



Australian Government

Department of the Prime Minister and Cabinet

# DATA SHARING AND RELEASE

LEGISLATIVE REFORMS  
DISCUSSION PAPER

September 2019

## **Data Sharing and Release Legislative Reforms Discussion Paper**

© Commonwealth of Australia 2019

### **Copyright Notice**

With the exception of the Commonwealth Coat of Arms, this work is licensed under a Creative Commons Attribution 4.0 International licence (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/>).



### **Third party copyright**

Wherever a third party holds copyright in this material, the copyright remains with that party. Their permission may be required to use the material. Please contact them directly.

### **Attribution**

This publication should be attributed as follows:

© Commonwealth of Australia, Department of the Prime Minister and Cabinet, *Data Sharing and Release Legislative Reforms Discussion Paper*

### **Use of the Coat of Arms**

The terms under which the Coat of Arms can be used are detailed on the following website:

<https://www.pmc.gov.au/government/commonwealth-coat-arms>

### **Other uses**

Enquiries regarding this document are welcome at: [datalegislation@pmc.gov.au](mailto:datalegislation@pmc.gov.au)

# MINISTER'S FOREWORD



Whether it is claiming a Medicare rebate, having a passport checked before an overseas trip, lodging a tax return or simply looking at the weather forecast, every day millions of Australians rely on services delivered by the Australian Government.

Australians expect government services to be seamless, easy and fast—just like their normal experience of shopping and banking. This fuels the need for the government to keep pace with the private sector—and aspire to be a market leader—when it comes to delivering services for Australian people and businesses.

The Morrison Government is committed to making it easier and faster for Australians to access the services they need by ensuring people and businesses are at the very heart of service design and delivery.

As the Minister responsible for the National Disability Insurance Scheme and Government Services, I have been talking with people right across Australia about how even the smallest improvement to government services can have a big impact on people's lives. Improvements such as fewer questions on an aged care form, making it easier to report income online, or even a single, clear point of access—such as an app on your phone—can all have an immediate and lasting positive impact.

We can and will do more for improving people's experience when dealing with government—and data plays an important role in achieving this goal. The government already holds significant amounts of public data collected as part of our everyday work delivering services to Australians. Government, in many respects, is the custodian of Australia's data and this data is already being used to inform policy development and the delivery of services—yet much more can be done with this truly national asset.

Through better use and sharing of public data across government, Australians will no longer have to tell us the same basic information over and over again, and we will be able to create a connected and seamless user experience for those accessing government services. Additionally, Australia's research sector will be able to use public data to improve the development of solutions to public problems and to test which programs are delivering as intended—and which ones are not.

The sharing of public data has incredible potential at both the national level and at the individual level, but it must be done prudently and safely. Maintaining trust with the Australian community is fundamental to realising the full potential of this national asset. That is why the Government will ensure any public data sharing arrangements are underpinned by enhanced safeguards, privacy and security protections.

The Australian Government is developing new public sector data sharing and release legislation that will enshrine these protections, along with a clear, consistent and transparent approach to the sharing of public data. It is crucial we get the legislation right—which is why feedback on our approach is so important.

This Discussion Paper acknowledges the feedback and perspectives we have heard so far during the extensive engagement undertaken with privacy experts, researchers, legal experts, businesses and all levels of government over the past 12 months. I would like to thank all who have worked with us to identify concerns and opportunities, and for providing valuable advice and insights into how public sector data can help solve problems of national and individual significance.

We will continue to engage with you and the broader community as we work our way through the development of the new legislation and how we deliver not just better services, but also a better experience for Australian people and businesses.

I encourage you to read the Discussion Paper and generously contribute your time, ideas and feedback so we can ensure we make the most of this important national asset to benefit all Australians.

A handwritten signature in black ink, reading "Stuart Robert". The signature is written in a cursive, flowing style.

**The Hon Stuart Robert MP**

Minister for the National Disability Insurance Scheme  
Minister for Government Services

# CONTENTS

1. Setting the Scene: Australia's data reform agenda	1
2. Data Sharing and Release framework	13
3. Sharing data for public benefit	21
4. Strengthening safeguards	29
5. Building trust through transparency	35
6. The National Data Commissioner's oversight of the data system	39
7. When things go wrong	47
8. What's the plan from here?	53
Attachments	55



**As a national  
resource, public  
sector data benefits  
all Australians.**

# 1. SETTING THE SCENE: AUSTRALIA'S DATA REFORM AGENDA

**The Australian Government is committed to modernising how public sector data is used. It is working to unlock its potential safely and in line with community expectations.<sup>1</sup> As a national resource, public sector data can benefit all Australians through better and more targeted government policies, programs and service delivery, and improved research to address real problems.**

In 2016, the Government asked the Productivity Commission to look at how data was used across the Australian economy. The Productivity Commission found Australia's use of data was falling behind other countries and recommended data reforms to unlock the full potential of public sector data. The Government is currently implementing the recommendations, including legislative reforms discussed in this paper.

In 2018, the Office of the National Data Commissioner was established within the Department of the Prime Minister and Cabinet to improve data sharing and use across the Australian public sector. The interim National Data Commissioner, Ms Deborah Anton, was appointed to oversee the development of new legislation to support these data reforms.

While the government currently shares data for a range of important and valuable projects, establishing these sharing arrangements involved onerous legal negotiations and resulted in inconsistent safeguards and standards. The new legislation, with a working title of Data Sharing and Release legislation, fulfils the needs of Australians to receive better public services, policies and research outcomes driven by transparency and accountability in the system.

The new legislation will empower government agencies to safely share public sector data with trusted users for specified purposes. Its aim is to streamline and modernise data sharing, overcoming complex legislative barriers and outdated secrecy provisions. The legislation will also allow government agencies to draw on expert advice to assist them to share data safely using contemporary tools and techniques.

## CONSUMER DATA RIGHT

The Australian Government has separately established a Consumer Data Right to unlock data held by the private sector to drive greater competition and give consumers greater control and use of their own data, such as bank accounts. The Consumer Data Right and the Data Sharing and Release legislation are both part of the government's efforts to reform Australia's data legislation. While the Consumer Data Right relates to private sector data, the Data Sharing and Release legislation is focused on government-held data. Both pieces of legislation will be principles-based, allowing them to adapt as the technological and legal environment evolves.<sup>2</sup>

<sup>1</sup> The Australian Government's response to the Productivity Commission Data Availability and Use Inquiry, 1 May 2018, available at <https://dataavailability.pmc.gov.au/>.

<sup>2</sup> For more information on the Consumer Data Right, see <https://treasury.gov.au/consumer-data-right>.



## 1.1 A conversation about data reform: from Issues Paper to Discussion Paper

On 4 July 2018, the Australian Government invited public comments on an Issues Paper outlining the proposed Data Sharing and Release legislation. We received 108 submissions that drew insights from the public, private and not-for-profit sectors and from individuals.<sup>3</sup> We have since explored, tested and asked questions about those insights in over 50 half-day roundtable discussions across all Australian capital cities with interested stakeholders as well as bilateral discussions. This Discussion Paper is the next step on an iterative journey towards reforming the way public sector data is shared and used. For an overview of how our thinking has evolved since the Issues Paper including what we have done to address feedback, see Attachment B. We will listen, learn and improve our policy positions as a result of your feedback on this Discussion Paper.

This Discussion Paper presents the valuable insights we have heard and highlights concerns expressed about data sharing. We also discuss examples where the legislation may be able to help the public with government services. We want to hear whether these examples resonate with the public, and whether they are considered reasonable and beneficial objectives for the Australian community. We invite your contributions to help us continue to refine the new legislative framework to make sure we have the balance right.

## 1.2 Talking the same language: data sharing and data release

The data world can be confusing, filled with complicated and often conflicting terminology. To make sure we are on the same page, it is important to define the terms as we use them in this Discussion Paper and in the upcoming legislation.

### WHAT IS PUBLIC SECTOR DATA?

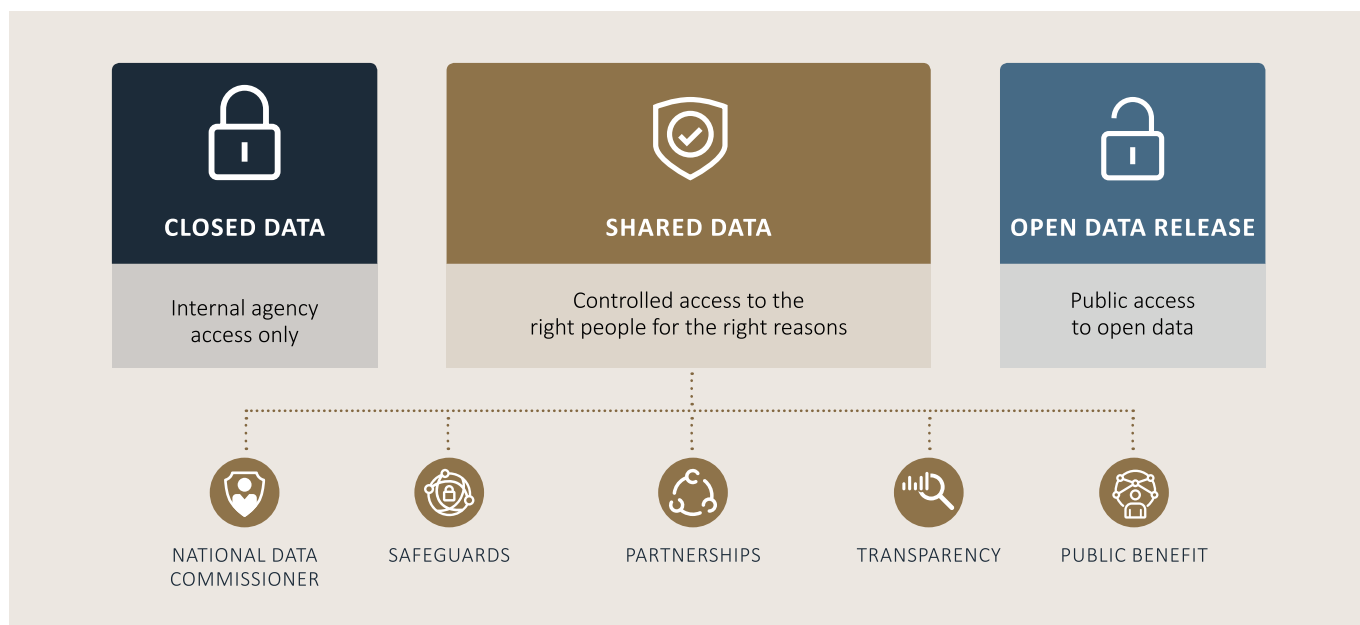
**Public sector data** is data held by the Australian government as it fulfils its various functions. Government agencies collect, hold and use data on topics as diverse as weather patterns, who is coming and going from Australia, and administrative data about access to government services by both businesses and individuals.

**Data** means any facts, statistics, instructions, concepts, or other information in a form capable of being communicated, analysed or processed (whether by an individual or by other means including a computer, electronic and automated means). Data can exist at different levels of detail, including aggregated to the category or population or at the more detailed unit record.

<sup>3</sup> Issues Paper and public submissions are available at <https://www.pmc.gov.au/resource-centre/public-data/issues-paper-data-sharing-release-legislation>



**Figure 1:** Data Sharing and Release legislation focuses on shared data



Until now, the public conversation in Australia has mainly been a binary one of open or closed data. Government agencies either kept data in-house or made it publicly available through data.gov.au or other websites. Open data release fuels curiosity, benefits the economy and leads to new and innovative uses of data. It must address privacy and security risks — once released, data cannot be retracted or protected against future uses and misuses. Closed data protects privacy, but carries the risk that research does not use the best information, government policies are not targeted where they are most needed, and citizens find it difficult and annoying to access government services. Closed data also keeps the Australian public in the dark about what government does with the data it collects and holds (see Figure 1).

