# Table of Contents

**Table of Contents**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting the Scene</td>
<td>2</td>
</tr>
<tr>
<td>The Public Data Policy Statement seeks to ensure the value of public</td>
<td>3</td>
</tr>
<tr>
<td>data is maximised</td>
<td></td>
</tr>
<tr>
<td>The Productivity Commission’s <em>Data Availability and Use Inquiry</em></td>
<td>3</td>
</tr>
<tr>
<td>recommended national reforms.</td>
<td></td>
</tr>
<tr>
<td>The Australian Government has committed to reforming data governance.</td>
<td>4</td>
</tr>
<tr>
<td>1. A new Data Sharing and Release Bill</td>
<td>6</td>
</tr>
<tr>
<td>The DS&amp;R Bill will be principles-based</td>
<td>6</td>
</tr>
<tr>
<td>The DS&amp;R Bill will introduce new data sharing and release arrangements.</td>
<td>6</td>
</tr>
<tr>
<td>The National Data Commissioner will oversee the data system and provide</td>
<td>7</td>
</tr>
<tr>
<td>guidance on the new arrangements.</td>
<td></td>
</tr>
<tr>
<td>We want to hear your views.</td>
<td>7</td>
</tr>
<tr>
<td>2. Key Principles of the Data Sharing and Release Bill</td>
<td>8</td>
</tr>
<tr>
<td>Safeguard data consistently and appropriately</td>
<td>8</td>
</tr>
<tr>
<td>Enhancing the integrity of the data system</td>
<td>8</td>
</tr>
<tr>
<td>Build trust in use of public sector data</td>
<td>8</td>
</tr>
<tr>
<td>Establishing institutional arrangements</td>
<td>9</td>
</tr>
<tr>
<td>Promote better sharing of public sector data</td>
<td>9</td>
</tr>
<tr>
<td>3. Scope of the Data Sharing and Release Legislation</td>
<td>10</td>
</tr>
<tr>
<td>The DS&amp;R Bill will cover a broad scope of entities and data</td>
<td>10</td>
</tr>
<tr>
<td>The Bill will provide authority for sharing and release of data where</td>
<td>10</td>
</tr>
<tr>
<td>currently prohibited</td>
<td></td>
</tr>
<tr>
<td>The Bill will interact with other legislated data safeguards</td>
<td>10</td>
</tr>
<tr>
<td>4. Streamlining Data Sharing and Release</td>
<td>12</td>
</tr>
<tr>
<td><em>Proposed process for sharing data under the DS&amp;R Bill</em></td>
<td>13</td>
</tr>
<tr>
<td>A purpose test will ensure data is shared for the right purposes</td>
<td>14</td>
</tr>
<tr>
<td>The Five-Safes framework will ensure consistent risk management</td>
<td>15</td>
</tr>
<tr>
<td>Data sharing and release as appropriate to the right users</td>
<td>16</td>
</tr>
<tr>
<td>Streamlined data sharing and release agreements</td>
<td>16</td>
</tr>
<tr>
<td>Other requirements and guidance will continue to apply</td>
<td>17</td>
</tr>
<tr>
<td>5. Roles and responsibilities within the system</td>
<td>18</td>
</tr>
<tr>
<td>Data custodians: maintain responsibility for the data they collect</td>
<td>18</td>
</tr>
<tr>
<td>Accredited Data Authorities: technical expertise which could assist</td>
<td>18</td>
</tr>
<tr>
<td>data custodians</td>
<td></td>
</tr>
<tr>
<td>Trusted users: accredited after demonstrating safeguards for data</td>
<td>19</td>
</tr>
<tr>
<td>handling</td>
<td></td>
</tr>
<tr>
<td>6. National Data Commissioner</td>
<td>20</td>
</tr>
<tr>
<td>Promoting best practice through guidance and reporting</td>
<td>20</td>
</tr>
<tr>
<td>Monitoring and oversight of the integrity of the system</td>
<td>20</td>
</tr>
<tr>
<td>Engaging with other entities and bodies</td>
<td>21</td>
</tr>
</tbody>
</table>
Setting the Scene

The Australian Government recognises that the data it holds is a strategic national resource that holds considerable value for growing the economy, improving service delivery and transforming policy outcomes for all Australians. Greater use and sharing of public data facilitates increased economic activity and improves productivity. Without improving data accessibility within government, the opportunity for enhanced productivity, increased competition, improved service delivery and research outcomes will be missed.

The Australian Government holds a large range of data about the environment, individuals and businesses, all with different attributes and different levels of sensitivity. When this data is used and combined, it provides government with new insights into important and complex policy questions and allows for improved service delivery.

Existing data sharing arrangements across the public service are complex and hinder the use of data. Barriers to greater sharing of data within government include:

- a dense web of legislative requirements which lack consistency
- a culture of risk aversion, leading to overly cautious legislative interpretation and approval process complexity, and
- lack of a whole-of-government approach.¹

New data sharing and release arrangements will benefit Australians by streamlining the way public data is shared and released within government and with trusted users. New arrangements will provide efficient, scalable and risk-based trusted data access to datasets that have substantial and community-wide benefits for research, innovation and policy. The new arrangements will increase the authorised sharing and release of data and improve data safeguards to ensure risks are managed consistently and appropriately.

