendation relating to risk-based privacy assurance (recommendation 4) which intends to build data custodian's confidence that appropriate, risk-based safeguards are in place.

Recommendation 2: Strengthen existing cross-jurisdictional data sharing

a. Amend the Act to specifically recognise data sharing with the Commonwealth Government and other state and territory governments is lawful and possible under the Act.
b. Clarify the scope and risk management process for cross-jurisdictional data sharing via policy and//or other supporting mechanisms, in line with the proposed Intergovernmental Agreement on Data Sharing and NSW privacy legislation. This could involve a risk management framework to agree how data sharing across jurisdictions will take place in a safe way that still supports constructive data sharing practices but doesn't compromise privacy protections or gives rise to other risks.

This recommendation will support current work underway to combine data across Australian jurisdictions to shape whole of government policy making and service delivery to improve the end-to-end customer experience.

Recommendation 3: Address data sharing needs in emergencies in NSW privacy legislation

As per the Public Health (COVID-19 Gathering Restrictions) Order 2021 (Health, 2021) which enabled the exchange of data under the Public Health Act, neither the Data Sharing Act nor the NSW privacy legislation explicitly enable the expedited sharing of personal information during emergencies, natural disasters and hazards to alert and protect citizens at risk. Based on advice from the Privacy Commissioner as to where the legislative change should occur, it is recommended that provisions be included in NSW privacy legislation to enable the sharing of personal information in response to emergencies, natural or other disasters and hazards as defined in the *State Emergency and Rescue Management Act 1989*. This is consistent with the Commonwealth Government's approach in Part VIA of the *Commonwealth Privacy Act 1998.*

This recommendation will enable the NSW Government to respond effectively, and efficiently during emergencies to better alert and protect citizens at risk.

Recommendation 4: streamline the approach for approval of de-identified linked datasets to be used within government

Consult with the Privacy Commissioner to develop a standardised framework for streamlined, timely, risk-based privacy assurance to guide the creation of de-identified linked datasets and insights for use within government, including drawing upon models in other jurisdictions such as that in Victoria. This framework should reference the technical tools and capabilities available within government to effectively manage information security and protect privacy and create a high trust environment for record linkage and data sharing.

This recommendation should improve the efficiency and effectiveness of creating de-identified linked datasets in line with robust privacy protection. It will also support greater use of data sharing by building data custodian's confidence that appropriate, risk-based safeguards are in place.

Recommendation 5: Clarify data sharing precedence to increase data sharing

a. Clarify, that with the exception of exclusions set out in Section 5(2) of the Act (i.e. NSW privacy legislation, GIPA and State Records Act), the Act permits a government sector agency to share data with the DAC or another government sector agency for the

purposes set out in the Act in cases where the sharing of the data is constrained by a provision in other NSW legislation.

b. Develop documentation to clarify existing exclusions to this provision (i.e. NSW privacy legislation, GIPA and State Records Act).

This recommendation will clarify the position of the Act relative to existing legislation and promote the use of the Act to its full potential.

Recommendation 6: Improve the efficiency of data sharing

Support the introduction of a standard data sharing agreement between agencies to agree standard terms and conditions upfront to increase efficiency in data sharing.

This recommendation will address the ad-hoc nature of data sharing agreements by reducing duplication of effort, costs and delays in drafting such agreements.

Recommendation 7: Clarify data sharing functions across NSW Government

Clarify that the key functions that relate to data sharing described in the Act apply to any NSW Government agency that has the relevant capability to perform that function.

This recommendation will facilitate the Act being used to its full potential and by agencies other than just the DAC.

Recommendation 8: Clarify DAC's role and authority

Clarify that while DAC is the central body for data and analytics services across NSW Government, it is not intended that terms of the Act restrict DAC to activities explicitly outlined in the Act. DAC can undertake activities that any government agency is ordinarily allowed to undertake.

This recommendation will clarify the DAC's role and scope of activities.

Recommendation 9: Create centralised linked data sets

Implement centralised linked data sets and develop a library of high value data sets across NSW Government. Apply risk-based data sharing safeguards, as appropriate, in alignment with Recommendation 4. This will facilitate efficient and timely data sharing across Government which can reduce duplication of efforts, coordinated by the DAC as the central body for data sharing.

This recommendation will facilitate efficient and timely data sharing across Government which can reduce duplication of efforts, coordinated by the DAC as the central body for data sharing.

Recommendation 10: Clarify the scope of data sharing

Clarify data sharing under the Act enables private sector data (where provided to NSW Government agencies) to be shared within NSW Government as required. This should be considered in line with contractual or equitable obligations of confidentiality or commercial-in-confidence, as well as the Act's other qualifications on an agency's ability to share data.

This recommendation will enable greater access to private sector data to inform policy, planning and delivery, where appropriate and in line with relevant data protections.

Recommendation 11: Clarify definitions in the Act

Clarify the Act's definitions with reference to industry best practice definitions and/or definitions used in data sharing guidance provided by the Office of the National Data Commissioner.

This recommendation will clarify the interpretation of the Act by aligning it to Commonwealth standards, noting definitions outlined in NSW privacy legislation and the GIPA Act.

Recommendation 12: Support consistent interpretation and greater usability of the Act

a. Clarify the intention of the Act's provisions to support consistent interpretation and greater usability of the Act.

b. Update existing supporting materials for the Act to provide greater clarity around how to implement the Act.

The intended outcome of this recommendation is to clarify the interpretation of the Act to build sector confidence in using the act to its full potential.

Recommendation 13: Support efficient data verification

Clarify that any agency that provides data in accordance with a Ministerial direction will work with the DAC (or any other NSW Government agency performing the function) so that data is interpreted correctly and data insights are verified efficiently.

The intended outcome of this recommendation is to support accurate and efficient data sharing.

Recommendation 14: Promote greater, more timely and more efficient data sharing through the use of the Act

Better promote the Act and its supporting frameworks to enable greater use.

This recommendation will increase awareness of the Act and uplift the confidence and capability of the sector to share data insights.

3. Introduction

3.1 Background on the Act

The Act was introduced in 2015 in recognition of the need to improve data sharing between NSW Government agencies. Prior to that time, data was primarily siloed – government agencies were collecting and retaining data but were not required to share. Voluntary data sharing between agencies was managed by memorandums of understanding (MOU) or data sharing agreements – a process that was time consuming, ad hoc and bespoke to the specific data analysis in mind at the time of project initiation. This often led to delays in connecting datasets, incomplete datasets or data insights and limited potential for those datasets to be re-used for future analysis and insights.

The Act confirmed the newly established DAC as a key player in promoting and enabling cross-agency data sharing. It granted the DAC powers to obtain data from government sector agencies under certain circumstances, and with appropriate safeguards in place.

The Act also emphasised the importance of improved data sharing more broadly. It referred to government sector data as a public resource to support government policy making, program management and service planning and delivery. This, as the Second Reading Speech details, is critical for efficient strategic decision making, and ultimately for creating better outcomes for the people of NSW.

The Act was the first of its kind in Australia. Since this time South Australia, Victoria and the Commonwealth have established (or are in the process of establishing) similar data sharing legislative regimes (see section 4.2 for more detail).

It is important to note that the Act makes up only one part of the statutory framework governing data sharing across NSW government. It co-exists with agencies' enabling legislation (often containing data sharing provisions) and NSW privacy legislation (see section 4.1 for more information). As the interaction between the Act and these co-existing legislative schemes has the potential to facilitate or detract from timely and effective data sharing and insights, this review received numerous submissions on the topic and these comments have been considered as part of this review. This approach is consistent with objective 3(b) of the Act to 'remove barriers that impede the sharing of government sector data with the DAC or between other government sector agencies.'