The binary approach of closed or open data misses the opportunities data sharing can provide in between, which is the focus of the Data Sharing and Release legislation. Our approach recognises that government agencies can share information with the right users for the right purpose and be assured safeguards are applied. We think government agencies should be able to share information safely and consistently for the benefit of all Australians.

---

### THE BINARY OF CLOSED OR OPEN DATA MISSES THE OPPORTUNITIES DATA SHARING CAN PROVIDE IN BETWEEN, WHICH IS THE FOCUS OF THE DATA SHARING AND RELEASE LEGISLATION.

---

We need to make a distinction between data *sharing* and open data *release*. By data *sharing*, we mean providing controlled access to the right people for the right reasons with safeguards in place. By data *release*, we mean open data that is made available to the world at large.

The Data Sharing and Release legislation will provide legal grounds to empower the government to share public sector data for specified purposes with the right safeguards. The open data agenda is already supported by a range of legal mechanisms, but government agencies need support to understand and use them. The National Data Commissioner will work with other government agencies and regulators, including the Australian Information and Privacy Commissioner, to improve guidance on using existing mechanisms to release open data.

## 1.3 What are we trying to achieve?

We want to make the best possible use of public sector data. There are many benefits that will flow from this legislation, including better service delivery, transparency, research and public administration.



The Australian public will benefit directly from the legislation through improved service delivery, including:

- Tell Us Once: the legislation will allow you, to easily and quickly tell government agencies only once about a change in your details, for example your address, saving time and expense for both you and for government.
- Pre-filling forms: simplifying how citizens fill in forms by pre-filling them with information already provided to the government, similar to the way myTax works.



For Australia's government and the citizens it serves, this legislation will improve public administration by:

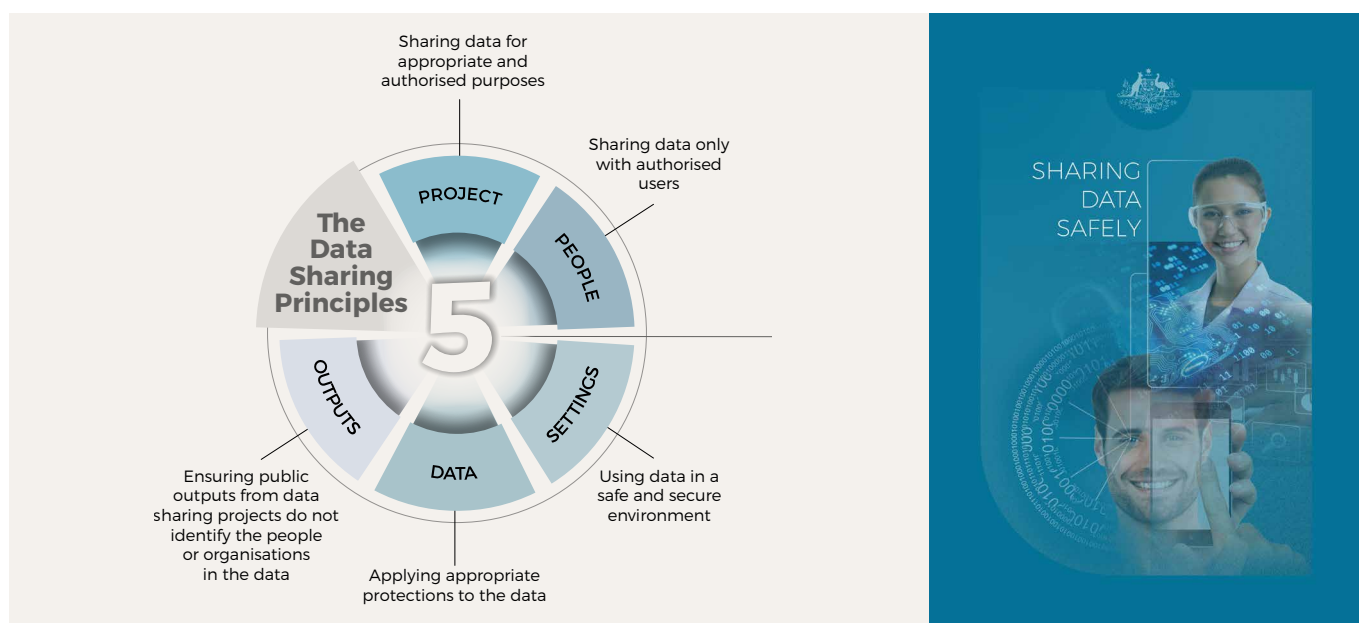
- Reducing over-collection of data across the public sector by sharing existing data across government agencies and reducing the collection burden on individuals. For example, if you report your circumstances to one government agency to receive a service, you would not need to provide the same information again to another government agency to receive other services.
- Increasing the transparency of government operations around the use of public sector data, which improves the community's trust in the government's handling of data.
- Minimising the risk of data breaches and the burden of storing duplicate datasets, by allowing government agencies to draw on datasets held by a collecting agency in a federated model, rather than holding multiple versions in each agency.
- Improving the way the Australian government makes public policy. For example, by combining information collected by the government and universities to improve education services
- Investing in the quality of public sector data, including using expert services.



For Australia's research sector, the legislation will provide access to data to advance knowledge and create better public policy, by:

- Improving capability and the quality of research outcomes from Australia's universities and research institutions.
- Providing trusted researchers with the opportunity to more accurately evaluate the effectiveness of government policies and programs.
- Strengthening cooperation between the Australian government and researchers, leading to more robust outputs tested by leading experts.

**Figure 2:** The Data Sharing Principles are part of a risk management framework to share data safely



We have heard there is public support for these objectives and that many in the community already expect the government to do these things. Public sector data is a valuable resource that should be used to address the growing needs and expectations of the community.

To achieve these objectives, we need to get the framework right. It is currently possible to achieve some of these outcomes, but it can take years to overcome legal, cultural, technical and capability obstacles. We are hoping to shift thinking about data sharing from *'can I share?'* to *'how can I safely share?'* We are laying the groundwork for that change by giving government agencies a clear legal authority to share provided that they apply the Data Sharing Principles<sup>4</sup>—focusing them on achieving best practice data sharing rather than just legally compliant data sharing. See Figure 2 and Section 4.2 for an overview of the Data Sharing Principles that set out requirements for safe sharing under this legislation.

The Data Sharing and Release legislation will provide a holistic risk management framework for data sharing, with the National Data Commissioner as a central trusted authority to provide advice and guidance on the framework.

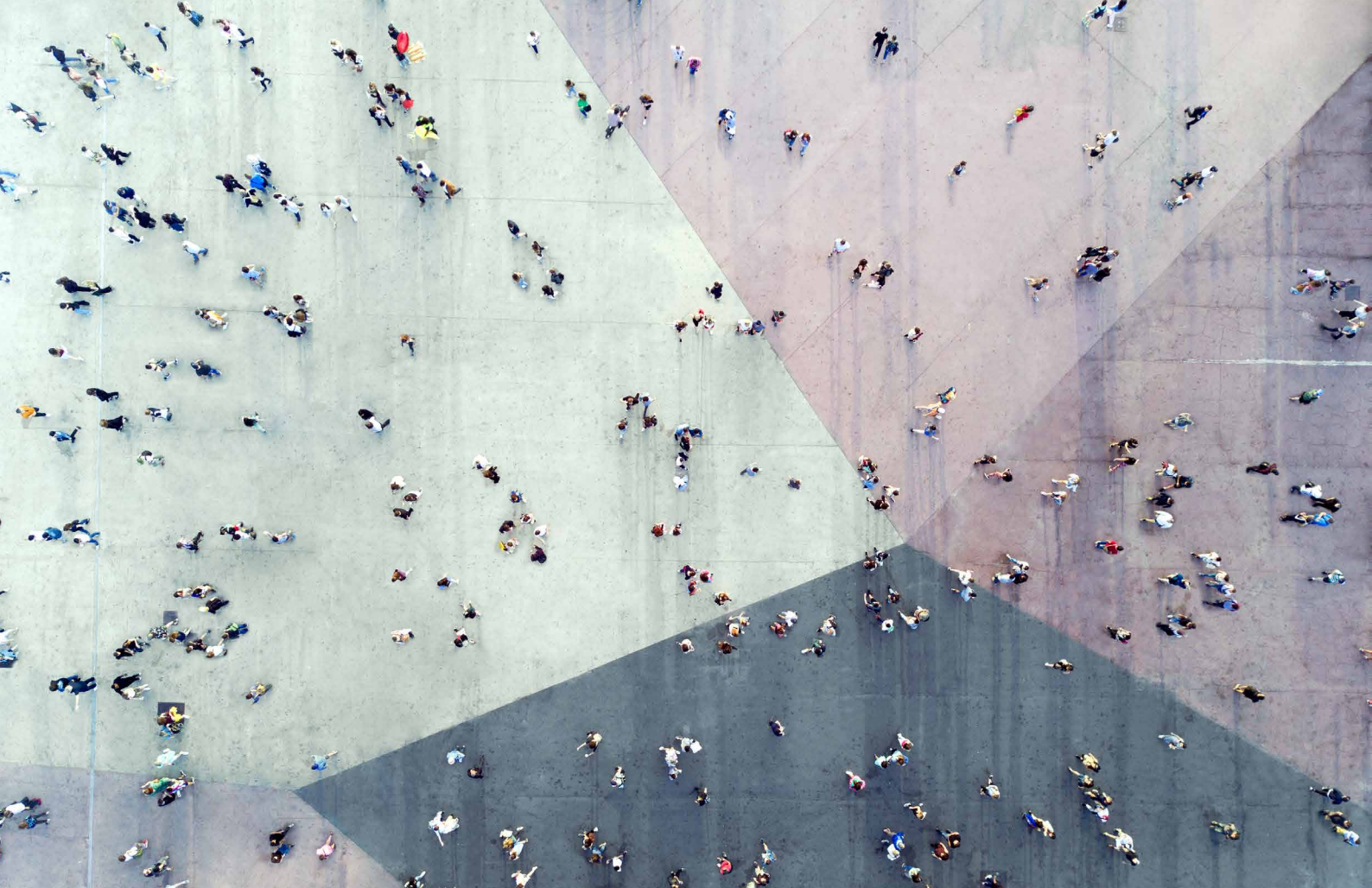
## 1.4 What have we heard so far?

We have asked lots of questions and have heard a range of issues, concerns and solutions. The story that emerges, as you will see from the detail below, is a positive and constructive debate focused not only on the benefits but also the risks. Ultimately, there is considerable support for progressing this public conversation about data use and re-use and creating a new regulatory framework to enable data to have a more significant role in supporting our future. Attachment B provides a summary of the evolution of policy based on your feedback.

### Strong support for a National Data Commissioner

We heard strong support for the establishment of a National Data Commissioner as an independent authority with oversight of the new data sharing system. A Commissioner was seen as playing an important dual role: championing greater data sharing while promoting safe data sharing practices. We heard the Commissioner should be empowered to apply strong penalties to intentional or negligent misuse and should cooperate with other regulators, including the Australian Information and Privacy Commissioner.

<sup>4</sup> The Data Sharing Principles is a risk management framework that builds on the best practice to manage safe access to data. See <https://pmc.gov.au/sites/default/files/publications/sharing-data-safety-brochure-march-2019.pdf>



### **Competing views on the benefits and risks of the legislation**

There were divergent views on the balance of benefits and risks of sharing and release of public sector data. For example, while understanding the importance of privacy, the research community highlighted the enormous benefits that come from providing them with controlled access to rich and detailed public sector data: developing life-saving research, testing the outcomes of public policy programs and government policies and improving the accuracy of data. On the other hand, privacy stakeholders point to the risks of eroding individuals' privacy, the importance of protecting the personal information government collects compulsorily, and the expectation that government be accountable and transparent in its data use.