This paper outlines key concepts and principles which may guide development of the new data sharing and release arrangements. While the paper includes scenarios involving more sensitive data in an effort to demonstrate how new arrangements could work, data about individuals and businesses is only one part of the data system. The concepts and principles in the paper cover all data held by the Australian Government and the proposed data sharing and release arrangements will provide a consistent and scalable framework applicable to data of all attributes and sensitivities.

Your views are sought on the issues outlined in this paper.

**The Public Data Policy Statement seeks to ensure the value of public data is maximised**

In late 2015, the Prime Minister released the Australian Government Public Data Policy Statement. This statement provides a mandate for Australian Government entities to optimise the use and reuse of public data to drive innovation across the economy. This includes mandating the release of data as open by default when it is safe to do so.

Since this Statement was released there has been a dramatic increase in the number of datasets publicly available. Data.gov.au now hosts over 29,000 data records.

**The Productivity Commission’s Data Availability and Use Inquiry recommended national reforms**

In early 2016, Treasurer Scott Morrison asked the Productivity Commission to undertake an inquiry into the benefits and costs of options for increasing the availability and improving the use of public and private sector data by individuals and organisations.

The Commission was required to:

---

¹ Productivity Commission 2017, *Data Availability and Use*, Report No. 82, Canberra
• look at the benefits and costs of making public and private datasets more available
• examine options for collection, sharing and release of data
• identify ways consumers can use and benefit from access to data, particularly data about themselves, and
• consider how to preserve individual privacy and control over data use.

The Productivity Commission undertook extensive consultation through public submissions, roundtables and public hearings to form their findings, views and recommendations. The PC received 336 public submissions during the Inquiry — 211 prior to the Draft Report and 125 in response to the Draft Report. Submissions included:
• 94 from industry associations or representative bodies
• 69 from governments or government agencies
• 59 from private sector businesses
• 58 from academics or research groups
• 38 from individuals
• 18 from not-for-profit or other non-business groups.

The PC also held separate discussions with around 130 businesses, business groups, academics, government agencies and individuals in Australia and overseas. Three roundtable discussions were held throughout the Inquiry with academics, Australia Government agencies and members of the Business Council of Australia. Two public hearings were held in November 2016.

The PC identified a “lack of trust by both data custodians and users in existing data access processes and protections and numerous hurdles to sharing and releasing data are choking the use and value of Australia’s data”, and recommended “the creation of a data sharing and release structure that indicates to all data custodians a strong and clear cultural shift towards better data use that can be dialled up for the sharing or release of higher-risk datasets”.

On 8 May 2017 the Australian Government tabled the Productivity Commission’s Data Availability and Use Inquiry (PC Inquiry). The Inquiry made 41 recommendations aimed at overcoming barriers and issues with Australia’s current data system to move from one based on risk avoidance, to one based on value, choice, transparency and confidence. The PC Inquiry recommendations balance the need for greater data access and use arrangements with proactive management of risks.

**The Australian Government has committed to reforming data governance**

On 1 May 2018, the Australian Government released its response to the PC Inquiry. The Government committed to reforming data governance within government to better realise the benefits of increased data use, while maintaining trust and confidence in the system.

To prepare its response, the Department of the Prime Minister and Cabinet consulted with:
• 78 peak industry bodies and businesses
• 15 community, consumer and civil society representatives
• 16 research sector bodies
• 43 Commonwealth public sector bodies, and
• 9 state and territory public sector bodies.

Better use of public sector data can help us improve government services for Australians and ensure our programs and policies are informed by evidence. Greater access to public sector data with a consistent approach to managing risk can improve research solutions to current and emerging social, environmental and economic issues. To unlock these benefits, the Australian Government committed to:
• Establishing a **National Data Commissioner** to implement and oversee a simpler, more efficient data sharing and release framework.
• Introducing **legislation** to improve the sharing, use and reuse of public sector data while maintaining the strong security and privacy protections the community expects.
• Introducing a **Consumer Data Right (CDR)** to allow consumers to share their transaction, usage and product data with service competitors and comparison services.

Based on the wide consultation underpinning the PC Inquiry recommendations, these reforms will increase data access and use within government and with trusted users outside government, while improving data privacy and security with strengthened and consistent safeguards.

This paper explores issues related to the implementation of data governance reforms, including the National Data Commissioner and the Data Sharing and Release legislation. The Consumer Data Right is being developed concurrently and being led by the Treasurer – see [https://treasury.gov.au/consumer-data-right/](https://treasury.gov.au/consumer-data-right/).
1. A new Data Sharing and Release Bill

This paper outlines the key principles proposed to guide the development of legislation to realise the value of public sector data and modernise the Australian Government data system. These principles build on the investment and commitments to date by the Australian Government (including those outlined in the Australian Government Public Data Policy Statement and previously published by the Australian Information Commissioner (OAIC) on open public sector information) to realise the immense value of public sector data to improve government services and policies.

The purpose of the DS&R Bill will be to streamline the process for sharing public sector data and improve data safeguards across the public service. The Bill will aim to increase authorised sharing and release of the range of data held by the Australian Government while improving data safeguards and risk management tools to create a more transparent environment for data sharing.