3.2 Requirement for a statutory review after five years

Section 20 of the Act requires the Minister to undertake a review as soon as possible five years after the date of assent (24 November 2015) to determine whether the Act's policy objectives remain valid and whether its terms are appropriate for securing those objectives.

A report on the outcome of the review must be tabled in both Houses of the NSW Parliament within 12 months of the end of the five-year period (by 24 November 2021).

3.3 Objectives of the Act

Section 3 sets out that the objectives of this Act are to:

(a) 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

(b) remove barriers that impede the sharing of government sector data with the DAC or between other government sector agencies

(c) facilitate the expeditious sharing of government sector data with the DAC or between other government sector agencies

(d) provide protections in connection with data sharing under this Act by:

(i) specifying the purposes for, and the circumstances in, which data sharing is permitted or required

(ii) ensuring that data sharing involving health information or personal information continues to be in compliance with the requirements of the privacy legislation concerning the collection, use, disclosure, protection, keeping, retention or disposal of such information

(iii) requiring compliance with data sharing safeguards in connection with data sharing.

3.4 Consultation process

The Department ran a consultation process over February and March 2021. The consultation focused on:

- whether the Act is achieving its objectives
- common pain points with the Act and data sharing generally, including opportunities for improvement
- best practice legislative models
- citizen and industry views on data sharing in the NSW Government
- future data sharing needs of government over the next five years.

Consultation consisted of:

- 31 stakeholder interviews involving representatives from NSW Government clusters (including Cluster Chief Data Officers), Commonwealth Government agencies, state and territory governments, industry, not-for-profit organisations, peak bodies, regulators, community stakeholders and NSW Government governance groups (NSW Data Leadership Group, Cross-Agency Social Policy Data Analysis Group (CASPDAG) and the NSW Data Champions Network).
- public consultation through the digital NSW Government Have Your Say Platform.

The Department received a total of 124 public consultation responses, including:

- 81 survey responses
- 38 quick poll responses
- 5 written submissions (The Law Society of New South Wales, Spatial Services (NSW Government), Australian Research Data Commons (ARDC), NSW Information and Privacy Commission (IPC) and NSW Council for Civil Liberties).

Public consultation submissions were made by the government sector (63%), private citizens (31%) and private industry (6%).

The Department reviewed and considered all the feedback from stakeholder interviews, survey responses and written submissions in the preparation of this report.

4. Snapshot of the data sharing landscape

4.1 NSW legislation relevant to data sharing

The Act is not the only NSW legislation that governs data sharing. It operates alongside other legislative responsibilities on government sector agencies to collect, publish and provide access to data.

The table below sets out the key NSW legislation governing the sharing of data and operational arrangements and how they interact with the Act.

NSW legislation	Purpose	Interaction with *Data Sharing (Government Sector) Act 2015* (Act)
Privacy and Personal Information Protection Act 1998 (**PPIPA**)	Governs the way agencies can use or share personal information.	PPIPA overrides the Act. The sharing of personal information under the Act remains subject to existing NSW privacy legislation.
Health Records and Information Privacy Act 2002 (**HRIPA**)	Governs the way agencies can use or share health information.	HRIPA overrides the Act. The sharing of health information under the Act remains subject to existing NSW privacy legislation.
Government Information Public Access Act 2009 (**GIPA** Act)	Establishes that agencies must provide public access to certain datasets and reports.	The Act does not apply to information considered to be "excluded information of an agency" specified in Schedule 1 of the GIPA Act. Data shared under the Act must be maintained and managed in compliance with GIPA (where applicable).
State Records Act 1998	Ensures that agencies maintain records of their activities.	Data shared under the Act must be maintained and managed in compliance with *State Records Act 1998* (where applicable).
Agency specific enabling legislation	May set out data sharing rules and responsibilities specific to an agency. For example, Chapter 16A of the *Children and Young Persons (Care and Protection) Act 1998*.	Not clear whether the agency specific enabling legislation or the Act takes precedence. Section 5 of the Act makes disclosure of government sector data to the DAC or another government sector agency lawful for the purposes of any other Act or law that will otherwise operate to prohibit that disclosure. This has been used to override secrecy provisions contained in other legislation.

4.2 Data sharing legislation in other Australian jurisdictions

This statutory review has considered developments in data sharing legislation in all other Australian jurisdictions. While the NSW Data Sharing Act was innovative for its time, there have been significant developments since 2015:

- Governments in South Australia and Victoria have since introduced similar legislation in 2016 and 2017 respectively.
- The Commonwealth Government is currently developing the *Data Availability and Transparency Bill*.
- The Western Australian Government has committed to introducing privacy and responsible information sharing legislation for the WA public sector. Extensive public consultation on a proposed legislative model was undertaken in late 2019.

The table below sets out the key elements in the Victorian, South Australian and proposed Commonwealth legislation.

Scope	**Commonwealth –** *Data Availability and Transparency Bill*	**Victoria –** *Victorian Data Sharing Act 2017*	**South Australia –** *Public Sector (Data Sharing) Act 2016*	**NSW –** *Data Sharing (Government Sector) Act 2015* (DSA)
Objectives of the Act	To facilitate data sharing for the purposes of: 1. Delivery of Government services 2. Informing government policy and programs 3. Research and development	To establish the statutory office of the Chief Data Officer (CDO), and promote the sharing and use of public sector data for the purposes of: 1. Policy making 2. Service planning and design	To facilitate data sharing for the purposes of: 1. Delivery of Government services 2. Policy Design 3. Data analytics 4. Law enforcement 5. Emergency planning and response	To facilitate data sharing for the purposes of: 1. Delivery of Government services 2. Policy design 3. Research 4. Data analytics
Government deliverables that are out of scope	Sharing for an enforcement-related purpose, or for a purpose related to, or prejudices, national security, is out of scope.	1. Data shared for service delivery purposes 2. Certain types of data are out of scope namely: data that would disclose confidential sources or individual in a witness protection program, investigative measures or procedures or prejudice national security 3. Sharing with the non-government sector	Legally privileged and Cabinet data	Sharing with other jurisdictions and law enforcement
Authorised data sharing participants	Commonwealth bodies, state and territory bodies, private sector	Victorian Government agencies	SA Government, private sector, other states,	Public sector agencies (i.e. NSW Government, local councils and State-

	organisations, universities and academics, not-for-profit organisations, commercial and foreign entities.		Commonwealth, NGO's	Owned Corporations)
Authority level to direct data sharing	**No –** There is no duty for government agencies to share data, although data custodians must consider reasonable requests and provide reasons for a refusal to share to the applicant.	**Yes – CDO** may make a formal request for data but the obligation is only to provide the data or written reason for refusal, rather than being obliged to share	**Yes –** The Premier can issue a binding direction on any public sector agency to share data	**Yes –** Minister may direct sharing of data with the DAC (has not been exercised)
Data sharing & privacy safeguards	1. An accreditation framework by the Data Commissioner, to ensure only entities that are capable of handling data securely participate in the scheme to minimise risk of unauthorised access or use, 2. Data sharing purposes, to ensure data sharing is in the public interest, 3. Data sharing principles, to ensure data sharing is done safely and risks are managed, 4. Data sharing agreements, to set consistent terms for data sharing arrangements, and also an important transparency measure, 5. Exclusions for types of data, including national security data, the electoral Roll, and My Health Record and COVIDSafe App data. 6. Strong transparency mechanisms and effective oversight by the National Data Commissioner.	1. Permitted purpose for policy making, service planning and design only 2. Requiring identifiable data to be de-identified before analysis and outputs 3. Annual reporting to the privacy regulators 4. New offences for unauthorised access, use or disclosure 5. Privacy laws still apply- the Act provides an additional legal pathway to share identifiable data for data integration purposes	1. Modelled on Five Safes (*Trusted Access Principles*) 2. SA Protective Security Framework 3. No privacy legislation in South Australia. 4. There are *Information Sharing Guidelines* (ISG) that guide the handling of data and *Information Privacy Principles*.	1. NSW Privacy legislation takes precedence over the Act 2. Confidential and commercially sensitive information 3. Custody/Control safeguards (GIPA, State Records Act) 4. Other safeguards as set out in regulations (Note: No regulations developed under the Act).