### **The research sector is a vital part of the data system**

University researchers have formed one of the main groups who have engaged with us. We have heard about the opportunities for them to do more to improve policies and programs by having better access to government data. Researchers pointed to their ability to help fill government capability gaps, using their expertise to help solve intractable problems which will lead to better outcomes for all Australians. Researchers supported a data sharing system actively encouraging and enabling collaboration with researchers. There was support for building on the good work of some government agencies, including the Australian Bureau of Statistics and Australian Institute of Health and Welfare, who were seen to be taking important steps towards making data available to researchers in a safe and effective manner. The non-government sector also pointed to socially valuable research which could be enabled by providing their researchers with better access to data.



## Concerns about the legislation overriding existing data secrecy provisions

Some are concerned the legislation could provide a blanket override of secrecy provisions without fully appreciating the need for secrecy provisions on a case by case basis. This concern was repeated in feedback on our Issues Paper as well as contributions through forums and one-on-one discussions with stakeholders. We also heard the other side of this: the research sector is concerned secrecy provisions are used by the Australian Public Service to indiscriminately lock up data, restricting uses in the public interest. The research sector was also concerned that data sharing agreements could be used to unfairly shift the burden of responsibility onto the recipients of data, rather than responsibility being shared. These remain serious concerns we must approach cautiously. The National Data Commissioner's role to monitor and identify systemic barriers to greater sharing of data will be a measured approach to drive a culture of openness and transparency.

## Concerns about privacy and interactions with existing mechanisms

We heard broad support for cooperation between the Australian Information and Privacy Commissioner and the National Data Commissioner to address the 'grey areas' between freedom of information, privacy and data sharing laws. We heard support for the Australian Information and Privacy Commissioner's membership on the National Data Advisory Council. Stakeholders warned against duplication of roles with existing regulators and asked for consistent definitions to reduce possible confusion with the *Privacy Act 1988*. There were also frequent and recurring debates about de-identification and the difficulty of ensuring information is appropriately de-identified, leading some to suggest the term be retired entirely.

## Competing views on consent

There were robust discussions and debate in roundtables about consent. Views ranged widely and often expanded into debates about the role of consent in general (beyond just data sharing) and international developments.<sup>5</sup> The benefits of consent were highlighted: giving individuals control of data and how it is used, as well as greater visibility and transparency. Many participants noted the inherent complexities of consent: what constitutes consent, when does the wider societal benefit outweigh the individual's right to consent, and whether it is reasonable to place the burden on individuals to read long privacy policies or if the government should regulate to a higher privacy standard. Particular to our system, many warned that a consent model could create biases in data and result in the allocation of government services to where citizens who had consented rather than to citizens in greatest need.

Many supported efforts to progress the public conversation around consent, especially with the rise of different international approaches. In the context of the Data Sharing and Release legislation, we heard that it was important we be clear on how consent is understood and integrated into our scheme to ensure the public is not taken by surprise. Some discussed other schemes that did not use a consent model but were accepted by the public, such as the health research consent waiver in the *Privacy Act 1988*, and the role of ethics processes in those schemes, including the National Health and Medical Research Council (see Section 4.6 for a longer discussion of consent).

## A considered approach to Indigenous data is important

We heard the need to pay close attention to matters related to Indigenous data. We heard concerns relating to Indigenous access to Indigenous data and Indigenous data sovereignty. The National Indigenous Australians Agency is in the early stages of developing a more effective approach to Indigenous data, including a possible whole-of-government Indigenous data strategy, and we are working together to get it right.

---

<sup>5</sup> Including issues raised by the ACCC Digital Platforms inquiry. <https://www.accc.gov.au/focus-areas/inquiries/digital-platforms-inquiry>

## Concerns about the purposes for sharing data

The purposes for which data should be shared under the legislation have been a critical and contentious area of discussion. The Issues Paper invited feedback on the idea of sharing and release of public sector data for broad purposes, including compliance. Some criticised the purposes proposed in the Issues Paper as too broad, while others were concerned they were too restrictive. In general, the feedback showed a consensus around use of public sector data for improving policy, program evaluation, service delivery and research and development.

Opinions were most divided in relation to compliance and commercial purposes. While compliance is seen as a legitimate function of government, we heard the importance of ethical oversight, transparency and accountability and redress mechanisms to handle when things go wrong. Similarly, while sharing data with the private sector can contribute to a more efficient economy, there are clear limitations on what the public consider fair and reasonable. For more detail on why we precluded compliance and our current thinking on commercial uses see Section 3.3.

## Need for guidance to ensure consistent application

The Issues Paper discussed the Data Sharing and Release legislation using safeguards modelled on the Five-Safes Framework.<sup>6</sup> We heard strong support for using international best practice to safely share data, however, there was apprehension about the word ‘safe’ as it implied risks could be made completely safe. Legal and privacy experts were concerned the Five-Safes were not privacy safeguards and privacy should be specifically addressed in legislation. We heard this feedback and remodeled the Five-Safes as the Data Sharing Principles.

In partnership with the Australian Bureau of Statistics we released the *Best Practice Guide to Applying Data Sharing Principles* in March 2019. This guide was developed in consultation with experts both locally and overseas and has been well received.<sup>7</sup>

## The benefits of a national data system

The value of better data sharing between the Commonwealth and States and Territories was a consistent theme in discussions across Australia. Some felt many of the most challenging research and policy problems span different levels of government, and pointed to productive examples of sharing between States and the Commonwealth. We heard a national data system would enable more national solutions to national problems. Most recognised the challenge of creating legislation to enable a national system, but asked for reform in this area as a priority. Many also recognised the benefits of Data Sharing and Release legislation, including adopting the Data Sharing Principles to enable States and Territories to build a consistent approach to data sharing, even before legislation being adopted in their jurisdictions.

## Importance of a streamlined accreditation process to build trust

The Issues Paper proposed accrediting all users and data service providers before they could participate in data sharing enabled by this legislation. We heard broad support for accrediting users, with privacy advocates emphasising the need for users to be properly qualified to handle personal information. Universities, state bodies and the private sector expressed interest in being accredited as users and felt accreditation criteria should not be overly onerous. Others questioned whether we needed to accredit all users, as this could duplicate existing processes.

Some government agencies and stakeholders felt they would benefit from experts helping them apply the legislation and share data more effectively. They saw value in the National Data Commissioner accrediting data service providers and providing oversight to engender trust and increase transparency in the system.

6 The Five Safes are used by the Australian Bureau of Statistics and are included in other data sharing frameworks across Commonwealth and State agencies and internationally.

7 Sharing Data Safely package including the Best Practice Guide is available at <https://www.pmc.gov.au/news-centre/public-data/empowering-public-service-share-data-safely>.

## Support for enhanced transparency in the use of public data

There was strong support from privacy experts, civil society and others for the publication of Data Sharing Agreements to increase the transparency of how public sector data is used. We heard mixed views on the level of detail that should be published: some argued Data Sharing Agreements should be comprehensive and published in full, while others suggested requiring publication of only a basic version of the Data Sharing Agreement.

## Concerns around what happens when things go wrong

We heard about the importance of having measures in place for when things go wrong. Some stakeholders reflected that strong penalties are necessary to ensure data is shared responsibly. Some researchers also accept the need for strong deterrence, but felt it was important to find a careful balance: encouraging safe data sharing and not creating a risk averse environment. We heard the proposed system would place more responsibility on researchers and other users of public sector data, but the proposed safeguards and requirements were considered reasonable and appropriate. See section 7 for a more detailed discussion of these issues.

## 1.5 What has changed since the Issues Paper?

Since receiving feedback from the Issues Paper, we have made considerable progress to develop our policy positions. This has involved developing a more technical and detailed framework and making significant changes to meet your expectations and achieve our policy intentions. We have designed and issued new Data Sharing Principles for the Australian system in consultation with world experts.

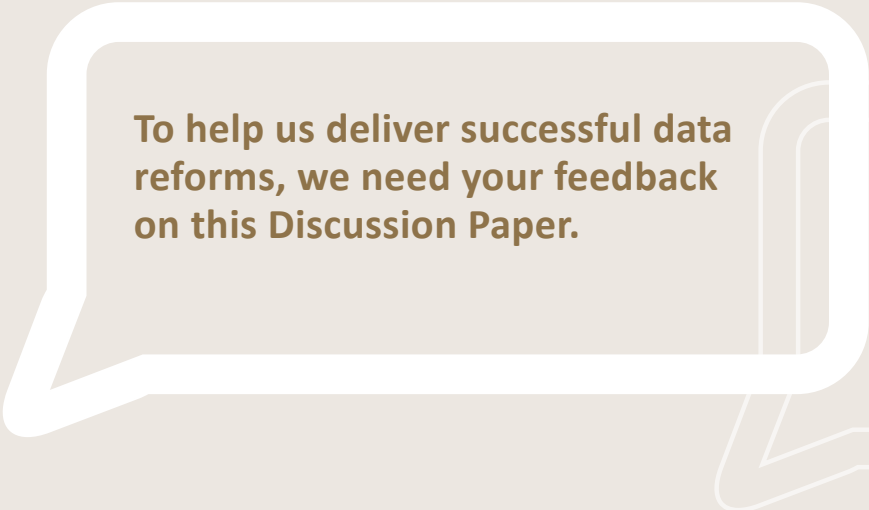
As agreed with Minister Robert, data sharing for compliance and assurance purposes will not be allowed under the Data Sharing and Release legislation. Compliance and assurance activities are better carried out under the legislation that provides the basis for compliance and assurance decisions. By keeping data sharing and decisions for these activities together in legislation, Australians can easily identify why and based on what data the decisions have been made.

Listening to feedback from consultations and our National Data Advisory Council, we have nuanced our position on consent. While consent is important in certain situations, the societal outcomes of fair and unbiased government policy, research and programs can outweigh the benefits of consent, provided privacy is protected. The Office of the National Data Commissioner will encourage the use of consent where appropriate when applying the Data Sharing Principles, although the legislation will not require it in all circumstances. The Data Sharing and Release legislation will never authorise the release of personal information as open data.

In response to concerns about overriding all secrecy provisions, the Data Sharing and Release legislation will not compel sharing. Government agencies will be responsible for deciding whether to use the legislation, only if they are satisfied data can be shared safely. The National Data Commissioner will not be able to compel or overturn decisions to share or not to share, instead focusing on ensuring that when data is shared, it is done safely. In addition, although the Data Sharing and Release legislation does not compel sharing, we will be finalising a list of secrecy provisions to be exempt from the override. Government agencies will be able to make a case for maintaining secrecy provisions that should not be overridden by the legislation. The list of exemptions will be provided for public consultation alongside the Exposure Draft of the legislation.

We also heard more detail of the complex landscape around open data release. The National Data Commissioner will be empowered to advocate for open data, but the legislation will not provide a new legislative authorisation for open data release as we heard the current mechanisms are sufficient.

This Discussion Paper is an update on these developments and other ways we are iteratively improving the Data Sharing and Release framework based on consultations. Your feedback has been invaluable to us so far and we especially thank you for taking the time both in person and in writing to ensure Australia's public sector data future is shaped for the better.



**To help us deliver successful data reforms, we need your feedback on this Discussion Paper.**

## 1.6 Have your say

In line with our philosophy to listen, learn and improve our practices, we need your feedback on this Discussion Paper to help deliver these data reforms. To guide your submissions, we ask that as you read this paper you consider the questions below.