This paper focuses and seeks views on the development and design of a new Data Sharing and Release Bill (the DS&R Bill). The issues outlined in this paper and the proposed arrangements are based on the extensive consultation of the PC Inquiry and engagement with stakeholders.

This paper is the first step in designing and drafting new legislation. The paper does not represent official government policy but instead outlines an approach for consideration.

The DS&R Bill will be principles-based

The DS&R Bill will be based on key principles designed to move the paradigm from one which restricts access to data to one which authorises sharing and release when appropriate data safeguards are in place. The DS&R Bill will aim to promote better sharing of public sector data whilst ensuring appropriate safeguards to build trust in use of public data and maintain the integrity of the data system.

These principles recognise the different types of data held by government and the many benefits of increased data sharing for citizens. Greater sharing of the data the public sector holds can lead to:

- more efficient and effective government services for citizens
- better informed government programs and policies
- greater transparency around government activities and spending
- economic growth from innovative data use, and
- cross-sectoral research solutions to current and emerging social, environmental and economic issues.

The Bill will apply to Commonwealth entities and Commonwealth companies and include most data collected by these entities, with appropriate exceptions (see Section 3). It will provide a legislative approach to share, access and release data that is otherwise prohibited, when appropriate conditions and safeguards are met.

The DS&R Bill will introduce new data sharing and release arrangements

For data sharing and use to be authorised under the Bill, a purpose test and data safeguards need to be met (see Section 4). The Bill will authorise data sharing and release for particular purposes only, which could include:

- informing government policy making
- supporting the efficient delivery of government services or government operations
- assisting in the implementation and assessment of government policy, and
- research and development with clear and direct public benefits.
The DS&R Bill will apply appropriate and consistent safeguards to data sharing and release for these purposes. Through the internationally recognised Five-Safes disclosure risk management framework, safeguards can be dialled up or down as appropriate depending on the sensitivity of the data and whether privacy needs to be maintained (see Section 4). Consistent risk management will help prevent data misuse or unintentional disclosure and ensure data privacy and security are maintained.

The DS&R Bill will create accredited bodies within the data system, each with different roles, skills and expertise: data custodians, Accredited Data Authorities and trusted users (see Section 5). The DS&R Bill will build in accountability for these actors within the system, to ensure all take responsibility for the way data is managed and shared.

The National Data Commissioner will oversee the data system and provide guidance on the new arrangements

The DS&R Bill will outline the National Data Commissioner’s (NDC) role in implementing and overseeing a simpler, more efficient data sharing and release framework (see Section 6) including accrediting parts of the data system. The NDC’s role is to monitor and enforce the provisions of the DS&R Bill (and associated legislative instruments). The NDC will work closely with other entities, including the Office of the Australian Information Commissioner (OAIC), and be advised by a new National Data Advisory Council (NDAC).

We want to hear your views

This paper outlines an approach to the DS&R Bill which aims to balance sharing data held by government with appropriate risk management. The principles underpinning the DS&R Bill are relevant across all aspects of the possible approach outlined above.

Specific questions are posed throughout the paper to prompt your feedback and comments. Please provide your comments and feedback by 1 August 2018 to datalegislation@pmc.gov.au. All submissions will be made public unless explicitly requested otherwise.

On the basis of your feedback, the Australian Government will consider how it will approach the design and development of the DS&R Bill.

Further consultation will occur through a Privacy Impact Assessment and Exposure Draft Bill processes.
2. Key Principles of the Data Sharing and Release Bill

The DS&R Bill aims to reflect a balanced approach to realising the maximum benefits of public sector data while meeting community expectations that we handle data safely and appropriately. The Bill will seek to optimise the use and re-use of public sector data by removing inefficiencies and inconsistencies with public sector data use and sharing to increase the social and economic outcomes for all Australians.

The overall aim of the DS&R Bill will be to:

- safeguard data sharing and release in a consistent and appropriate way
- enhance the integrity of the data system
- build trust in use of public data
- establish institutional arrangements, and
- promote better sharing of public sector data.

Safeguard data consistently and appropriately

The Productivity Commission found that a risk averse culture and complex and inconsistent requirements among Australian Government agencies was a barrier to data sharing and release. Much of the Australian Government’s data is not personal or sensitive, yet current arrangements remain fragmented and prevent effective decision making on the sharing or release of this data, even within government.

To support agencies to appropriately and consistently manage data sharing and release, the DS&R Bill will provide a clear framework for public sector agencies to make informed decisions on whether or not data should be shared or released, and the appropriate conditions and risk management for their particular circumstances.

Before any data is shared or released, the DS&R Bill will require a purpose test be met, and require safeguards to be in place through the Five-Safes framework. These safeguards will need to be flexible enough to be applicable to any kind of data, yet stringent enough to ensure data security and privacy is maintained. Even data classified as personal data has differing levels of sensitivities – health data is more sensitive than data about your personal preference for transport to work – and must be dealt with flexibly in terms of facilitating its access.

Enhancing the integrity of the data system

The new legislation will set out the new NDC’s role, including their oversight and regulation of the new data sharing and release framework. Through a series of powers, including oversight, guidance and enforcement, the NDC will work with OAIC to support government agencies and drive a cultural change across the public service towards greater and appropriate use and reuse of data with consistent risk management. The NDC will also report on the state of the data system and be able to audit parts of the system to make sure data is being managed appropriately and that the rules that keep data safe are met.