	7. Periodic review of the Bill, to ensure it is operating as intended. 8. Existing requirements for data handling continue to apply, such as under the Protective Security Policy Framework and the Privacy Act, to ensure data is consistently managed.			

Victorian Government - *Victorian Data Sharing Act 2017* (VDS)

The *Victorian Data Sharing Act 2017* (VDS) allows for data-sharing between Victorian government departments and agencies for the purposes of policy making, service planning and design. It does not cover service delivery.

It establishes the statutory office of the Chief Data Officer (CDO) but does not expressly refer to the central data analytics agency that supports that statutory office (unlike the Data Analytics Centre which is referenced in the NSW Act).

The VDS provides an express legal authorisation under Victorian privacy laws to enable sharing of identifiable data for the purposes of data linkage. Victorian agencies are required to take reasonable steps to ensure no individual can be reasonably identifiable in the integrated dataset before any analysis takes place and must ensure that any outputs are de-identified prior to any disclosure.

Victorian Government – VPS Data Sharing Framework

The VDS is supported by a proposed VPS Data Sharing Framework which includes a policy with a clear 'responsibility to share' between Victorian Government where there is no legitimate basis to refuse the request, and a Heads of Agreement which sets some overarching terms and conditions for data sharing. The *Commonwealth Data Sharing Principles* are proposed to be adopted to align Victorian data handling practices with national requirements. The framework builds on the COVID-19 Data Sharing Policy and Heads of Agreement, which was endorsed by all Secretaries in 2020, to support the COVID-19 response.

South Australian Government - *Public Sector (Data Sharing) Act 2016*

The *Public Sector (Data Sharing) Act 2016* is currently the broadest data sharing legislation in Australia. It allows for data to be shared for most purposes, including policy making, program management, service planning and delivery. It also allows for sharing with law enforcement, which is a notable exception in Victorian and Commonwealth legislation.

This legislation overrides all South Australian legislation and allows public sector agencies to enter into data sharing agreements with any public sector body (including interstate, non-government) and private industry so long as:

- privacy safeguards (Trusted Access Principles based on the Five Safes model) are met, and
- the Premier signs the agreement.

Unlike Victoria, NSW and the Commonwealth, South Australia does not have privacy legislation. Instead, there are information sharing guidelines and other privacy related policies around the handling of data.

Exceptions include legally privileged information, Cabinet documents, and other sensitive information held by Justice.

Health data whilst exempt, may be shared where approved by the Minister for Health.

Commonwealth Government - *Data Availability and Transparency Bill*

The *Data Availability and Transparency Bill 2020* (DAT Bill) was introduced to the House of Representatives on 9 December 2020.

The DAT Bill creates an accountable and transparent data sharing scheme for the Australian Government to safely share public sector data by providing controlled access to the right people, for the right reasons, with safeguards in place. These safeguards ensure that sharing happens securely, and data is protected, to build trust in the scheme and its operation.

The DAT Bill takes a principles-based approach to data sharing and includes a system of safeguards to manage risk and streamline sharing processes. This includes the 'five-safes' framework which guides the handling and distribution of data, data-scheme entities going through a process of ensuring compliance with the Privacy Act, three permitted purposes of data sharing, strong consent protocols, and accreditation of data-scheme entities to ensure they meet security and privacy standards. The DAT Bill does not require agencies to share data; it provides an alternative pathway to share where it is currently prevented by secrecy provisions or where it simplifies existing pathways. The DAT Bill was developed using a privacy by design approach to ensure protections for individuals' privacy.

The National Data Commissioner (NDC) will be empowered with advice, guidance, regulatory, and advocacy functions to oversee the scheme.

5. Findings of the review

5.1 Objectives of the Act

The Act authorises government sector agencies (primarily NSW Government agencies) to actively share government sector data to improve policy making, program management and service planning and delivery. Data is to be shared efficiently and promptly in compliance with privacy legislation and data sharing safeguards.

Of particular interest to this review, Object 3(b) of the Act highlights the intention to remove barriers that impede data sharing within NSW Government and Object 3(c) seeks to facilitate the expeditious sharing of government sector data with the DAC or between other government sector agencies.

What we heard

We heard that while the objectives of the Act remain valid, there are various issues that impede efficient and effective data sharing.

Agencies are not directly using the Act and significant cultural and operational barriers still exist

There is limited evidence of the Act being directly used by NSW Government agencies. Most NSW Government clusters reported:

- a lack of awareness of the Act across the NSW public sector
- either not using the Act, or minimal experience using the Act for limited purposes (i.e. to override a secrecy provision in accordance with section 5)
- that using alternative mechanisms to the Act that are available under Privacy legislation to facilitate data sharing because the agency was not clear whether the Act allowed the agency to do what it needed to, or the Act would not allow this.
    - For example, because the Act requires sharing of personal information to comply with the Privacy legislation, the use of personal information for certain activities, such as data integration (i.e. data linkage) has required a Public Interest Disclosure (**PID**) or Privacy Code of Practice (**PCoP**) to be established, unless there was an exemption available (e.g. Human Research Ethics Committee approval). Agencies have also used Memorandum of Understanding and Data Sharing Agreements to set out data sharing arrangements.

Data sharing across NSW Government can be slow and inconsistent

It should be noted that there have been steady improvements in data sharing across government since the Act first commenced. Over the last five years, the landscape and need for data sharing has evolved and the objectives and supporting information in the Act should be updated to reflect the current and future needs of data sharing across NSW Government. Currently most clusters are of the view that data sharing within NSW Government is now inconsistent, time intensive and slow.

Clusters commonly reported that while there has been improved data sharing since the Act was introduced in 2015, significant operational and cultural barriers remain which prevent data sharing not only between agencies, but within agencies. Barriers include:

- treating similar data requests as individual, resulting in duplication of effort, cost, and delays
- manual nature of providing data, including when de-identifying data and ensuring re-identification is eliminated and/or minimised
- lack of a consistent, agreed approach to data sharing, meaning a new process needs to be established and agreed for each project
- lack of supporting materials to operationalise the Act (i.e. guidance materials specifically targeted to data sharing activities to support its implementation)
- lack of certainty for agencies on how to apply data sharing safeguards under the Act. Stakeholders suggested that a regulation under section 15 of the Act is needed to provide confidence about how the data will be managed (refer to section 5.5 for further details)
- impact of the interdependency of privacy legislation and length of time for relevant approvals under the NSW privacy legislation.

Data sharing challenges during Machinery of Government changes

The Act does not provide an express means of ensuring data sharing continuity during a Machinery of Government (**MOG**) change which has the potential to prevent or make data sharing difficult, particularly within the same cluster. In instances where there is personal information involved this becomes the remit of privacy legislation.

The Department of Communities and Justice (**DCJ**) indicated that data sharing within the cluster is challenging following the MOG changes that occurred in 2019, merging the former Department of Family and Community Services and the former Department of Justice. In this

example, this lack of continuity has impeded the cluster's ability to provide a holistic view of a customer's life journey and therefore limits the efficiency and effectiveness of service delivery to that merged customer base.