- 1** Do you think the distinction between data sharing and data release is clear?  
How could this distinction be clearer?
- 2** What are the challenges for open release of public sector data?
- 3** Do you think the Data Sharing and Release legislative framework will achieve more streamlined and safer data sharing?
- 4** What do you think about the name, Data Sharing and Release Act?
- 5** Do the purposes for sharing data meet your expectations? What about precluded purposes?
- 6** What are your expectations for commercial uses? Do we need to preclude a purpose, or do the Data Sharing Principles and existing legislative protections work?
- 7** Do you think the Data Sharing Principles acknowledge and treat risks appropriately?  
When could they fall short?
- 8** Is the *Best Practice Guide to Applying Data Sharing Principles* helpful? Are there areas where the guidance could be improved?
- 9** Do the safeguards address key privacy risks?
- 10** Are the core principles guiding the development of accreditation criteria comprehensive?  
How else could we improve and make them fit for the future?
- 11** Are there adequate transparency and accountability mechanisms built into the framework, including Data Sharing Agreements, public registers and National Data Commissioner review and reporting requirements?
- 12** Have we achieved the right balance between complaints, redress options and review rights?
- 13** Have we got our approach to enforcement and penalties right for when things go wrong?  
Will it deter non-compliance while encouraging greater data sharing?
- 14** What types of guidance and ongoing support from the National Data Commissioner will provide assurance and enable safe sharing of data?

You can provide feedback on these questions and any other matters you would like to raise in writing or through other forums we are organising. If you are not already on our mailing lists, please contact us at [www.datacommissioner.gov.au/contact](http://www.datacommissioner.gov.au/contact), so you get our news and notifications of upcoming workshops and events.



**Closing date for  
submissions on the  
Discussion Paper is  
15 October 2019.**

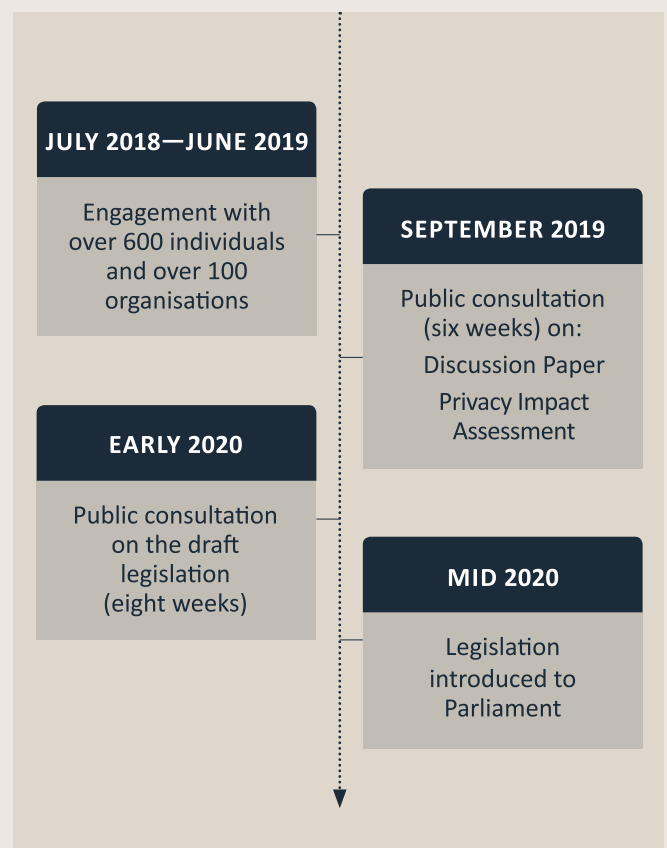
## 1.7 What will we do with your feedback?

In addition to receiving submissions on this paper, we will undertake another round of engagement following the release of this Discussion Paper to hear community views. Your feedback will help us build a strong and workable system to support the cultural change necessary to achieve our ambitious reform agenda. Our previous engagement rounds have been with interested stakeholders and internal to government, but we are now expanding our engagement to reach more of the Australian public. We may not be able to solve everyone's difficulties with data, but we hope to have understood them before we introduce the Data Sharing and Release legislation to Parliament.

We continue to engage with government stakeholders. We are working with regulators such as the Office of the Australian Information Commissioner, Commonwealth Ombudsman, Australian Competition and Consumer Commission and international counterparts to minimise duplication and regulatory burdens where we can. We are working with our State and Territory counterparts to work towards a consistent experience of government wherever you are. We have more meetings of our National Data Advisory Council in coming months to also hear their expert opinions on the development of the legislation.

We plan to release more blog posts on our website [www.datacommissioner.gov.au](http://www.datacommissioner.gov.au) from the National Data Commissioner and other experts. You will also hear from us with draft legislation in early 2020, when it is ready for feedback (see Figure 3). Through cooperation and shared expertise, we will build a coherent national data system that fosters innovation, confidence and best practice.

**Figure 3:** More opportunities to have your say





**The Data Sharing  
and Release  
framework sets a  
new direction for  
how public sector  
data in Australia is  
used and reused.**

## 2. DATA SHARING AND RELEASE FRAMEWORK

### 2.1 A new regulatory framework

The Data Sharing and Release framework sets a new direction for how public sector data in Australia is used and reused. To unlock the potential of this data, we are building on the Government's response to the recommendations made by the Productivity Commission's Data Availability and Use Inquiry. We have designed a framework underpinned by three key features:

1. An independent National Data Commissioner driving change and supporting best practice sharing and release of public sector data.
2. A National Data Advisory Council advising the National Data Commissioner on ethical data use, community engagement, technical best practice, as well as industry and international developments.
3. New legislation to authorise a streamlined data sharing system and encourage greater sharing of public sector data. The legislation will strengthen data safeguards, while modernising Australia's public sector data framework.

### 2.2 National Data Commissioner: a champion for cultural change in data use

Creating a new framework is only part of the data reforms. A much larger part of the journey is changing the Australian public service culture to achieve the paradigm shift from 'need to know' to 'responsibility to share' where there is clear public benefit. The National Data Commissioner will be a champion and advocate for greater data sharing and release. This includes advocating for consistent and effective best practice data governance across the public sector.

The objectives of the National Data Commissioner will be to:

- promote the use and reuse of public sector data
- enhance the integrity of the public sector data system
- engage with the community and earn trust about use of public sector data
- ensure the Data Sharing and Release legislation is applied in a consistent and effective manner.

The interim National Data Commissioner is overseeing the development of the legislative framework that will support data reforms, including the above objectives.

Importantly, the legislation will be principles-based to allow flexibility in its interpretation to ensure it is constantly adapting to new technologies and community expectations around data sharing. The National Data Commissioner has a significant role in driving the reforms by providing practical guidance and advice as the system is rolled out and matures (see more on the role of the National Data Commissioner in Chapter 6).

## 2.3 The National Data Advisory Council

The National Data Advisory Council is an important source of expertise to support the National Data Commissioner's guidance, advice and advocacy functions. It advises the National Data Commissioner on ethical data use, community expectations, technical best practice and industry and international developments. The National Data Commissioner may also seek advice from the National Data Advisory Council on issues relating to the broader data environment.

The National Data Advisory Council met for the first time on 27 March 2019 and again on 25 July 2019. It is expected to meet between two and four times a year. The Council comprises nine members from the Australian government, business and industry, civil society groups and academia.<sup>8</sup> Government representatives include the Australian Statistician, the Australian Information and Privacy Commissioner and the Australian Chief Scientist. The National Data Commissioner will also directly engage with other experts to seek advice on new and emerging challenges and ways to address them.

## 2.4 New legislation for data custodians to share public sector data

The Data Sharing and Release legislation will authorise Commonwealth agencies and companies, called Data Custodians, to share public sector data for the right reasons with the right safeguards in place.

Data Custodians collect or generate 'public sector data' for the purpose of carrying out their functions and have a legal responsibility to manage this data. This includes information collected directly from people through surveys and forms as well as data generated internally through administrative or statistical processes (see Attachment A—Key Terms).

The objectives of the Data Sharing and Release legislation will be to:

- consistently safeguard public sector data sharing and release
- enhance the integrity of the data system
- build trust in use of public sector data
- establish institutional arrangements
- promote better sharing of public sector data.

The Data Sharing and Release legislation will not allow public sector data to be shared if it is considered too sensitive, for example, because it would threaten Australia's national security or because the Australian community does not support it. There are two main classes of information that will likely be exempted from the scope of the legislation:

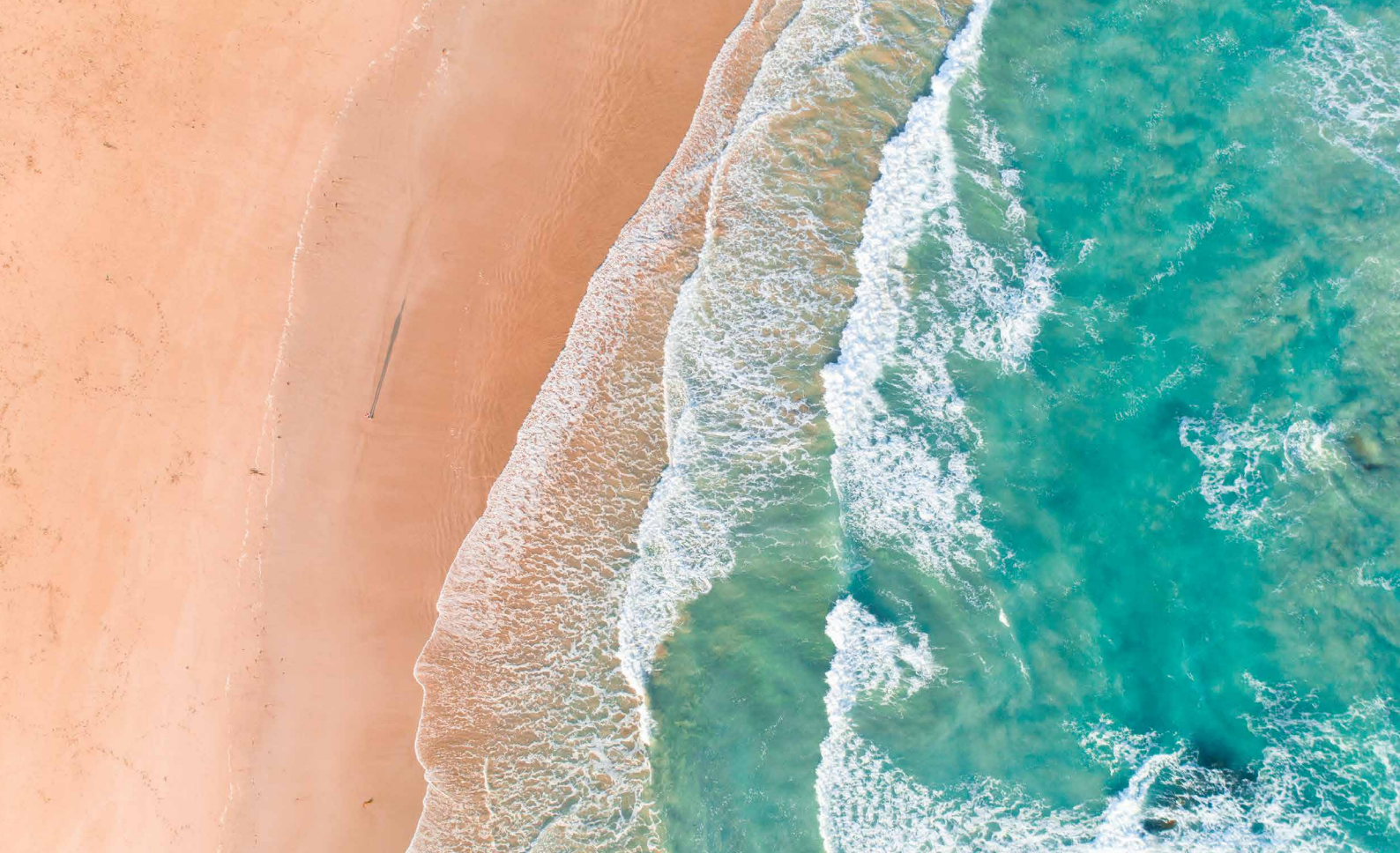
- information collected or held by the National Intelligence Community<sup>9</sup>
- information provided under the *My Health Record* scheme.