Build trust in use of public sector data

Transparency and accountability will be at the core of the new legislation. The DS&R Bill aims to boost transparency and accountability in how data is shared and released, including in the decisions made when sharing or releasing data and how risks are managed by those involved. The Bill will ensure data is shared for the right purposes, with risks appropriately managed.

The Bill will impose robust and consistent accreditation requirements to ensure those using and accessing data are doing so appropriately. Entities which have strong experience in data sharing and release could be accredited as Accredited Data Authorities to aid others in sharing or releasing data to trusted users.
Establishing institutional arrangements

The DS&R Bill will establish the functions and power of the NDC and its supporting office. Technical support will be provided by the Australian Bureau of Statistics.

The National Data Commissioner will be supported by a National Data Advisory Council - made up of representatives from Government and selected experts from academia, industry and privacy groups (see Section 6). The National Data Advisory Council will provide advice on ethical data use, community expectations, technical best practice, and industry and international developments.

Promote better sharing of public sector data

The vast range of data held by Australian Government agencies is a valuable national resource that has the potential to deliver immense social and economic benefits. In line with the Australian Government Public Data Policy Statement, the DS&R Bill will help increase use and re-use of public sector data by removing inefficiencies and inconsistencies to improve social and economic outcomes for all Australians.

Australian Government data includes information about the environment, about individuals and about businesses, and when this data is used appropriately, it can provide government with new insights into important and complex policy questions and to improve service delivery. Currently, data use is fragmented and sharing of data within government is often limited by lack of authority, cultural barriers and lack of clarity in the purposes of data use and reuse. The DS&R Bill will seek to provide an alternative authority to share, access and release data that is otherwise prohibited, when appropriate conditions and safeguards are met.

Questions

1. Are these the correct factors to taken into account and to guide the legislative development?
2. What else should the Government take into consideration when designing the legislation?
3. Scope of the Data Sharing and Release Legislation

The DS&R Bill will cover a broad scope of entities and data

The new DS&R Bill will apply to all Commonwealth entities and Commonwealth companies (as defined under the *Public Governance, Performance and Accountability Act 2013*) and encompass all data collected by these government bodies for any purposes, including government administration, service delivery and research. Data collected from individuals, businesses and other entities, and data generated internally by Australian Government bodies is in scope. There will be appropriate exceptions for national security and law enforcement data. Existing contractual obligations, including around purchased datasets, will continue to apply.

The Bill will accredit trusted users and data authorities to streamline future interactions (see Section 4). As recommended by the Productivity Commission, the Bill could also enable sharing and release of Australian Government data with States and territories and non-government sectors for specified purposes and subject to certain conditions.

The Bill will provide authority for sharing and release of data where currently prohibited

While some government agencies already have appropriate mechanisms to use and share data, many do not. The Productivity Commission identified some of the cultural and legislative barriers that prevent sharing and release of data, including inconsistent approaches to data sharing and release in legislation and practice, which can lead to a risk-averse culture and inconsistent application of requirements by agencies.

The DS&R Bill is intended to provide an alternative authority to share and release data, in addition to existing authorisations, should requirements of the DS&R Bill be satisfied (see Section 4). For example, where data sharing is restricted by existing legislation the new legislation may be used to share data if conditions and safeguards are met, unless explicitly excluded. Exclusions will include national security and law enforcement data. The DS&R Bill will not by default compel all data to be shared but rather will support data custodians to make informed decisions and manage risk consistently to enable appropriate sharing and release.

There are more than 500 existing data secrecy and confidentiality provisions across more than 175 different pieces of Australian Government legislation. The vast majority of these provisions prevent sharing of data, except in specific limited circumstances. The Productivity Commission noted that ‘while some may remain valid, they are rarely reviewed or modified. Many would no longer be fit for purpose.’

The DS&R Bill will carefully consider existing secrecy provisions to balance the need to protect certain types of government data, with data sharing and release for public interest purposes.

The Bill will interact with other legislated data safeguards

This DS&R Bill will aim to facilitate the sharing and release of data while ensuring appropriate safeguards are met. The DS&R Bill will operate alongside many existing requirements for collection, storage, integration and management of data which will continue to apply.

Commonwealth entities will continue to be required to uphold the highest standards of privacy and security for the data they hold. Safeguards legislated in the DS&R Bill would exist alongside existing data safeguards in:

- the *Privacy Act 1988*
- *Privacy Amendment (Notifiable Data Breaches) Act 2017*
  - Australian Government Agencies Privacy Code
  - National Archives of Australia information management standards, and
  - Protective Security Policy Framework requirements relating to releasing classified information.
Questions

3. Should the scope be broader or narrower?
4. Are there entities that should be included or excluded from scope? How would this be justified?
5. Should any specific categories of data be specifically out of scope? How would this be justified?
6. Should exemptions, for example for national security and law enforcement, occur at the organisational level or for specific data categories?
7. Are there instances where existing secrecy provisions should prevail?
4. Streamlining Data Sharing and Release

Improving Australia’s use of data represents a key opportunity to substantially enhance national productivity. Making data more available is an achievable reform and would liberate economy-wide productivity improvements over many years.