The NSW Bureau of Crime Statistics and Research (**BOCSAR**) were granted a PCoP (gazetted in June 2000, well before the 2019 MOG changes) which allows BOCSAR to receive protected data to conduct research and analyses that enhance understanding of crime and criminal justice. DCJ have been able to leverage the BOCSAR PCoP to share DCJ data however the use of any integrated data must still align with the PCoP which is too narrow for DCJ in its entirety. To facilitate the sharing of data more broadly across DCJ and for other purposes, DCJ are working on the development of a PID.

Agencies need more support to use the Act

A common theme is that the Act needs to have more supporting materials to provide guidance on how the Act should operate in practice.

Clusters commonly reported that there was no guidance on how to address many of the perceived barriers to streamlining the data sharing process. Feedback highlighted a need for clear, simple, and practical guidance material that interpreted the requirements of the Act for business as usual purposes and to support appropriate decision-making regarding compliance, without heavy reliance on legal counsel. Views expressed about the scope of the guidance material included:

- addressing data governance issues around what data can be shared and what cannot
- addressing how data can be used
- accounting for how de-identification will occur, for what purpose and by who
- what and how data insights can be shared
- what insights could be published
- how to manage access controls to data
- what remedial action to take in the unlikely event of a data sharing breach – i.e. who fronts the costs of remediation and how remediation measures can be implemented in practice.

The NSW Government Data Strategy includes an action to consolidate whole of government data policy, including developing a common data sharing agreement and a streamlined approval process across government, aligning with the Australian Government's data sharing scheme as appropriate. This should build on the collaborative cross-sector data sharing that occurred in response to COVID-19.

The Victorian Government, in the context of COVID-19 data sharing, has addressed some of these operational and cultural barriers through its COVID-19 data sharing policy. This is believed to have resulted in less complexity, reduced duplication of effort and reduced legal burden. Victoria is now in the process of implementing COVID-19 data learnings permanently.

Establishment of centralised data assets and library

To facilitate efficient and timely data sharing, some clusters supported establishing whole of government linked data assets where appropriate (e.g. the Human Services Data Set has been established in the human services sector) and a library of existing data sets across NSW Government so there is visibility across the sector about what data is already available. A data discovery exercise is in progress through the NSW Data Leadership Group to gain visibility of the high value data assets held across the sector. There is growing

consensus that high value data assets should be considered digital infrastructure by government and that they should be treated as such and included in the State Infrastructure Strategy.

It was proposed that a nominated agency be responsible for linking data containing personal identifiers (and then deidentifying it before use), maintaining these data assets on behalf of all agencies and restricting access to those who need it to perform their job (examples include DAC, CHeReL for health-related data sets). There were mixed views on how regularly these linked data sets needed to be updated, with some clusters supporting real time updates, while others were happy with periodic updates.

Findings

There is broad support for whole of government data sharing legislation in NSW and the policy objectives of the Act. Data sharing and analysis is more important than ever across all endeavours of life, and governments are becoming more adept at using data insights to inform and shape better policy, services and programs. The Act's objectives remain valid.

There have been a number of initiatives under the Data Sharing Act, which have delivered significant community benefit, particularly in the context of COVID-19. However, a number of delays and practical issues have been identified by stakeholders in undertaking projects under the Act which require action.

The Act is not yet maximising achievement of its objectives because agencies need:

- greater support to address their current data sharing needs
- further detailed guidance on how to share data safely in practice
- improvements to some data sharing processes to instil greater confidence
- more supporting information to use the Act effectively and put it into practice
- consistent, risk-based and streamlined approval processes.

It should be noted that there are some data sharing guidance materials already published on the Data.NSW website (https://data.nsw.gov.au/data-sharing-principles. The IPC has also published guidance on data sharing (https://www.ipc.nsw.gov.au/guide-data-sharing-and-privacy), and a fact sheet on de-identification of personal information (https://www.ipc.nsw.gov.au/fact-sheet-de-identification-personal-information) There may be a lack of awareness of these materials across the NSW public sector and a single information point would be beneficial.

Enhancements to the Act and its supporting materials could better support achieving its objectives, particularly to enable the efficient and timely sharing of data. These enhancements are outlined in the recommendations set out in this report. This may require additional guidance material to be developed for agencies but could also mean amendments to the Act and/or privacy legislation are needed. Where this report refers to clarifying the operation of the Act, it may ultimately be appropriate to do this through guidance, legislative amendments, or a combination of both.

At the highest level, the feedback received from stakeholders indicates that the intended operation of the Act needs to be clarified to support agency implementation, in particular to:

- provide more detail on the data sharing process for some parts of the Act
- revise existing guidance materials to provide clarity and direction about the Act's intended scope, authority, interpretation and practical application
- clarify the interaction of the Act with NSW privacy legislation.

Standard data sharing mechanisms are needed to agree standard terms and conditions upfront and support efficient data sharing across government. The DAC advised that currently there is a Human Services Information Sharing Memorandum of Understanding to standardise data sharing in the Human Services field.

Improved awareness of the Act through these initiatives is likely to support greater sharing of data insights across NSW Government agencies and better policy, program and service delivery outcomes for the people of NSW.

Linked datasets and the data insights derived from them are increasingly viewed as critical government assets and digital infrastructure. Like all government infrastructure, these assets will require careful management and maintenance over time. During consultation, there was support for the creation of a library of existing data sets across NSW Government to promote visibility across the sector about what data is already available, as well as a nominated agency being responsible for linking data containing personal identifiers (and then deidentifying it before use and disclosure), maintaining these data assets on behalf of all agencies and restricting access to those who need it to perform their job (i.e. examples include DAC, CHeReL for health-related data sets).

Recommendation 6: Improve the efficiency of data sharing

Support the introduction of a standard data sharing agreement between agencies to agree standard terms and conditions upfront to increase efficiency in data sharing.

This recommendation will address the ad-hoc nature of data sharing agreements by reducing duplication of effort, costs and delays in drafting such agreements.

Recommendation 9: Create centralised linked data sets

Implement centralised linked data sets and develop a library of high value data sets across NSW Government. Apply data sharing safeguards, as appropriate, in alignment with Recommendation 4. This will facilitate efficient and timely data sharing across Government which can reduce duplication of efforts, coordinated by the DAC as the central body for data sharing.

This recommendation will facilitate efficient and timely data sharing across Government which can reduce duplication of efforts, coordinated by the DAC as the central body for data sharing.

Recommendation 12: Support consistent interpretation and greater usability of the Act

a. Clarify the intention of the Act's provisions to support consistent interpretation and greater usability and take up of the Act.

b. Update existing supporting materials for the Act to provide greater clarity around how to implement the Act.

The intended outcome of this recommendation is to clarify the interpretation of the Act to build sector confidence in using the act to its full potential.

Recommendation 14: Promote greater, more timely and more efficient data sharing through the use of the Act

Better promote the Act and its supporting frameworks to enable greater use of data sharing.

This recommendation will increase awareness of the Act and uplift the confidence and capability of the sector to share data insights.

5.2. Defined terms

Section 4 defines key terms used in the Act. This includes terms like Data Analytics Centre, government sector agency, government sector data, control, data provider and data recipient.

What we heard

Terminology is inconsistent with contemporary language around data sharing

Terminology in the Act used to describe an agency's power over, or relationship to, data is outdated. For example:

- an agency's role in respect to data is not static. An agency can play multiple roles throughout the data lifecycle, and these roles can vary depending on the data set (i.e. an agency can be a custodian in one instance, and a data provider in another).
- technology has changed the concept of "control" of data. For example, cloud computing means that data can be held in multiple locations with multiple "owners" or agencies with access rights. While the Act specifically includes data held in the cloud, there is an assumption that the data can be held by a single person or body. However, there is not a clear interpretation of who "controls" the data in practice.
- the ARDC written submission further highlights the need to remove language such as 'data ownership' or the 'possession of data' from the Act. The submission also points out the need to remove language that links information or electronic documents to particular agencies.
- there is inconsistent data terminology and definitions in legislation across Australia. Consultation highlighted the need for NSW to adopt industry best practice

terminology and, where possible, align with data sharing legislation in other Australian jurisdictions to better support interjurisdictional data sharing. For example, the Act references 'data provider' and 'data recipient', whereas the Commonwealth DAT Bill uses 'data custodian'.