We will be consulting with Commonwealth agencies once we have draft legislation to finalise our exemption list. The proposed exemption list will be subject to public scrutiny as part of the consultation on the draft legislation.

---

<sup>8</sup> Further details regarding the Council's current membership can be found at: <https://www.datacommissioner.gov.au/advisory-council>.

<sup>9</sup> For details about the National Intelligence Community: <https://www.oni.gov.au/national-intelligence-community>.



## INDIGENOUS DATA

The government is working to address matters related to Indigenous data and it will continue to engage and work with the community and stakeholders to ensure the right policy and practices are used. The National Indigenous Australians Agency is in the early stages of developing a more effective approach to Indigenous data, including a possible whole-of-government Indigenous data strategy, and we are working together to get it right.

## BUILDING TOWARDS A NATIONAL SYSTEM

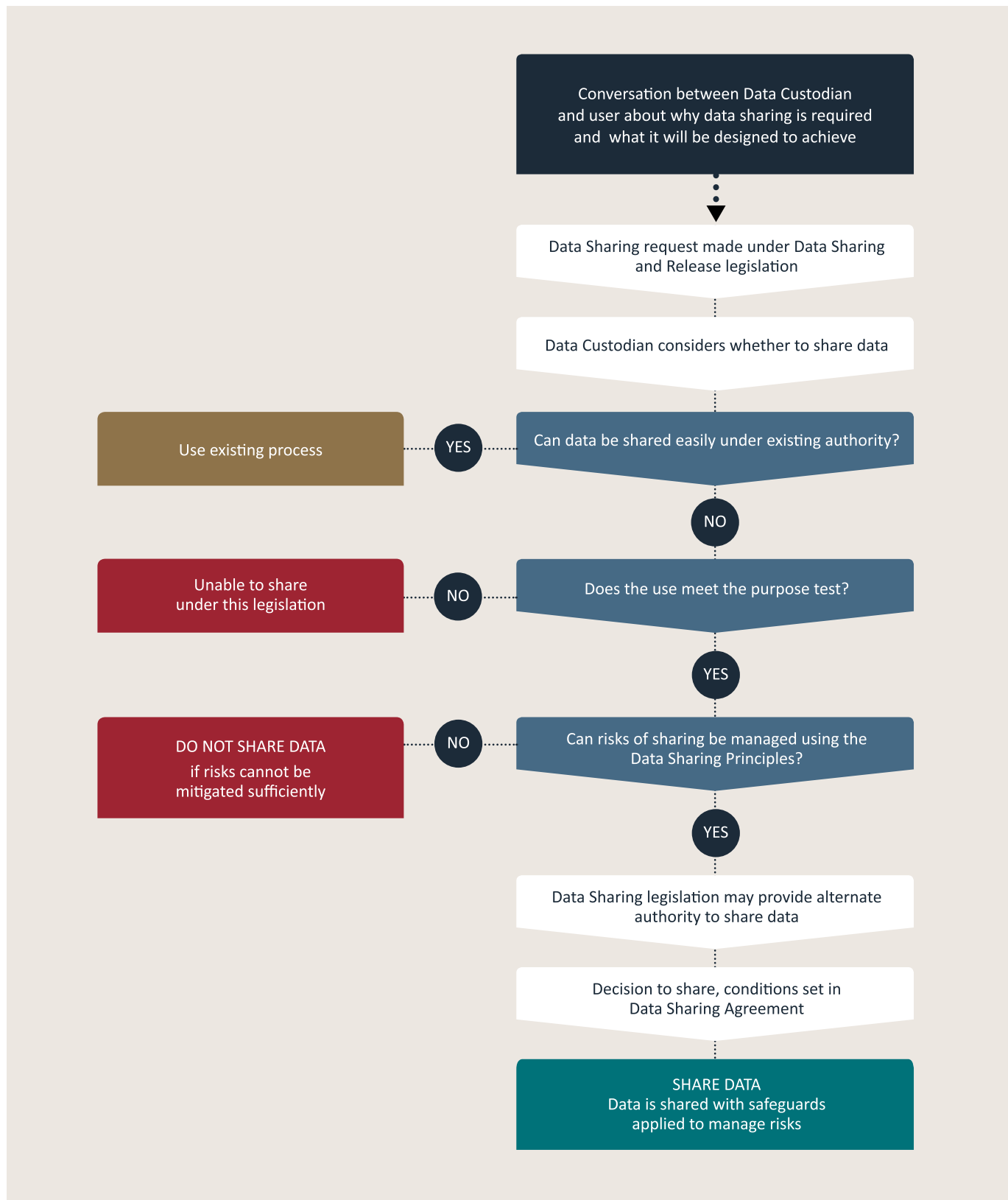
We are working towards building a national system. Our scheme will begin with a focus on Commonwealth data and enable participation by all levels of government. Commonwealth, State, Territory and local government authorities may be accredited and access shared data under the legislation, but State and Territory data will not initially be in scope.

The National Data Commissioner will work with State and Territory government agencies and regulators to ensure consistent approaches to data sharing across jurisdictions. Collaboration on guidance, standards and approaches will help streamline, simplify and align aspects of the overall system. This consistency will help build trust in governments' use of data by establishing minimum standards and clear expectations for data handling.

Adopting consistent approaches across jurisdictions will help create a more harmonious system to function alongside State and Territory data sharing legislation. Future reforms will explore reciprocating State and Territory legislation to authorise sharing of data across borders to build a national system.



**Figure 4:** Process for sharing public sector data under the Data Sharing and Release legislation



## 2.5 How will sharing work under the legislation?

The government currently shares public sector data through various laws and mechanisms developed at various points in time, with little consistency or a single point of oversight. The Data Sharing and Release framework will provide an alternative pathway for government agencies who want to share data (see Figure 4). It removes the need for lengthy legal processes to establish authority, and instead focuses on consistently applying important safeguards and protections to data sharing. This pathway includes key features explored in Chapter 4 of this paper.

Data sharing must satisfy the purpose test, i.e. be reasonably necessary to inform government policy, programs, or service delivery, or be in support of research and development. Safeguards, through the five Data Sharing Principles, must be applied to holistically minimise and mitigate the risks of the data sharing, by determining the specific controls to be applied. Finally, the details must be recorded in a Data Sharing Agreement to be published for greater transparency of public sector data sharing.

The National Data Commissioner will build trust in the system by accrediting users and data service providers. The Commissioner will also support best practice through guidance and education, aimed at voluntary compliance with the legislation, and will escalate to a graduated enforcement model when necessary to protect public sector data. The graduated enforcement approach is discussed further in section 7.5.

---

**THE DATA SHARING AND RELEASE LEGISLATION WILL MAKE IT EASIER TO IMPROVE AND BUILD ON EXISTING WORK SUCH AS THE DATA INTEGRATION PARTNERSHIPS FOR AUSTRALIA TO DELIVER BETTER RESEARCH AND POLICY INSIGHTS.**

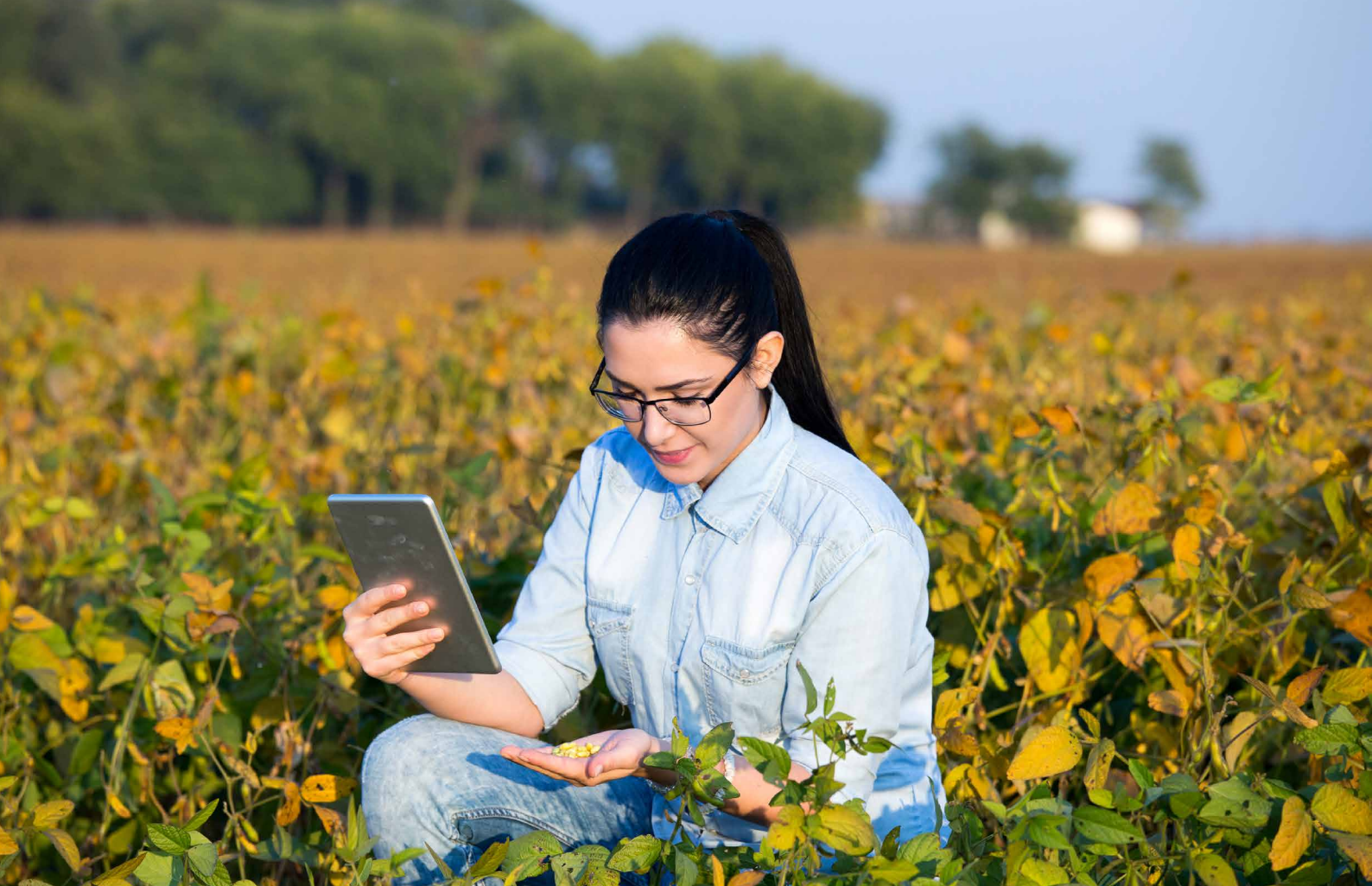
---

The Data Sharing and Release legislation will make it easier to improve and build on existing work such as the Data Integration Partnerships for Australia to deliver better research and policy insights. This includes streamlining the development and access to integrated datasets to trusted users who can use them safely. For example, integrated datasets developed under the Data Integration Partnerships for Australia have been used to deliver a National Drought Map<sup>10</sup> to help meaningful support reach drought affected farmers and communities.

In the process of streamlining the system, there is also the opportunity to realise benefits from datasets that can generate significant community-wide value. The Productivity Commission recommended establishing these datasets as a national asset called the 'National Interest Dataset'.

---

10 National Drought Map is available at <https://map.drought.gov.au/>



## 2.6 What about open data release?

### A champion to support greater open data release

The Government's response to the Productivity Commission's report committed to creating the National Data Commissioner as a powerful champion with a mandate to unlock the productivity benefits of valuable datasets, identify opportunities for improved data use and build national frameworks and guidelines.