The Australian Government has, under its Public Data Policy Statement, mandated for Australian Government entities to release non-sensitive data as open by default. Many agencies across the Commonwealth operate on this basis where they make data on issues such as biodiversity and geographical features open by default.

Government agencies already have some ways to share and release other types of data under existing frameworks and authorities. Where these arrangements are effective and efficient, they should continue to be used to derive maximum benefits for Australians.

There are instances however where these pathways are not available to those agencies wanting to share or release the data they hold. The DS&R Bill will provide a pathway for sharing and releasing data when existing avenues are not available or are complex and ineffective.

The objective of the DS&R Bill is to provide a flexible and modern framework. The starting point for the data sharing and release framework is a focus on creating incentives for self-management of risks and voluntary improvement of data management practices within public sector agencies.

The process for sharing data under the DS&R Bill is proposed below. It will support agencies to make decisions on when and how to share and release data. This process will be overseen by the National Data Commissioner and agencies will be supported to apply the framework (see Section 6).
Proposed process for sharing data under the DS&R Bill

1. Request for data to data custodian
   - Should data be open by default?*
     - Yes
       - Data custodian or ADA considers the type of data and the risks and applies the Five-Safes framework to treat risks
     - No
       - Can data be shared (easily) under existing authority?
         - Yes
           - Continue to use existing processes
         - No
           - DS&R provides an alternative authority
             - Does the use of the data meet the purpose test?
               - Yes
                 - Decision to share, with conditions outlined in Data Sharing Agreement
               - No
                 - Unable to share under DS&R
               - No
                 - The National Data Commissioner will provide oversight and guidance on implementing the Data Sharing and Release framework

2. Release
   - Data is appropriately de-identified for public release.

3. Share
   - Data is shared appropriately, having managed risks, including through bulk data transfers and access through data laboratories.

4. Deny request
   - If risks of sharing cannot be treated sufficiently, request will be denied.

* As per the Public Data Policy Statement

Five Safes framework
- Safe data: can the data disclose identity?
- Safe people: can the users be trusted?
- Safe setting: does the access environment prevent unauthorised use?
- Safe outputs: are the project results likely to disclose identity?
- Safe project: is the purpose of use appropriate?

Purpose test
- Inform Government policy making
- Support efficient Government service delivery or operations
- Assist in implementation and assessment of Government policy
- Research and development with clear and direct public benefits
A purpose test will ensure data is shared for the right purposes

The new legislation will allow data sharing and release for specific purposes only. The legislation will authorise data sharing if the data is to be used to:

1. **inform government policy making**, which could include understanding cross-portfolio impacts, identifying trends, modelling policy interventions, assessing broader system trends and evaluation to inform future policy
2. **support the efficient delivery of government services or government operations**, which could include evaluating existing programs, modelling program interventions, targeting programs based on user needs, improving services such as by pre-filling forms, administering or enforcing compliance requirements
3. **assist in the implementation and assessment of government policy**, which could include evaluation of policy and programs, analysis of policy and programs by integrating with additional data or information (e.g. analysis by location)
4. **research and development with clear and direct public benefits**, which could include research by government on a particular topic (unrelated to existing policy or programs), cross-disciplinary research, work by research institutions and academics.

Legislating a purpose test in the DS&R Bill will ensure that data is only shared for the right purposes. New South Wales, Victoria and South Australia have a similar test in their data sharing legislation.

### New South Wales’ and South Australia’s legislated purposes for data sharing

Under both the New South Wales *Data Sharing (Government Sector) Act 2015 No 60 (NSW)* s7 and South Australia’s *Public Sector (Data Sharing) Act 2016 (SA)* s8(1), data may be shared:

- a) to enable data analytics work to be carried out on the data to identify issues and solutions regarding Government policy making, program management and service planning and delivery by the government sector agencies,
- b) to enable related government sector agencies (such as branches, offices and other agencies within or otherwise related to a Public Service agency) to develop better Government policy making, program management and service planning and delivery by the agencies,
- c) such other purposes as may be prescribed by the regulations.

### Victoria’s legislated purposes for data sharing

Under the *Victorian Data Sharing Act 2017* s5, “data must only be handled under this Act for the purpose of informing government policy making, service planning and design.”

### Questions about the purpose test

8. Do you agree with the stated purposes for sharing data?
9. Are there any gaps in the purpose test that would limit the benefits of public sector data use and reuse?
10. What further detail could be included in the purpose test?
11. Should data be shared for other purposes? If so, what are those purposes?
12. Should there be scope to share data for broader, system-wide purposes?
13. Should the purpose test allow the sharing of data to administer or enforce compliance requirements?
The Five-Safes framework will ensure consistent risk management

The Australian Government holds a large range of data with different attributes and sensitivities. The DS&R Bill aims to provide a framework to appropriately manage the use, sharing and release of all data depending on the specific circumstances and context. The same risks do not apply to all data, so this Bill will aim to provide the right framework to allow flexibility for a range of risks to be managed depending on the context.

The Five-Safes framework is an internationally recognised risk management framework used widely, including by the ABS, and in the UK, New Zealand and Europe. The Five-Safes framework would apply to all data when considering appropriate sharing and release. The framework is flexible to respond to different types of data (such as personal data or environment data) and different levels of risks. Entities that want to share or release data would be required to manage the associated risks through applying appropriate disclosure risk management practices for each of the ‘safes’.