References to DAC should be updated to reflect current practice

This Act is commonly referred to as the "DAC Act" in NSW Government, which is indicative of how some of the objectives of the legislation (i.e. to support data sharing across *all* of NSW Government) can be overlooked. References to the DAC should be reviewed and where necessary expanded to also include more generic terms that focus on an agency's role with data (e.g. data provider and data consumer). This will better recognise the Act's whole of government data sharing focus.

The degree of emphasis on the DAC in the Act has also resulted in perceived limitations to its functions that do not apply to other agencies. For example, the DAC has previously been prevented from sharing data outside of the NSW Government as it was viewed that DAC's powers were limited to the provisions expressly contained in the Act.

Findings

The current Act was drafted in 2015 when the DAC was first established. The Second Reading Speech is clear that a key aim of the Act is to provide the DAC with the legislative authority to obtain data (in certain circumstances) from government sector agencies with the appropriate safeguards in place.

Adopting more contemporary terminology, aligned to industry best practice will:

- help to future proof the Act
- more closely align to the practical reality of data sharing in NSW Government, including reflecting the broader role all agencies play in data sharing help to reduce uncertainty when interpreting the Act, and
- ensure greater alignment with other jurisdictions. As discussed below, there is broad support for the Act to be expanded to include data sharing beyond NSW Government (see section 5.6) and consistent terminology (where suitable) will support this.
- With the DAC now an established entity within NSW Government, the data landscape has evolved, and a clearer message needs to be communicated in and around the Act about other agencies in NSW Government being able to perform data analytics functions as well.

Recommendation 7: Clarify data sharing functions across NSW Government

Clarify that the key functions that relate to data sharing described in the Act, apply to any NSW Government agency that has the relevant capability to perform that function.

This recommendation will facilitate the Act being used to its full potential and by agencies other than just the DAC.

Recommendation 8: Clarify DAC's role and authority

Clarify that while DAC is the central body for data and analytics services across NSW Government, it is not intended that terms of the Act restrict DAC to activities explicitly outlined in the Act. DAC can undertake activities that any government agency is ordinarily allowed to undertake.

This recommendation will clarify the DAC's role and scope of activities.

Recommendation 11: Clarify definitions in the Act

Clarify the Act's definitions with reference to industry best practice definitions and/or definitions used in data sharing guidance provided by the Office of the National Data Commissioner.

This recommendation will clarify the interpretation of the Act by aligning it to Commonwealth standards, noting definitions outlined in NSW privacy legislation and the GIPA Act.

5.3 Government sector data sharing

Part 2 of the Act outlines the various mechanisms for sharing data. It covers voluntary data sharing, mandated data sharing under Ministerial direction and the DAC's authority to share insights.

Section 6 of the Act authorises government sector agencies (other than the DAC) to voluntarily share data with the DAC or other government sector agencies:

- for data analytics purposes to identify issues and solutions regarding government policy making, program management and service planning and delivery
- to enable agencies to develop better government policy making, program management and service planning and delivery
- for purposes set out in the regulations (note: no regulations currently exist under the Act).

This sharing is conditional on data sharing safeguards being met.

Sections 7, 8 and 10 authorise the Minister for Customer Service to direct a government sector agency or a State-Owned Corporation to provide the DAC with specific data or information about data sets that the agency controls.

Section 9 authorises the DAC to share insights with other government agencies but is silent on the authority of other agencies to share insights. Section 9 has also been interpreted by some that the DAC can only share data insights that it has generated with the government sector agency that provided the data.

What we heard

The Ministerial direction to share data has not been used

There are no known instances of the Ministerial direction to share data being used. The DAC reported that there have been a few instances where a Ministerial direction pathway had

been considered, however these data sharing requests were resolved between Departments.

The DAC noted a strong preference to work collaboratively with agencies providing data to ensure that data is interpreted correctly and insights are verified. It was suggested that the Act or supporting materials be updated to accommodate this need for collaboration.

Consultation with the Victorian Government highlighted that the Request & Respond approach under the *Victorian Data Sharing Act 2017* was viewed as a form of escalation that may adversely impact stakeholder relationships. Conversely the South Australian Government indicated that there was some support amongst its agencies for including a direction to share in their legislation (there is no current provision for this).

The Law Society's written submission suggested that the scope of the Ministerial direction (or right to call-in data) could be extended, subject to certain requirements:

- the agency calling in the data must be able to demonstrate that the Five Safes Principles have been considered and met in relation to the data
- transparency requirements should be included, for example in the form of an annual report to Parliament or the Privacy Commissioner on the use of this power (as is the case in Victoria)
- such a right should be subject to provisions in subject-specific legislation, for example, laws relating to access to driver licence information and CCTV information should not be overridden, and
- enables the one-off provision of a data set, rather than an ongoing data feed, or access to a database (i.e. replace the section 41 exemptions process in PPIPA, rather than set up a long term, comprehensive data sharing regime).

Agencies have a role in verifying data analytics work performed by the DAC

There was some divergence in opinion on the ability of the DAC to distribute data insights beyond the agency that provided the data. This relates specifically to whether the agency or agencies have the absolute authority to prohibit the sharing of data insights work carried out by the DAC with any other agency, person or body.

There was strong support for the agency that provided the data to play a role in:

- verifying the data insights
- reviewing insights and interpretations
- deciding the current and future use of the data and data insights
- determining how, and with whom, the data insights are shared.

This is not absolute control over the decision making – instead agencies should be part of the decision-making process, but where there is an overriding public interest to share, this should be actioned.

It was also recognised that often data analytics involves data provided by more than one agency – providing all agencies with absolute control over how the data insights will be utilised would be time consuming and impractical.

The DAC strongly supported agencies having a role in validating analytical outcomes and reviewing insights and interpretations. The DAC indicated that it actively seeks agency involvement in any decisions to distribute data more broadly.

Submissions by private citizens and private industry through the Have Your Say platform supported seeking data custodian consent before any on-sharing of data.

There was minimal support for providing the agency with absolute power to determine access to insights or for allowing the DAC (or any other analytics entity) to have authority to treat the data insights as a government asset that can be shared without the agency's involvement.

Findings

The review notes the concerns over using Ministerial direction for data sharing but recognises that there may be instances where intervention is needed. The Act (or supporting materials) should be updated to make it clear that the agency (or agencies) that provide data in accordance with a Ministerial direction have a right and responsibility to work with the DAC (or any other NSW Government agency performing the function) to ensure that data is interpreted correctly, and to verify the insights.

Section 9 of the Act should be amended to enable de-identified data insights to be on-shared by the agency that performs the analytics function (i.e. like DAC), on the condition that the agency or agencies that provide the data are given the opportunity to:

- verify the accuracy of the data insights, and
- have visibility over the current and future use of the data and data insights, and
- have been consulted on the decision to share.

Agencies should not object to the on-sharing of data insights unless there is an overriding public interest. Whilst agencies have expressed strong support to amend section 9 of the Act on the condition of consent, the need for continued encouragement to share de-identified data insights is required to ensure the objectives of the Act (section 3) are met. These objectives include:

- promoting the management and use of government sector data that supports good government policy making, program management and service planning and delivery
- removing barriers that impede the sharing of government sector data with the DAC or between other government sector agencies; and
- to facilitate the expeditious sharing of government sector data.