The National Data Commissioner will be a champion for open data release advocating for government agencies to safely release public sector data. While the Data Sharing and Release legislation will only provide an authority to share data, the Commissioner will also advise government agencies on how to apply the Data Sharing Principles (See section 4.2) to mitigate risks of both sharing *and* release. Sometimes the application of the Principles will lead to data being shared in a controlled environment rather than released to the public. If a data sharing project produces outputs that are made public, the data made public will have to meet the requirements for data release.

The National Data Commissioner will contribute to the open data agenda by increasing transparency on how public sector data is used and handled. The National Data Commissioner will publish annual reports on the performance of the system and maintain public registers on the use of the Data Sharing and Release legislation, discussed in section 5.2. These registers will support greater access to public sector data by making public sector data holdings clearer.

The Data Sharing and Release legislation will not duplicate existing legislative authorisations to release open data. The National Data Commissioner will work with other government agencies and regulators, such as the Australian Information Commissioner, to improve guidance on using existing mechanisms to release open data, as well as work to improve its dissemination across the Australian Public Service.



## A confusing space in need of clarity, not duplication

We were given a broad mandate by the Government's response to the Productivity Commission's *Data Availability and Use* inquiry to streamline and modernise sharing and release of public sector data. We are taking an iterative approach to identify barriers and test solutions to increase the release of open data.

The Australian Government's Public Data Policy Statement, released in 2015, provides a clear mandate for Commonwealth agencies to release non-sensitive data by default. This has helped increase the availability of open data. However, more needs to be done.

We have engaged extensively on data release and are aware of the complex landscape of existing legislative mechanisms. Government agencies are confused and uncertain about the existing mechanisms and lack the confidence to use them. We heard that broader cultural barriers in the Australian Public Service related to data use, including a general risk aversion in decision making and a lack of understanding of what can be done and how to do it, also come into play to limit the release of open data.

Existing mechanisms related to open data in Australia include:

- The Australian government's Public Data Policy Statement provides a clear mandate to release non-sensitive data as open data by default. Non-sensitive data includes information that is not protected by a secrecy provision or the *Privacy Act 1988*.
- The de-identification of data so it may be disclosed consistently with the *Privacy Act 1988*.<sup>11</sup>
- The *Freedom of Information Act 1982* promotes a pro-disclosure culture across government, including through the Information Publication Scheme.<sup>12</sup>
- The *Archives Act 1983* provides a right of access to Commonwealth government records in the open access period.

- Data.gov.au is the central source of Australian open government data, with more than 80,000 datasets currently available.
- Some portfolio legislation allows government agencies to release data, either through laws that expressly state government agencies can release, like the *Patents Act 1990*, or by staying silent on the matter and leaving it to government agencies to decide if the data is suitable for open data release.

These overarching mechanisms already exist for government agencies to release open data. Rather than increasing this complexity by providing another authorisation to release open data, we heard the need for actions to support understanding, cultural change and transparency. Solutions focused on reducing regulatory burden and simplifying processes to support the Australian Public Service to overcome a cultural reluctance to release data.

We also acknowledge many datasets should never be released as open data. As more information is released publicly it increases the risks around re-identification of sensitive information by combining multiple datasets. As the risks are heightened, we need to be careful of new releases of data over time. Sharing under the Data Sharing and Release legislation provides a way to use data without losing control, while providing appropriate oversight (see Section 1.2) so the benefits continue to be realised.

11 The Office of the Australian Information Commissioner and Data61 released the 'De identification decision making framework' to assist organisations to de-identify data. <https://www.oaic.gov.au/privacy/guidance-and-advice/de-identification-decision-making-framework/>

12 See *Freedom of Information Act 1982* Pt II.



**Sharing public  
sector data enables  
a better economy,  
society and  
environment.**

## 3. SHARING DATA FOR PUBLIC BENEFIT

### 3.1 Key Points

1. Better use of datasets can provide a richer picture of Australia's economy, society and environment, and significantly increase the value government agencies and researchers can obtain from data. It can also enable government to deliver better services to citizens.
2. Under the Data Sharing and Release legislation, data sharing may occur for public benefit. The purpose test is satisfied if sharing is reasonably necessary to inform government policy, program and service delivery or for research and development.
3. Data sharing for any other purposes, including compliance, law enforcement and national security is not permitted under this legislation. Government agencies must use other legislative avenues such as their primary legislation to share data for such purposes.
4. A Data Sharing Agreement must be in place for data sharing under the legislation to explain why the data is being shared, how risks will be managed and establish accountability.

### 3.2 When can we share data for the public benefit?

The public sector data reforms must lead to more and better data sharing and build public trust and confidence in government data sharing. We heard from people that trust in government data handling can change quickly and we need to clearly explain the reforms and how the safeguards will work.

We also heard there is a need to provide people with clear benefits for data use. We understand through our consultation and research there is broad support for three purposes for data sharing; in fact, many stakeholders assumed government agencies already share data for these reasons. A purpose test is satisfied if sharing is reasonably necessary to inform or enable:

- government policy and programs
- research and development
- government service delivery.

This Discussion Paper provides more detail on these purposes and supporting use cases (see Figure 5). There is one important difference between the three purposes: the first two (government policy and programs and research and development) may involve the sharing of personal information, but will result in outcomes for entire cohorts. In contrast, the final purpose (government service delivery) will involve the sharing of personal information and support better outcomes targeted at individuals no matter what cohort they belong to.



## Government policy and programs

**Government policy** is a rule or principle that guides government decisions.

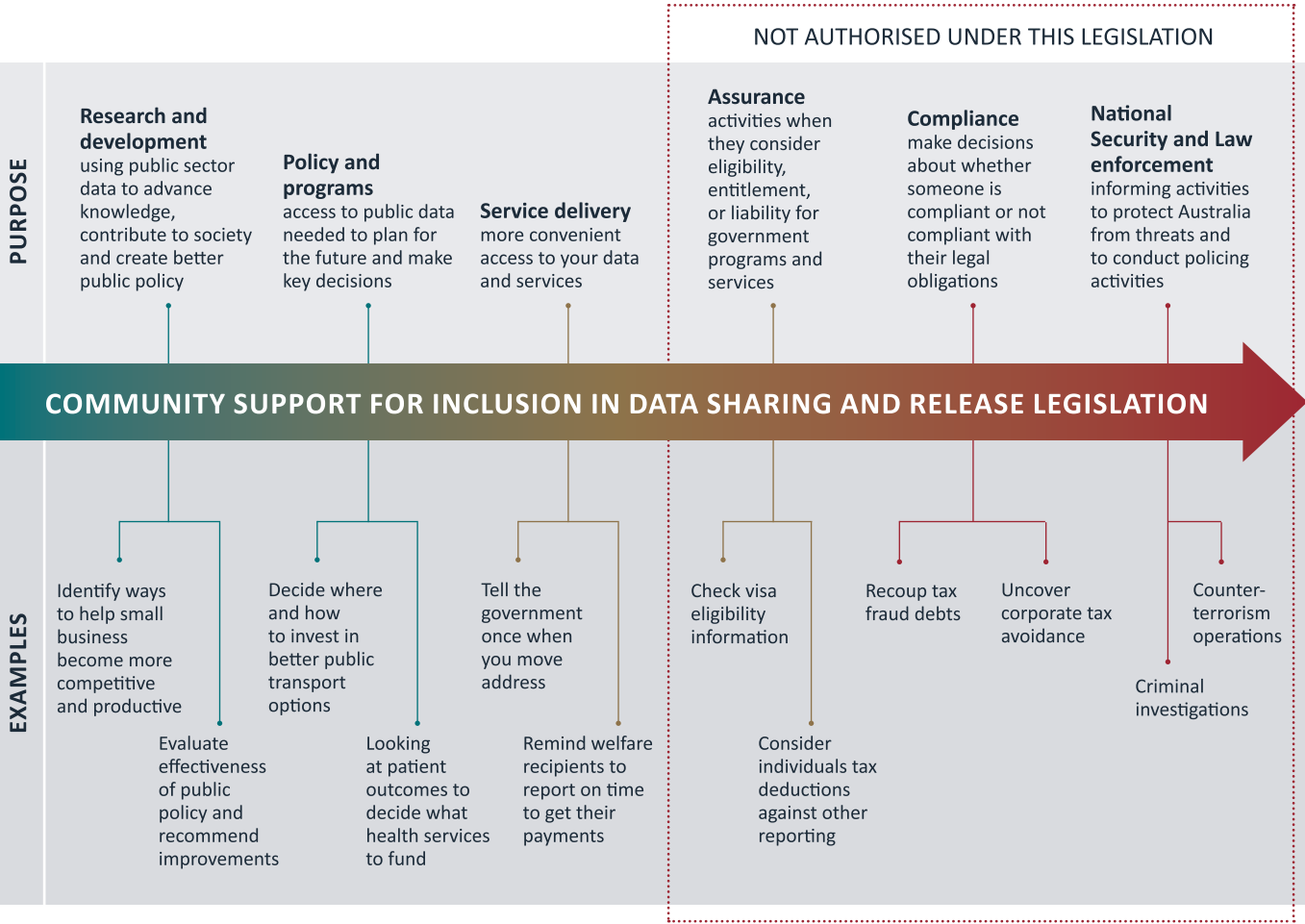
**Government program** means an organised system of services, activities or opportunities to achieve a goal or outcome.

Data custodians will be able to share public sector data for projects and activities to inform government policy and programs. This will include data sharing to evaluate government policies and programs to identify areas for improvement and minimise unintended consequences. Data sharing for these purposes could:

- enable the discovery of trends and risks to inform policy making
- provide a holistic understanding of cross-portfolio impacts and ‘wicked problems’
- enable modelling of policy and program interventions
- program risk analysis and impact measurement
- test the effectiveness of policies and programs
- ensure the government is spending money effectively
- identify program gaps, challenges and successes to inform new or improved programs.

Data sharing for these purposes may impact on individuals, but they will not be directly targeted. For example, one of the key features of the Gonski 2.0 school funding reforms was greater attention to funding schools on the basis of need—the capacity of parents to contribute. Previously, the financial wellbeing of the student population of a school was assessed from the socio-economic circumstance of where a school was physically located. This was recognised to be a very rough indicator of the financial circumstances of parents, not able to reflect the financial diversity of the student population. However, with reported income data available to Government and using safe data linkage techniques, the Australian Bureau of Statistics can now safely construct a measure that better reflects the average financial situation of the student body for each school. This enables Government to deliver a much fairer allocation of funding to schools in the future.

**Figure 5:** Government purposes spectrum, from research, policy and programs and service delivery, into assurance, compliance and national security and law enforcement activities



### Research and development

**Research and development** means activities to advance knowledge, contribute to society and create better public policy, undertaken by a range of actors including universities and the private sector.

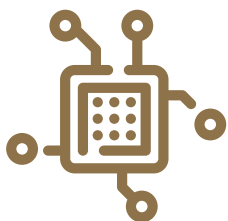
Data Custodians will be able to share data for research and development. Academics, scientists and innovators will have greater access to public sector data to undertake research on how to make our economy, environment and society healthier into the future.

Some immensely important research breakthroughs have already happened when public sector data has been shared with researchers.<sup>13</sup> For example, Professor Fiona Stanley AC and colleagues used public sector health data to prove that taking folate during pregnancy significantly reduces the likelihood of neural tube defects, which lead to birth defects including spina bifida. Her research was key to the Department of Health requiring folic acid and iodine to be added to bread.

Research and development can have commercial applications. We heard concern from the public about the use of public sector data for commercial purposes. We want to preclude commercial uses that the public do not support, but do not want to prevent research delivering public benefits. For more on where we think this line may be, please refer to Section 3.4.

13 Refer to Overview and Chapters 2.1 and 2.3 in the Productivity Commission's *Data Availability and Use Inquiry* report.