The Five-Safes framework takes a multi-dimensional approach to managing risk. Each ‘safe’ refers to an independent but related aspect of risk. The framework poses specific questions and will help assess and describe each risk aspect (or ‘safe’) in order to identify appropriate control measures prior to data sharing.

The five elements of the framework are:

- Safe data: can the data disclose identity?
- Safe people: can the users be trusted?
- Safe setting: does the access environment prevent unauthorised use?
- Safe outputs: are the project results likely to disclose identity?
- Safe project: is the purpose of use appropriate?

This framework will allow data custodians to place appropriate controls, not just on the data itself, but on the manner in which data is accessed. The Five-Safes framework is designed to facilitate safe data sharing and prevent over-regulation. The Five-Safes is compatible with the ‘reasonable steps’ requirement in the Privacy Act’s APP 11 (personal information) and the Protective Security Policy Framework (classified government information), and be used for all types of data. Guidance on Five-Safes will be developed by the NDC in consultation with relevant agencies including the Office of the Australian Information Commissioner to appropriately address privacy risks and the Australian Bureau of Statistics for technical advice.

These requirements focus on: the type of data, personnel security, physical and ICT security, access security, data standards, and destruction. The Five-Safes also contains an additional set of requirements to tailor risks according to the type of project or purpose.

Depending on the type and the sensitivity of the data to be shared, different controls or ‘safes’ will need to be applied at different levels. For example, if the data is less sensitive, it can be released to a broad range of users for a variety of purposes with fewer controls applied. On the other hand, if the data is more sensitive, or identifies individuals or businesses, the ‘safes’ need to be stringently applied, for example by data only being made available to authorised researchers in a secure access facility for specific purposes.

The Five-Safes framework further recognises that modifying the relevant data itself is only one way to manage re-identification risk, as applying controls across the environment where the data is provided can also be very effective in controlling the risk of re-identification. For example, agencies may be able to provide access to sensitive data in a secure environment, such as virtual laboratories with controlled outputs to manage this risk.

For more information, see the Five-Safes in practice on the ABS website.
Questions about data safeguards

14. Is the Five-Safes framework the appropriate mechanism to ensure data is safeguarded?
15. Are there any additional safeguards that should be applied?
16. Are there any instances when the Five-Safes could not be applied?
17. Is the Five-Safes appropriate when data is shared and used for the specific purposes in the purpose test above?
18. How should the responsibility for managing risks be shared in the framework?
19. How would you envisage Five-Safes principles be applied over the life-cycle of data to ensure data safeguards are continually met?
20. Under what circumstances should trusted users be able to access sensitive data?

Data sharing and release as appropriate to the right users

After applying the purpose test and Five-Safes framework, the data custodian will make a decision on whether to release or share the data, or to deny the request:

- Public release of data may occur when data is appropriately de-identified.
- Data may be shared appropriately if risks are able to be managed, including through data transfers and access through secure data laboratories.
- Request for access to data can be denied if risks of sharing cannot be addressed sufficiently.

Streamlined data sharing and release agreements

In March 2016, the Government released its Guidance on Data Sharing for Australian Government Entities to streamline data sharing arrangements and improve decision making for policy and implementation processes. It recognised that existing arrangements through Memoranda of Understanding (MoUs) are unnecessarily complicated, time consuming and do not add value in return, and recommended entities use simplified written agreements to facilitate sharing.

The DS&R Bill will require data sharing arrangements between agencies and users to be detailed in data sharing agreements to ensure data is shared under conditions identified through the Five-Safes framework. Through a simplified and streamlined approach, the data sharing agreement will make clear the rights, responsibilities and safeguards for data sharing between the data custodian and the trusted user. The New Zealand Privacy Act (1993) and the South Australian Public Sector (Data Sharing) Act (2016) provide for data sharing agreements in a similar way.

Data sharing agreements could record information on:

- what data is being shared
- how the purpose test is being met, and
- how disclosure risk management practices are applied.

These agreements may cover similar aspects to Memoranda of Understanding, but in a way that is simpler, streamlined and consistent. The National Data Commissioner would provide templates and guidance on the required form and content of data sharing agreements to ensure consistency and ease.

The DS&R Bill would provide for data sharing agreements to be publicly available, unless publishing them would pose personal and national security risks, or be in breach of commercial-in-confidence claims. This could also aid discovery of the datasets agencies hold that users may request.
Questions about public sector data sharing arrangements

21. Would this arrangement overcome existing barriers to data sharing and release?
22. Would streamlined and template agreements improve the process?
23. Do you agree that data sharing agreements should be made public by default?
24. What level of detail should be published?
25. What else should a data sharing agreement contain?
26. What other transparency mechanisms could be mandated?

Other requirements and guidance will continue to apply

The DS&R Bill aims to provide authority to share and release data if the right purpose and conditions are met. The DS&R framework will not govern the collection or management of data other than for the purposes of sharing and release and would exist alongside existing data safeguards in the Privacy Act 1988, Privacy Amendment (Notifyable Data Breaches) Act 2017 and Archives Act 1983.

The DS&R Act would not govern arrangements in existing sharing arrangements or existing sharing agreements, which would continue to operate until they expire.