Recommendation 1: Support on-sharing of data insights

a. Amend section 9 of the Act to enable de-identified data insights to be on-shared by the agency that performs the analytics function, on the condition that the agency or agencies that provided the source data have been consulted on the decision to share and:
   - had the opportunity to verify the accuracy of the data insights,
   - have visibility over the current and future use of the data insights, and
   - have access to the data insights.

b. Agencies should support sharing the data insights unless there is an overriding public interest against the data being shared.

This recommendation will promote data sharing collaboration across agencies while minimising the risk of misuse and misinterpretation. This recommendation should be read in conjunction with the recommendation relating to risk-based privacy assurance (recommendation 4).

Recommendation 13: Support efficient data verification

Clarify that any agency that provides data in accordance with a Ministerial direction will work with the DAC (or any other NSW Government agency performing the function) so that data is interpreted correctly and data insights are verified efficiently.

The intended outcome of this recommendation is to support accurate and efficient data sharing.

5.4 Relationship of the Act with other laws

Section 5 sets out how the Act interacts with other legislation. It outlines how:

- the Act can be used to facilitate data sharing that might otherwise be prohibited (secrecy provisions); and
- NSW privacy legislation takes precedence over the Act.

What we heard

The Act's ability to override secrecy provisions is underutilised and not widely understood

Consultation uncovered one cluster that has used the Act to displace secrecy provisions in other legislation. Other clusters were unaware of this provision and/or used alternative mechanisms to achieve the same effect.

The hierarchy of data sharing legislation needs to be clarified

While the Act is clear that the NSW privacy legislation currently takes precedence over the Act, there is a lack of clarity on how the Act interacts with data sharing provisions in other NSW legislation (in addition to the secrecy provisions). Clusters commonly reported that it was unclear if data sharing provisions in agency or business specific legislation were displaced by the Act. The lack of clarity was often cited as a key reason why clusters believed other agencies were unwilling to share data.

Concerns regarding how some data may be used

Consultation revealed some concerns about datasets being shared or data insights being used for an enforcement-related purpose, national security reasons or driving potentially unintended prejudices even though the data is deidentified. These uncertainties and concerns could also be a reason why some data custodians may be unwilling to share the data they hold.

Findings

To facilitate and remove barriers to whole of government data sharing, there is a need to clarify the precedence of the Act over other agency or business specific legislation that might otherwise constrain data sharing.

In South Australia, the data sharing legislation takes precedence over all other legislation where a conflict arises, and it contains provisions that allow a Minister to direct an agency to share data even when exemptions exist.

Section 5(1) of the Act provides that a disclosure of government sector data by a government sector agency to another government sector agency is lawful for the purposes of any other Act or law that would otherwise operate to prohibit that disclosure. However, this is subject to numerous qualifications, including requirements that:

- the disclosure is authorised (as per s. 5 of the Act) for an appropriate purpose (as per s.6);
- the privacy legislation is complied with;
- the data is not "excluded information of an agency" under Schedule 2 to the Government Information (Public Access) Act 2009 (GIPA Act);
- the secrecy provision in question does not appear in clause 1 of Schedule 1 to the GIPA Act;
- the data is not otherwise of a kind described in Schedule 1 to the GIPA Act; and
- additional Part. 3 safeguards can be complied with, including as to confidentiality and commercial-in-confidence, having regard to the existence of any contractual or equitable obligations.

Recommendation 5: Clarify data sharing precedence to increase data sharing

a. Clarify, that with the exception of exclusions set out in Section 5(2) of the Act (i.e. NSW privacy legislation, GIPA and State Records Act), the Act permits a government sector agency to share data with the DAC or another government sector agency for the purposes set out in the Act in cases where the sharing of the data is constrained by a provision in other NSW legislation.

b. Develop documentation to clarify existing exclusions to this provision (i.e. NSW privacy legislation, GIPA and State Records Act).

This recommendation will clarify the position of the Act relative to existing legislation and promote the use of the Act to its full potential.

To address potential concerns around data sharing for an enforcement-related purpose, or for a purpose related to prejudices, national security etc. further consideration and consultation is required.

5.4.1. Data sharing and privacy safeguards

Part 3 of the Act sets out the data safeguards that apply to data sharing under the Act. This section requires NSW Government agencies to:

- ensure that health and personal information is only shared in accordance with HRIPA and PPIPA - together known as the NSW privacy legislation.
- ensure that confidential or commercially sensitive information is managed in accordance with any contractual or equitable obligations.
- ensure that shared data is managed in compliance with any legal obligations concerning its custody or control (for example, requirements under the *Government Information (Public Access) Act 2009* or *State Records Act 1998*).
- any other requirements set out in the regulations (note, no regulations have been made under section 19 of the Act).

The Act was introduced in 2015 to signal a turning point for data sharing in NSW Government – it recognised the increasing value of data and the need for it to be shared across NSW Government agencies to inform evidence based policy and the development of effective, tailored services to the community. It also recognised the need for establishing appropriate safeguards to protect data.

Importantly, the Act has not displaced the protections for personal information in NSW privacy legislation, even where the intention is to create de-identified datasets and data insights. This approach has had a notable impact on the use of the Act over the past five years. As a result, privacy was a key theme in the consultation process.

What we heard

There were mixed views on the effectiveness of the current privacy safeguards – some want more, some want less, but everyone agrees they need to change

Consultation highlighted mixed views on the effectiveness of privacy safeguards in the Act and the relationship between the Act and NSW privacy legislation. There was broad agreement about the critical need to protect citizen privacy in data sharing, but there were divergent views on how this can best be done, particularly in relation to de-identified data.

There were some stakeholders who advocated for stronger privacy safeguards, arguing that the NSW privacy legislation alone was inadequate, pointing to recent data breaches as evidence of this. Of the private citizens that responded to the online Have Your Say public consultation, 56 percent indicated that they did not trust the Government to hold their data, while 80 percent held concerns about the government holding their data.

The Information and Privacy Commission (**IPC**) and NSW Council for Civil Liberties (**NSW CCL**) both noted in their written submissions the importance of including privacy safeguards and agencies considering the risk of reidentification when sharing linked data. The Law Society also confirmed the need to ensure the privacy of the individual is upheld.

NSW CCL added that sharing of personal information should be limited – it should only occur for the purpose of achieving a specific policy and/or program outcome or be in the interest of the public. NSW CCL proposed introducing an independent assessment process to ensure the appropriateness of sharing the personal information and whether the agency receiving the personal information has relevant skills and experience to manage the data safely.

A strong view, particularly amongst NSW Government clusters, is that the current privacy safeguards in the Act and in NSW privacy legislation are not always fit for purpose for data sharing under the Act. A common theme was that the current approach (where the NSW privacy legislation takes precedence over the Act) can significantly impede the timeliness of data-informed policy making, program management and service planning and delivery:

- agencies report uncertainty around the definition of ‘deidentified information’ – this has resulted in conservative and varied interpretations as to what is permissible to share and how it can be shared. Forming a view about whether a dataset is adequately de-identified must be assessed contextually and necessitates a risk based approach that includes assessing the data in the context of its use and access environments. Re-identification may be technically possible, but because of the safeguards in place (e.g. secure environment, robust access controls), the reasonable likelihood of this occurring is very low (https://publications.csiro.au/rpr/download?pid=csiro:EP173122&dsid=DS3).

- the privacy legislation comes into play before any data is shared, meaning that data sets containing personal or health information cannot easily be linked both within and across agencies. This issue is particularly prevalent in the human services sector, where agencies need to share identified data to create de-identified linked datasets. These datasets provide a holistic view of citizen outcomes across interrelated services to improve the design and efficacy of those services.
- agencies seeking to share data that contained personal or health information commonly reported lengthy delays applying for a bespoke PID (PPIPA, section 41; HRIPA, section 62) or a PCoP (PPIPA, Part 3; HRIPA, Part 5).