---

**DATA MAY BE SHARED SO THE GOVERNMENT CAN DELIVER BETTER SERVICES TO THE COMMUNITY, SUCH AS WELFARE PAYMENTS, EMPLOYMENT ASSISTANCE, HEALTHCARE REBATES, TAXATION REFUNDS, SUPERANNUATION ADVICE AND DISABILITY SUPPORT.**

---



## Government service delivery

**Government service delivery** means government activities that provide coordinated and structured advice, support and services to citizens and customers. An important part of service delivery is to improve user experience through simplification (e.g. tell us once), automation and proactive engagement.

Data custodians will be able to share data for government service delivery. Data may be shared so the government can deliver better services to the community, such as welfare payments, employment assistance, healthcare rebates, taxation refunds, superannuation advice and disability support. Under this purpose, data about individuals, including names and addresses may be shared to directly help an individual to access government services, for example pre-filling a form or application. This will only take place with suitable safeguards and in a carefully controlled environment.

Government already shares your data to help you at tax time by pre-filling your myTax form with information from your employer, bank, Medicare and private health insurance providers. Once the Data Sharing and Release legislation has commenced, government agencies could share your data so you only have to tell us once when your circumstances change, and we could update all relevant government records. For example, at present, citizens who apply for the National Disability Insurance Scheme and Support Pension have to provide the same medical certificate twice—once to the National Disability Insurance Agency and separately to Centrelink. Legislated secrecy restrictions mean government agencies cannot offer the choice for individuals to provide the certificate once despite that being easier for the user.

### 3.3 When is data sharing not authorised by this legislation?

The legislation will preclude the sharing of public sector data for the purposes of:

- compliance and assurance activities, and
- national security and/or law enforcement.

#### Compliance and assurance activities

**Compliance activities** are making decisions about whether someone is compliant or not compliant with their legal obligations. This includes activities to identify and prevent fraud against the Commonwealth.

**Assurance activities** are considering eligibility, entitlement or liability for government programs and services.

Data Custodians will not be able to share data for compliance and assurance activities under the Data Sharing and Release legislation. In consultations, while compliance and assurance activities were recognised as legitimate and important functions of government, stakeholders expressed concern about the appropriateness of using this legislation to achieve them.

The preference was for government agencies to share data and conduct those activities under the legislation that governs their activities, and to amend it if necessary. The Attorney-General's Department recently amended the *Crimes Act 1914* to authorise data sharing to prevent fraud.<sup>14</sup> Keeping the provisions related to a compliance decision together in legislation makes it easier for citizens to understand how these decisions are made and to know their review rights.<sup>15</sup>

Data Custodians will not be authorised to share data for compliance or assurance activities under the Data Sharing and Release legislation. For clarity: if data is shared with an entity under the Data Sharing and Release legislation (for one of the three permitted purposes) the entity cannot subsequently use the data for compliance or assurance activities—this would be a breach of the Data Sharing and Release legislation.

#### National security and law enforcement purposes

**National security and law enforcement** means activities to protect Australia from threats and to conduct policing activities.

Data Custodians will not be able to share data for national security and law enforcement purposes under the Data Sharing and Release legislation. This includes investigations, monitoring and taking action targeted at individuals and organisations to keep Australia safe.<sup>16</sup>

This is consistent with the Government's response to the Productivity Commission's Inquiry on Data Availability and Use, stating protections for particularly sensitive data including national security and law enforcement data will continue to apply. This approach is supported by stakeholders (including the National Intelligence Community).<sup>17</sup>

Data sharing for national security and law enforcement is provided under legislation specifically designed for those purposes. The Comprehensive Review of the Legal Framework of the National Intelligence Community (the Richardson Review) will consider improvements to support effective information sharing between National Intelligence Community agencies and Commonwealth, State, Territory and other partners.

The National Intelligence Community and law enforcement agencies may apply to be Accredited Users or Accredited Data Service Providers and seek access to public sector data for permitted purposes under the Data Sharing and Release legislation—for example, for policy development purposes, as distinct from law enforcement operations.

<sup>14</sup> Schedule 7, Crimes Legislation Amendment (Powers, Offences and Other Measures) Act 2018..

<sup>15</sup> Attorney-General's Department, Australian Administrative Law Policy Guide, 2011.

<sup>16</sup> Definitions will be based on the Victorian *Data Sharing Act 2017*.

<sup>17</sup> Information collected or held by the National Intelligence Community will likely be exempted from the scope of the legislation, see Section 2.4.

### 3.4 What about private sector use for commercial applications?

#### Open data drives innovation and competition

Open data release drives productivity, innovation and competition. The National Data Commissioner will champion the greater release of open data, including for commercial uses.

Open data can be used by anyone for any purpose, including by companies to analyse and develop products and services. Greater availability of open public sector data can help fuel new insights and breakthroughs. Using open data, companies can develop new medicines and test new car safety products.

Commercial uses of public sector data by the private sector could be limited to non-sensitive data that is openly released. For example, weather, traffic congestion or maritime shipping data is valuable to the private sector. Releasing open data for commercial use ensures we are making useful data available fairly to all entities, encouraging competition and innovation in the system.



The Australian Government has made over 80,000 datasets discoverable through its open data portal ([data.gov.au](https://data.gov.au)). Anyone, for any purpose, can use these datasets to draw insights and develop new products. Various government agencies continue to support events around the country to help new and innovative uses of data, including for commercialisation.



#### Open data fuelling new products

IP NOVA is a visual immersive search engine that helps users discover registered patents, trade marks, and plant breeder's rights from IP Australia's database. IP NOVA is used to:

- Search for invention and development ideas.
- Avoid duplicating research and development effort.
- Identify key trends in technology development.
- Find collaborators in specific technology fields.
- Improve business decision making, for example gathering information on future direction of competitors, potential technology partnerships and licensing.
- Obtain rich IP datasets to perform further research and analysis.



The Bureau of Meteorology makes a number of real-time forecast, warning and observation products and analysis charts available freely via the web. This data has many applications—from simple weather app developers marketing their products, to large agribusinesses who can use it to offer services to farmers to manage farm conditions.





### Data sharing for commercial uses needs to be in the public interest

We heard Australians are concerned about public sector data being used by the private sector. We are considering how to enable data sharing for research and development for commercial uses that benefit society, but do not harm individuals or businesses. Many stakeholders reflected that they were comfortable providing data to the government to receive better services and for government activities, but they did not want companies to access data to pursue their commercial interests. We are considering how to design the purpose test to maximise public benefits while meeting community expectations.

The purpose test cannot be considered in isolation. The Data Sharing and Release legislation presents holistic risk management, through the purpose test and the application of the Data Sharing Principles. We are not proposing preventing users' participation in data sharing based on their sector. Instead, the purpose test and the Data Sharing Principles are the avenues to prevent commercial uses not supported by the community. As yet we have not finalised our position on commercial use of public sector data. We welcome further discussions about this area to make sure we fully understand Australians' concerns.

### Other legislative protections

Providing businesses with secure access to certain data could help improve products and services by business and deliver benefits to citizens and the broader economy. However, we heard concerns about commercial practices unfairly targeting or misleading citizens, such as through unwanted marketing or price discrimination.

It is also important to be aware that the Data Sharing and Release legislation is not the only protection against unacceptable commercial uses of public sector data. Existing privacy, intellectual property, and consumer and competition laws include a range of protections, including against direct marketing, profiling, intellectual property and misleading consumers or leading to the misuse of market power. These laws will continue to protect Australians.

**Private sector will not be able to access public sector data for activities prevented under existing laws. For example companies will not be able to access public sector data to find people with health conditions for advertising new treatments. Companies will also not be able to access public sector data to know when someone receives a government payment to time advertising products, or target payday lending.**



**A modernised  
risk management  
framework will  
safely unlock greater  
benefits of public  
sector data for the  
public good.**

## 4. STRENGTHENING SAFEGUARDS

### 4.1 Key Points

1. A new principles based framework will streamline data sharing with the right protections in place. It provides an alternative to the ad-hoc safeguards currently used in practice.
2. The Data Sharing Principles provide five factors to consider holistically when managing data sharing risks. The factors are project, data, settings, people and outputs.
3. Data custodians need to consider what project the data will be used for, how detailed the data is, will the data be used in a safe and secure environment, who will use the data and can the project results be published without identifying individuals or businesses.
4. Data is only shared when the overall risks can be managed using the Data Sharing Principles.
5. The Data Sharing Principles enable a privacy by design approach to data sharing.
6. An independent Privacy Impact Assessment has been completed and published on the Data Sharing and Release framework.
7. The Department has accepted in full or in principle all eight recommendations from the Privacy Impact Assessment.
8. Consent remains an area of debate and requires further public discussion.

### 4.2 A modernised approach to sharing data safely: the Data Sharing Principles

The Data Sharing and Release legislation will include a modernised risk management framework that safely unlocks greater benefits of public sector data for the public good. The approach we have adopted builds on the internationally recognised Five-Safes Framework.<sup>18</sup> The Five-Safes Framework has helped government agencies such as the Australian Bureau of Statistics and Australian Institute for Health and Welfare and States including New South Wales, South Australia and Victoria<sup>19</sup> share data safely. Five-Safes is also used internationally to support government data sharing, including in the United Kingdom and New Zealand.

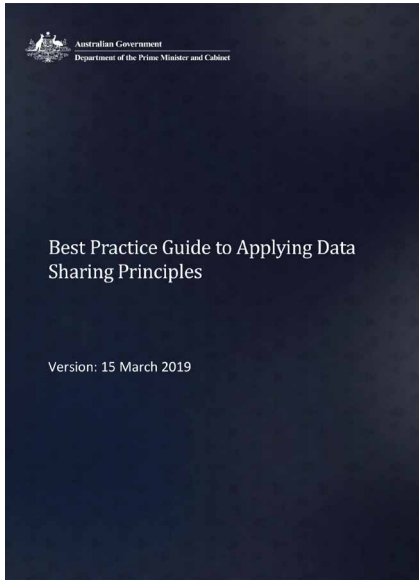
Our approach to public sector data sharing will adopt five Data Sharing Principles. The evolved Data Sharing Principles provide for strategic, privacy, security, ethical and operational risks to be considered as part of a holistic assessment. This approach also aligns with data principles<sup>20</sup> and ethical principles<sup>21</sup> used by the research sector to improve data management and guide responsible data use.

18 Felix Ritchie. "Australia's bold proposals for government data sharing." (25 September 2018), Blog Post. University of the West of England, available at <https://blogs.uwe.ac.uk/economics-finance/australias-bold-proposals-for-government-data-sharing/>.

19 New South Wales, South Australia and Victoria have state legislation that adopts the Five Safes framework for the purpose of authorising sharing.

20 Including FAIR data principles: Wilkinson, M. D. et al. The FAIR Guiding Principles for scientific data management and stewardship (2016).

21 For example—National Health and Medical Research Council (2015) Principles for accessing and using publicly funded data for health research.



DATA SHARING PRINCIPLES	
<b>Project</b>	Data sharing is for an appropriate project or program of work
<b>People</b>	Data is only available to authorised users
<b>Setting</b>	The environment in which the data is shared minimises the risk of unauthorised use or disclosure
<b>Data</b>	Appropriate protections are applied to the data
<b>Output</b>	Outputs are appropriate for further sharing or release

The Data Sharing Principles will be a key part of the legislation, setting out requirements for safeguarding any sharing activity authorised under this legislation. The Office of the National Data Commissioner will provide detailed guidance and training on how to apply the Data Sharing Principles.

On 15 March 2019, we released the Best Practice Guide to Applying the Data Sharing Principles<sup>22</sup> to start getting government agencies used to the Data Sharing Principles, and to determine areas where more guidance is necessary once the legislation commences. The Best Practice Guide provides technical advice on how to apply the Data Sharing Principles. The Office of the National Data Commissioner will update the Best Practice Guide and produce more guidance on the Data Sharing Principles as needed once the legislation commences and the system matures and evolves.