As outlined in Section 6, the NDC may provide guidance on the application of these arrangements, in consultation as appropriate with the Information and Privacy Commissioners. NDC could also provide additional guidance to build on the ‘Process for Publishing Sensitive Unit Record Level Public Data as Open Data’ to assist agencies share sensitive data safely.

Existing guidance will continue to apply, including the OAIC and CSIRO’s Data 61 De-Identification Decision-Making Framework, which allows for consideration of environment-based and data-based controls to be based on the Five-Safes framework after completing the De-Identification Decision-Making Framework.
5. Roles and responsibilities within the system

The DS&R Bill will provide for accredited bodies and entities within the data system, each with different roles, skills and expertise. The DS&R Bill will build in accountability for everyone within the system to ensure responsibility for the way data is managed and shared. The DS&R Bill would require agencies to report on decisions in relation to the release of data, similar to provisions in the Freedom of Information Act.

Data custodians: maintain responsibility for the data they collect

Data custodians are Commonwealth entities and Commonwealth companies (as defined under the Public Governance, Performance and Accountability Act 2013) who collect data for any purpose. They are responsible for collecting and managing this data under existing requirements. For the purpose of the new DS&R Bill, data custodians will be responsible for applying the principles and requirements of the DS&R Bill to share and release data appropriately. Data custodians will be responsible for assessing requests for access to data under the DS&R Bill including:

- assessing the request in line with the purpose test
- applying the Five-Safes framework to determine the appropriate controls and conditions for sharing or release
- entering into data sharing agreements as needed with trusted users, and
- sharing or releasing the data to the trusted user in line with the agreement.

The role of data custodian would be performed by the head of an organisation or agency. However, individual organisations may choose to delegate the role of data custodian to individuals or positions within their agency as specific custodian for particular datasets. These decisions will be at the discretion of agencies.

The sharing of data is at the discretion of the data custodians. The NDC will provide guidance to assist and empower data custodians to make decisions and apply the DS&R framework.

Data custodians may choose to outsource the management of data requests to an Accredited Data Authority (ADA) and authorise the ADA to manage all or some steps of the sharing or release request on their behalf.

Accredited Data Authorities: technical expertise which could assist data custodians

The PC Inquiry recommended a new intermediary in the form of an accredited body that has the necessary skills and knowledge to integrate, share and release datasets safely under the DS&R legislation and Five-Safes Framework.

Entities which have strong experience in data curation, collation, linkage, de-identification, sharing and release (for example Australian Bureau of Statistics (ABS), Australian Institute of Health and Welfare (AIHW)), could be accredited as Accredited Data Authorities (ADAs). Criteria and process for accreditation would be developed by the NDC and could build on requirements for accrediting Integrating Authorities.

Data custodians could provide data to an ADA to perform advanced data services to ensure data sharing and release is managed in accordance with the DS&R Bill requirements, including:

- improving the quality of the data (by cleaning or curating the data)
- de-identifying the data
- linking or combining datasets, or
- safely releasing or providing access to datasets.

Data custodians could authorise the accredited data authorities to on-share data in accordance with the DS&R Bill and data sharing agreement requirements.
Any charging associated with this work would need to be consistent with the Australian Government Charging Framework. This would involve understanding the cost of these services and making an informed policy decision on the price.

**Trusted users: accredited after demonstrating safeguards for data handling**

Trusted users are the end-users of data shared or released by data custodians. To streamline data sharing arrangements, trusted users would be accredited by demonstrating they can safely use and handle data under the requirements of the DS&R Bill, including the Five-Safes framework.

Accreditation criteria and processes would be established by the NDC. Trusted users who are employees or contractors of Government entities and companies, as well as external users, could seek accreditation in line with the scope of the DS&R Bill.

There will be long term strategic benefits from data custodians engaging with accredited data trusted users, including specifying particular individuals within entities who can demonstrate the ‘safe people’ criteria in Five-Safes framework. Accreditation would also reduce the onus on the trusted users to continually demonstrate their ability to meet the Five Safes Framework, and provide for quicker access to public sector datasets.

Accreditation would need to be maintained and could be audited by the NDC.

**Questions**

27. How long should accreditation as an ADA or Trusted user last?
28. What could the criteria for accreditation be?
29. Should there be review rights for accreditation?
30. Should fees be payable to become accredited?
31. Is the Australian Government Charging Framework fit for purpose in this context?
6. National Data Commissioner

The National Data Commissioner (NDC) will champion greater data sharing and release by providing consistent leadership and well-defined technical direction for implementing reforms to Australia’s data system.

The DS&R Bill will set out the NDC’s role in the Australian national data sharing and release framework and its role to monitor and enforce the provisions of the DS&R Bill (and associated legislative instruments). The NDC will oversee and regulate the DS&R Bill, while working to empower public sector agencies to share and release data in line with the provisions in the Bill.

**Promoting best practice through guidance and reporting**

The NDC will promote best practice by issuing guidance on how the data sharing and release framework will operate, including how to proactively manage whole-of-government risks of public sector data use. This guidance will draw from and complement guidance issued by other bodies (such as the ABS, AIHW, DTA, Finance, NAA or OAIC). Guidance will be updated as required to deal with changes in data practice and risk.