Many stakeholders believe that the interaction between the Act and PPIPA should be reviewed

During consultation many stakeholders recommended that the outcomes of this Review would be further strengthened with a review of PPIPA. Several agencies suggested simplifying the definition of personal information in section 4 of PPIPA to minimise ambiguity on what, and how, data can be shared.

Conversely the NSW CCL's submission argued that PPIPA needs to be reviewed to meet community expectations of privacy, remove excessive exemptions and prevent overriding of the PPIPA by other statutes.

Support for the Victorian approach that enables data linkage

There was broad support both within NSW Government and external to NSW Government for adopting a model similar to the *Victorian Data Sharing Act 2017* that enables identifiable data to be shared with the Victorian Chief Data Officer or a data analytics body for the purpose of data integration. The Victorian Chief Data Officer or the data analytics body are then required to take reasonable steps to ensure that the data is deidentified prior to data analytics work commencing[1]. This requirement is less strict than the requirement to ensure the data 'no longer relates to a reasonably identifiable individual' which applies before disclosing the data (for example in the public domain). This is because the analytics takes place in a controlled and trusted user environment.

NSW Government agencies would like the Act to generally enable personal identifiers to be used to create de-identified linked data assets, rather than needing to get an exemption under the privacy legislation through a PID or PCoP each time. Agencies believe the Act should enable the use of personal identifiers to do the data linkage, resulting in a de-identified data asset that is privacy preserving. As with the Victorian legislation, oversight by the Privacy Commissioner would be required.

Consultation also highlighted a common understanding that the volume of data will increase exponentially in the coming years, resulting in an increased demand for data linkage. Many stakeholders believe that the Act in its current form, particularly as it interacts with privacy legislation, will not enable this.

Findings

The timely creation of de-identified linked datasets is imperative to better support evidence-based policy and effective, tailored, services for NSW citizens. The power of developing and

[1] Victorian Data Sharing Act 2017, Guidance for departments and agencies, https://www.vic.gov.au/sites/default/files/2019-03/Victorian-Data-Sharing-Act-2017-web-guidance.pdf, DPC, 2017

using aggregated digital datasets and data insights within government has been demonstrated through recent initiatives that have delivered better services and outcomes for NSW citizens, as detailed in the Executive Summary to this report.

As the world becomes increasingly digital, whether through digital services or smart infrastructure and devices, so increases the volume of data held by governments and the potential for that data to inform better policy, services and programs. This review must assess whether the Act's terms are appropriate for securing its objectives in the future, with consideration of this evolving environment. In this context, the feedback provided to this review has given rise to the need to consider whether the existing ways in the which the Act intersects with other legislative regimes provides a streamlined, proportionate and risk-based approach to using these data-driven opportunities to deliver better future outcomes for our community.

Privacy approvals required on a case by case basis are not always the most efficient way of enabling data sharing

Submissions to the review suggested that the current interaction of the Act and the NSW privacy legislation is limiting the efficient and timely sharing of some NSW Government data. For example, the creation of linked data assets has required the use of PIDs or PCoPs, several of which have reportedly involved lengthy and resource-intensive processes. A key driver of these concerns is the need to apply for ad hoc approvals on a case-by-case basis.

Alternative approaches to record linkage have been implemented in other jurisdictions which implemented data sharing regimes after 2015. Of particular note is the Victorian model which enables identifiable data to be shared with the Victorian Chief Data Officer (**VCDO**) or a data analytics body for the purpose of data integration. The VCDO or the data analytics body are then required to take reasonable steps to ensure that the data is deidentified prior to data analytics work commencing. In Victoria, this process involves the Officer of the Victorian Information Commissioner (**OVIC**) and Health Complaints Commissioner (**HCC**) oversighting the performance of the VCDO who must report annually to the Victorian privacy regulators, OVIC and HCC. Reporting details the steps taken to ensure compliance with privacy laws, the data projects that have been undertaken, details of data requests and refusal and issues and challenges that have arisen. Any breach of the privacy laws must be reported to the privacy regulator and the original data provider. For more information see Guidance for departments and agencies on the Victorian Data Sharing Act 2017.

End users find existing guidance too generic and difficult to interpret and apply in a data sharing and analytical environment

Another issue raised by stakeholders with existing processes is the lack of clear guidelines specifically tailored to data sharing. Creating de-identified linked datasets involves the use of personal identifiers, which are removed once the linkage is completed. Under NSW privacy legislation, a PID or PCoP is used to permit the use of personal information to link the datasets. Although guidance is available for agencies on applying for PIDs and PCoPs, this information is general and is not specific to data linkage. Developing a standard framework for applying for PIDs or PCoPs for the creation of de-identified linked datasets would expedite this process. This would ensure that the relevant information needed to implement a PID or PCoP is readily available. It would also support the audit and attestation requirements for the privacy assessment that can often contribute to the lack of efficiency of this process.

Sharing de-identified data is constrained by uncertainty around the definition of de-identified information

Agencies report uncertainty around the definition of 'deidentified information' – this has resulted in conservative and varied interpretations as to what is permissible to share and how it can be shared.

A risk based approach is required which considers not just the technical possibility of reidentification but also its likelihood, and any existent safeguards in place which would ameliorate the risk in practice. Many of the data sharing activities under the Act to date have involved already de-identified datasets held solely within government.

Each dataset should be assessed contextually to determine whether it has been adequately de-identified. Re-identification may be technically possible, but because of the safeguards in place (e.g. secure environment, robust access controls), the reasonable likelihood of this occurring is very low (see OAIC report on The De-Identification Decision-Making Framework)

Advances in technology, including the development of privacy enhancing technologies support this approach. For example, before publishing open data on COVID-19 cases and tests, the DAC used the Personal Information Factor tool (https://data.nsw.gov.au/nsw-government-data-strategy/case-studies/case-study-personal-information-factor-pif-tool) on the datasets to assess the risk of identifying an individual in the data and provide a measure of the information that could be gained about them by accessing the datasets. Information security capability is increasing across government and government agencies must apply security controls when sharing data, including implementing information security management.

Five Safes Framework

There was strong support amongst NSW Government agencies to strengthen the data sharing safeguards with a modified version of the Five Safes Framework – a risk-based framework that helps to identify and manage data sharing risks. This approach has been used in equivalent data sharing legislation in South Australia (Trusted Access Principles), and the Commonwealth's *Data Availability and Transparency Bill* (Data Sharing Principles) that is currently before their Parliament. The Victorian Government has also adopted the Commonwealth's version of the Five Safes Framework in its COVID-19 Data Policy (and in policy supporting its *Victorian Data Sharing Act 2017*). The Law Society's written submission also supported the Five Safes Framework.

The rationale for shifting to the Five Safes Framework is that it contextualises data sharing. It requires agencies to assess the risks associated with sharing data with other agencies (i.e. people, projects, settings, output and data) and implement safeguards that are appropriate in those circumstances. It is suggested that it will be safer (or lower risk) to share a data set where there is a potential to re-identify an individual which is in a high trust environment (i.e. with an agency that has met the Five Safes standards) compared to a low trust environment.

It is noted that the DAC already use an approach consistent with the Five Safes Framework. The Five Safes are also referred to in the DAC's Infrastructure Data Management Framework (IDMF), Data Governance Toolkit and the Data Sharing Principles on the Data.NSW website.

Recommendation 4: streamline the approach for approval of de-identified linked datasets to be used within government.

Consult with the Privacy Commissioner to develop a standardised framework for streamlined, timely, risk-based privacy assurance to guide the creation of de-identified linked datasets and insights for use within government, including drawing upon models in other jurisdictions such as that in Victoria. This framework should reference the technical tools and capabilities available within government to effectively manage information security and protect privacy and create a high trust environment for record linkage and data sharing.

This recommendation should improve the efficiency and effectiveness of creating de-identified linked datasets in line with robust privacy protection. It will also support greater use of data sharing by building data custodian's confidence that appropriate, risk-based safeguards are in place.

5.5 Data sharing in emergencies

The Act currently does not contain any specific provisions relating to data sharing in the event of an emergency, natural disaster or hazard (e.g. pandemic outbreaks, droughts, floods, bushfires, storms, landslides, cyclones, tsunamis, earthquakes and heatwaves) or other disasters (e.g. terrorist attacks, explosions).

To respond to the COVID-19 pandemic effectively, the NSW Government introduced bespoke data sharing measures in the Public Health Order (**PHO**) on Gathering and Movement to enable data sharing. This authorised agencies to collect information (including personal and health information) from, or use or disclose information to, an agency where necessary for the purposes of protecting the health or welfare of members of the public during the pandemic.

Although some types of data shared under the PHO could have been shared under existing legislation, the PHO was preferred – it was the fastest means to achieve data sharing, and removed the need for agencies to seek legal advice or exemptions to certain Information Protection Principles under the NSW privacy legislation (i.e. on data collection, use and disclosure). The provisions in the PHO operate alongside the NSW privacy legislation, so other Information Protection Principles including maintaining security or giving people access to their own information, are still required.

There is no PHO equivalent that permits data sharing for other emergencies or natural or other disasters and hazards.

What we heard

The prevalence of bushfires and floods, and the ongoing COVID-19 pandemic present a compelling case for establishing a standardised approach to data sharing that can be activated in an emergency.

The NSW government's data-driven response to COVID-19 was supported by the DAC's central coordination of data sharing across government. Key enablers were integration of data and insights from agencies and non-government sectors, making them available for those with relevant approval to use, along with strong data governance to ensure

appropriate protection of the data and the PHO. The DAC supports a legislative mechanism of accommodating data sharing in the event of an emergency or natural or other disasters and hazards rather than requiring bespoke responses like the PHO. Legislation should outline an agreed approach to accelerate bringing data together from across government agencies and non-government sources, coordinated centrally by the DAC, to maximise the value of data insights more quickly and make them available to decision-makers when they need them, to better respond and adapt to emergency situations.

The NSW Information and Privacy Commission's written submission acknowledged that there is a strong public interest in allowing government agencies to share personal information in emergency situations. It was also acknowledged that any provisions allowing for and regulating the collection, use and disclosure of personal information during emergencies to be included in the PPIP Act and the Health Records and Information Privacy Act 2002. Such an approach aligns to comparable provisions at the Commonwealth level that are included in Part VIA of the Privacy Act 1998 (Cth). The IPC subsequently gave in-principle support for the inclusion of emergency data-sharing provisions in NSW privacy legislation.

On 9 July 2021, an Intergovernmental Agreement on Data Sharing was agreed by National Cabinet. It is an agreement for all jurisdictions to work together to share data by default where it is safe, secure, lawful and ethical to do so.

Findings

Given the NSW Government's successful data-driven response to COVID-19, the Government should review and consider available options to enable the NSW Government to facilitate effective, efficient, and timely responses to emergency situations, including central coordination and facilitation of data sharing by the DAC.

The PPIP Act and the Health Records and Information Privacy Act 2002 should be amended to include provisions for the collection, use and disclosure of government and non-government data for emergency or natural or other disasters and hazard. A definition of emergency and/or natural or other disaster and hazard needs to be agreed in consultation with IPC, Department of Communities and Justice, Resilience NSW and other emergency services agencies.

Amending NSW privacy legislation to support data sharing in an emergency would also further support the Intergovernmental Agreement on Data Sharing.

Recommendation 3: Address data sharing needs in emergencies in NSW privacy legislation

As per the Public Health (COVID-19 Gathering Restrictions) Order 2021 (Health, 2021) which enabled the exchange of data under the Public Health Act, neither the Data Sharing Act nor the NSW privacy legislation explicitly enable the expedited sharing of personal information in response to emergencies, natural disasters and hazards to alert and protect citizens at risk. Based on advice from the Privacy Commissioner as to where the legislative change should occur, it is recommended that provisions be included in NSW privacy legislation to enable the sharing of personal information during emergencies, natural or other disasters and hazards as defined in the *State Emergency and Rescue Management Act 1989*. This is consistent with the Commonwealth Government's approach in Part VIA of the *Commonwealth Privacy Act 1998.*

This recommendation will enable the NSW Government to respond effectively, and efficiently during emergencies to better alert and protect citizens at risk.

5.6 Sharing data outside NSW Government

The Act expressly enables data sharing between NSW government sector agencies (as defined in the Act), with a particular focus on sharing with the DAC. The Act does not apply to the sharing of government sector data between a NSW agency and the agencies of other States, Territories or the Commonwealth.

What we heard

There was overwhelming support to amend the Act to enable data sharing with the Commonwealth Government and other state and territory governments. NSW Government clusters supported this change, with a number of Commonwealth and State agencies reciprocating this support.

It was acknowledged that while NSW Government agencies can already share data with other Australian governments, an express provision and a clear process for doing so will provide agencies with more confidence. Currently, there is no single formal mechanism to allow for cross-jurisdictional data sharing. Many NSW agencies rely on business specific enabling legislation or developing individual agreements to facilitate cross-jurisdictional data sharing.

The Intergovernmental Agreement on Data Sharing was agreed at National Cabinet on 9 July 2021. It is an agreement for all jurisdictions to work together to share data by default where it is safe, secure, lawful and ethical to do so.

The DAC reported interest in receiving data from the private sector and sharing it (as appropriate) across NSW Government.

Mixed views were raised about the need for the Act to enable data sharing with the private sector (i.e. NSW Government agency sharing its data with the private sector) – with little interest in the need for the Act to cover this. It was generally accepted that data sharing with other Australian governments should be treated differently to sharing with private sector because governments have a shared goal of serving the public interest, due to the crossover of service delivery and their similar data sharing legislative regimes and protections.

Findings

The Act should be amended to support and strengthen existing data sharing practices with the Commonwealth and state and territory governments. The power of this provision is setting out the clear authority for NSW Government agencies to share and being transparent about the process underpinning it. Amending the Act would support and enable consistency with the Intergovernmental Agreement on Data Sharing.

It is not recommended that data sharing between the private sector and the NSW Government be included in the Act at this stage. However, it should be clarified that data sharing under the Act enables private sector data (where provided to NSW Government agencies) to be shared within NSW Government as required. DAC confirmed that private sector data provided to the NSW Government is generally deidentified data and requires confidentiality agreements to be adhered to.

Recommendation 2: Strengthen existing cross-jurisdictional data sharing

a. Amend the Act to specifically recognise data sharing with the Commonwealth Government and other state and territory governments is lawful and possible under the Act.

b. Clarify the scope of the new provision and risk management process via policy and/or other supporting mechanisms, in line with the intergovernmental agreement on data sharing and the NSW privacy legislation. This could involve a risk management framework to agree how data sharing across jurisdictions will take place in a safe way that still supports constructive data sharing practices but doesn't compromise privacy protections or gives rise to other risks.

This recommendation will support current work underway to combine data across Australian jurisdictions to shape whole of government policy making and service delivery to improve the end-to-end customer experience.

Recommendation 10: Clarify the scope of data sharing

Clarify data sharing under the Act enables private sector data (where provided to NSW Government agencies) to be shared within NSW Government as required. This should be considered in line with contractual or equitable obligations of confidentiality or commercial-in-confidence, as well as the Act's other qualifications on an agency's ability to share data.

The intended outcome of this recommendation is to clarify the interpretation of the Act.