Guidance could include topics such as:

- handling data requests, including rights and responsibilities
- required content and form of data sharing agreements
- public reporting of data sharing agreements once made
- prevention and management of data breaches (in consultation with the Office of the Australian Information Commissioner)
- emerging risks and opportunities in data use
- accreditation of Data Authorities
- accreditation of trusted users
- application of purpose test
- application of Five-Safes framework.

The National Data Commissioner will work with agencies to support and ensure the appropriate use of the DS&R Bill, including to increase the sharing and use of data within government. The NDC could provide statistics or reports on the data system, and on progress in sharing and release of data through the DS&R Bill, against set metrics and key performance indicators. These reports could include such matters as:

- Agencies’ progress in sharing and release of data
- ‘Good news stories’ on beneficial uses of data
- Non-compliance with the DS&R Bill, and
- Lessons learned around data sharing and release.

**Monitoring and oversight of the integrity of the system**

The DS&R Bill will take a multi-tiered approach to compliance and enforcement. For individuals and businesses to be assured that their data is being appropriately protected, the DS&R Bill could include consequences for non-compliance with the framework, to be overseen and enforced by the NDC.

To ensure accountability and integrity of the system, the NDC will have the power to monitor compliance by conducting audits, making inquiries and monitoring and investigating conduct under the DS&R Bill. The NDC will also audit accreditation processes for both Accredited Data Authorities and trusted users.
The Productivity Commission strongly counselled against recreating a ‘strict criminal liability culture’ because it would de-incentivise data sharing, and openness about any breaches. The DS&R Bill will give the NDC powers to penalise non-compliance, such as intentional misuse of data. Consequences for non-compliance would balance the need to authorise and encourage agencies to share or release data while at the same time ensuring a sufficient deterrent for misuse of data. Determining appropriate consequences will depend on the extent of the non-compliance and will be scaled in proportion to the sensitivity of data and the type of non-compliance. The public need reassurance that government data will be handled appropriately.

Non-compliance may include, for example, where sharing or release of data does not meet the purpose test, or where data is used or shared in breach of the terms of the data sharing agreement, or if the application of the Five-safes framework is inappropriate.

Determining appropriate consequences would depend on the extent of the non-compliance and if it was intentional or not. Application of consequences, including any enforceable undertakings or penalties, could be scaled in proportion to the sensitivity of data and the type of non-compliance. Actions that could be taken for non-compliance could include withdrawal of accreditation or access to data or entering into enforceable undertakings. Individuals and agencies could be liable for any unauthorised sharing or release of data, with both civil and criminal penalties for unauthorised access to, use of, or sharing or release of data.

Data custodians who release data under the DS&R Bill defensibly in good faith would benefit from an immunity so they are not criminally liable. The immunity could apply provided the data custodians act in good faith with a genuine belief that disclosure is required or permitted under the DS&R Bill. A similar immunity exists in the Freedom of Information Act 1982.

Engaging with other entities and bodies

The National Data Commissioner will engage widely, including establishing, and consulting with, a National Data Advisory Council. Ongoing dialogue with the public, business and public service will build trust in how data is being shared and released by agencies.

The new National Data Advisory Council will comprise key representatives from Government, such as the Australian Statistician and the Privacy Commissioner, and experts from academia, industry and privacy groups with a strong understanding of Australia’s data landscape. The Council will advise the National Data Commissioner on ethical data use, social licence and building trust, ethical best practice, and industry and international developments.

The NDC’s role will complement the roles of other statutory officers, like the Australian Statistician and the Australian Information Commissioner. The Office of the NDC will work alongside the national privacy regulator, the Office of the Australian Information Commissioner, to ensure that Australia’s data sharing and release framework is underpinned by a strong foundation of privacy and security.

The Office of the NDC will work with the Office of the Australian Information Commissioner on a range of key topics including data management, de-identification, data security, data breaches, the general handling of personal information and information management.

The ABS will provide technical guidance and support to the NDC. The ABS has extensive experience in data collection, processing, quality assurance, de-identification, and safe release for statistical and research purposes. The ABS will assist the NDC in issuing technical guidance on matters such as data governance, management standards, registers, security, de-identification practices, metadata, use and curation of data, and managing acquisition of private sector datasets. The ABS will draw on expertise from others including Data61 and the AIHW.

The NDC will complement the role of the Digital Transformation Agency, which advises government about digital service delivery shared platforms and digital skills capability across government, and

---

2 Productivity Commission 2017, Data Availability and Use, Report No. 82, Canberra, Pg 329
the National Archives of Australia, which has responsibility for setting information and records management requirements for government records.

Questions

32. Are these the right functions for the National Data Commissioner?
33. What review powers should the National Data Commissioner have?
34. Should the NDC have the power to conduct an investigation into system-wide issues?
35. What other actions could the NDC be able to take?
36. Are there other ways community values and expectations can be captured and addressed?
37. What aspects should be taken into consideration when considering consequences for non-compliance with the DS&R Bill?
38. Should the consequences differ depending on the type of data involved or the type of misuse, e.g. harsher penalties for intentional misuse?
39. Should penalties be strict liabilities?
40. What would be an appropriate penalty for intentional misuse of data?
41. How would responsibility for misuse of data be shared across the data system?
42. To what extent should there be a complaints mechanism and how should it work?
43. Should a complaints mechanism provide for complaints by the public?