### 4.3 Other legislative safeguards for data handling

The Data Sharing and Release legislation will operate alongside existing requirements for the collection, storage, integration and management of data. The following safeguards will continue to apply:

- *Privacy Act 1988*, including the notifiable data breaches scheme for personal information and the *Australian Government Agencies Privacy Code 2017* issued by the Australian Information Commissioner.
- *Freedom of Information Act 1982*.
- *Archives Act 1983* and National Archives of Australia information management standards.
- Protective Security Policy Framework<sup>23</sup> requirements relating to the release of classified information.

The Data Sharing and Release legislation will contain provisions for cooperation between the National Data Commissioner and other regulators, such as the Australian Information Commissioner.

<sup>22</sup> Available at <https://www.datacommissioner.gov.au/news/building-trust-through-data-sharing-principles>.

<sup>23</sup> The Protective Security Policy Framework provides guidance to entities to support the effective implementation of the policy across the areas of security governance, personnel security, physical security and information security. <https://www.protectivesecurity.gov.au>



#### 4.4 Taking a privacy by design approach to data reforms

The Data Sharing and Release legislation represents a significant change in the way the Australian government handles public sector data, including personal information, from ‘need to know’ to ‘responsibility to share’ where there is a clear public benefit.

Over the last year, we have engaged and invited comments from Australians about concerns and expectations related to privacy. We commissioned an independent Privacy Impact Assessment and it is being released alongside this Discussion Paper to support public transparency and comment. The Privacy Impact Assessment identifies our privacy strengths as well as the challenges we face and makes eight recommendations. The Office of the National Data Commissioner has accepted all eight recommendations, in full or in principle, as presented in our response (Attachment C).

The National Data Advisory Council was established, with the Australian Information Commissioner as a member, to advise us on important matters including privacy. The Office of the National Data Commissioner will continue to work cooperatively with the Office of the Australian Information Commissioner.

We are committed to genuine engagement with the Australian community on privacy matters and will continue this going forward. In our view, there is no ‘set and forget’ approach to privacy. Once the Data Sharing and Release legislation has passed Parliament and the system begins to operate, we will continue to review and ensure our privacy approach remains best practice and meets the Australian community’s expectations, including through enforcement, regulation, advocacy and guidance related to the functioning of the data sharing and release system.

#### 4.5 Laying down a considered privacy standard

To be most effective, the Data Sharing and Release legislation needs to modernise and streamline existing data sharing and privacy arrangements. Informed by our conversations with stakeholders and consistent with the recommendations of the independent Privacy Impact Assessment, we intend to build privacy positive measures into the legislation. Privacy positive measures include:

- requiring all entities handling personal information to be subject to equivalent legal privacy obligations, including individuals and small businesses who may be exempt from the *Privacy Act 1988*
- listing permitted and precluded purposes for sharing
- only authorise the sharing of data that is reasonably necessary for a permitted purpose (called ‘data minimisation’ in the Privacy Impact Assessment)
- designing the Data Sharing Principles to provide holistic risk management
- restricting on-sharing of information.

For State and Territory users, we will require they are covered by the Commonwealth *Privacy Act 1988*, or a State or Territory law that provides equivalent protection to the *Privacy Act 1988*. Equivalent privacy protections will provide:

- protections for personal information
- access to redress mechanisms for individuals if their personal information is mishandled
- monitoring and oversight by an appropriate regulator
- data breach notification requirements.

In addition to these measures, other safeguards in the Data Sharing and Release framework will secure the system and flow onto protecting privacy. Our approach to accreditation safeguards the system and builds trust through the National Data Commissioner (see Section 6.3). The Privacy Impact Assessment also indicated the Data Sharing Principles are ‘stronger and more relevant’ than some of the *Privacy Act 1988* requirements, including those related to data quality and security.<sup>24</sup>

We propose the Data Sharing and Release legislation not require consent for sharing of personal information. Instead, we are placing the responsibility on Data Custodians and Accredited Users to safely and respectfully share personal information where reasonably required for a legitimate objective. Consent may be built into the application of the Data Sharing Principles, including by making consent a requirement if it is practical and feasible (more on consent in Section 4.6).

We will also set higher protections for sensitive data<sup>25</sup> in a binding Sensitive Data Code. The Sensitive Data Code may set additional limitations for categories of sensitive data such as commercial-in-confidence, legally-privileged, security-classified, confidential, or culturally sensitive data. We will determine what data requires additional protections and what those protections are in consultation with relevant stakeholders. We will consult on the Sensitive Data Code alongside the draft legislation in early 2020. Other matters, such as advice on when and how to seek consent, will be provided in non-binding guidance as needed.

## Interaction with the Privacy Act

The *Privacy Act 1988* allows entities to collect, use and disclose personal information in certain circumstances, such as where individuals have provided consent, or where such activities are authorised by law. Laws that authorise the government’s actions often use the ‘authorised by law’ mechanisms in the *Privacy Act 1988*. These laws do not ‘water down’ or ‘override’ the protections contained in the *Privacy Act 1988*; they often create their own, sometimes higher, privacy safeguards that are specific to the data and handling in question. For example, *My Health Record* data and credit information cannot be stored outside of Australia and are protected even in their de-identified form, unlike other personal information. These protections have been developed in line with community expectations.

The Data Sharing and Release legislation will authorise the collection, use and disclosure of personal information under the *Privacy Act 1988*, and create its own privacy safeguards including the Data Sharing Principles. This holistic risk management framework has been developed with a keen awareness of the need to ensure it is applied in a manner that is a reasonable, necessary and proportionate use of the ‘authorised by law’ mechanism in the *Privacy Act 1988*. Where anyone sharing data under the Data Sharing and Release legislation fails to apply these safeguards, the sharing is not ‘authorised’. In this instance, the sharing would no longer be ‘authorised by law’ and the usual *Privacy Act 1988* obligations relating to collection and disclosure, including consent and penalties would apply.

Requiring anyone sharing and using personal information under the Data Sharing and Release legislation to be covered by equivalent privacy protections is an added protection, expanding the coverage of the *Privacy Act 1988* and other laws. This means anyone handling personal information under the Data Sharing and Release legislation will need to meet the *Privacy Act 1988* or equivalent obligations, including the Australian Privacy Principles relating to privacy notification requirements and security standards.

---

<sup>24</sup> Australian Privacy Principles 10 and 11, page 38 and 40 of the PIA.

<sup>25</sup> The definition of ‘sensitive data’ includes ‘sensitive information’ as defined in the *Privacy Act 1988*.



## 4.6 What about consent?

Consent is one of the most divisive topics we heard about in our consultations. The Privacy Impact Assessment identified our approach to consent as a potential obstacle in developing public trust, confidence and acceptance for the Data Sharing and Release framework. We agree and think it is important to take the time to discuss our approach to consent and why we think it is important.

Under the Data Sharing and Release legislation, consent will not be required in all instances of data sharing. Requiring consent for all data sharing will lead to biased data that delivers the wrong outcomes. The Data Sharing and Release legislation is about improving government policy and research by helping government and researchers use a better evidence base. If we required consent, then data would only be shared where consent was given. This will skew the data which is shared, leaving it unfit for many important purposes in the public benefit; it also runs the risk of leading to flawed policy and research which impacts negatively on society.

The research sector presented particularly robust arguments against taking a one-size-fits-all approach to consent during consultations. Rather than take a one-size-fits-all approach, we have taken an approach similar to the European approach in the General Data Protection Regulation (GDPR), which makes consent one of six 'lawful bases of processing.' The GDPR also recognises consent may not always be appropriate and cannot always be relied on. This approach is also consistent with the *Privacy Act 1988*.

We recognise consent can be an important privacy safeguard and should be used where appropriate. The Office of the National Data Commissioner may provide guidance and advice about when and how consent should be built into the Data Sharing Principles.



### Population-level data tells important stories about Australia

#### *Delivering better cardiac outcomes*

In an Australian first, the Victorian Agency for Health Information partnered with university researchers to use a dataset that combined de-identified hospital data with the Pharmaceutical Benefits Scheme data to verify if Australians are being prescribed the right medicines following discharge from hospital for atrial fibrillation (a type of heart arrhythmia) and acute myocardial infarction (heart attack).<sup>26</sup>

Prescriptions for blood-thinning (anticoagulant) agents are considered best practice for most patients being discharged from hospital with atrial fibrillation. Antiplatelet therapies are recommended for most patients with acute myocardial infarction. These medicines are used to reduce the risk of stroke or further heart attack.

The study identified the medicines that over 44,000 Victorians were prescribed in the 30-days following discharge from hospital. The analysis showed that there was significant variation and underuse of the recommended medicines after discharge, depending on where the patient was hospitalised.


The Victorian Agency for Health Information released a report on the research, recommending routine assessment of prescriptions against best practice guidelines at hospital discharge could be used to reduce risks of further complications. Outcomes from this research helped inform improvements in healthcare to save lives.

#### *Helping Australians fight the flu*

The Australian Influenza Surveillance Report is published on a fortnightly basis during the influenza season, typically between May and October.<sup>27</sup> The report is compiled from a number of data sources to monitor influenza activity and severity in the community.

<sup>26</sup> More detail on this research is available at <https://www.bettersafecare.vic.gov.au/reports-and-publications/delivering-better-cardiac-outcomes-in-victoria-an-initiative-of-the-national-data-linkage#goto-delivering-better-cardiac-outcomes-in-victoria-media-release>

<sup>27</sup> The Australian Influenza Surveillance Report and Activity Updates are available at <https://www1.health.gov.au/internet/main/publishing.nsf/Content/cda-surveil-ozflu-flucurr.htm>



**The National Data Commissioner will be empowered to enhance the integrity of the public sector data system and enforce transparency measures.**



# 5. BUILDING TRUST THROUGH TRANSPARENCY

## 5.1 Key Points

1. Transparency is a key pillar underpinning the Data Sharing and Release legislation to build public trust and confidence.
2. The National Data Commissioner will publish registers of Data Sharing Agreements, Accredited Users and Accredited Data Service Providers, and will report annually on the operation and integrity of the data sharing system.
3. The registers will increase transparency about what data is being shared and why and how it is being shared safely, including who is accessing the data.
4. The registers of Accredited Data Service Providers and Accredited Users will show who has been accredited to offer data services, to access and work with data.
5. The Notifiable Data Breaches Scheme in the *Privacy Act 1988* will continue to apply to personal information shared under the Data Sharing and Release legislation.
6. Better sharing and analysis of public sector data also provide transparency of the effectiveness of government policies and programs.

## 5.2 Transparency underpins trust in data sharing

You told us transparency of activities enabled by the Data Sharing and Release legislation is key to building trust. We will embed transparency measures within the legislation and provide for oversight by the National Data Commissioner. The transparency measures include:

- public registers of Data Sharing Agreements containing minimum mandatory terms to show what data is being shared and why and how it is being shared safely, including who is accessing the data
- public registers of Accredited Data Service Providers and Accredited Users to show who is accredited to offer data services, and access and work with data to provide assurance about skills and capabilities to protect, manage and use data
- the National Data Commissioner reporting annually on the integrity of the data system to highlight system-wide opportunities and risks.

The Data Sharing and Release legislation will empower the National Data Commissioner to enhance the integrity of the public sector data system and enforce transparency measures.

### 5.3 Data Sharing Agreements

Data Sharing Agreements will be a requirement for all data sharing under the Data Sharing and Release legislation. The National Data Commissioner will maintain a public register of Data Sharing Agreements that is easily searchable and improves discovery of public sector data.

We asked through our Issues Paper and consultations whether Data Sharing Agreements should be made public by default and what level of detail should be published. We heard consistent support for

publication of Data Sharing Agreements to improve transparency and accountability in the data sharing system. We heard they need to cover content, as outlined below, but to make the data sharing system work more efficiently that you wanted them to be simple, streamlined and consistent. We will also be addressing cost and resource implications associated with sharing data under these agreements. You asked us to provide templates and guidance.

We listened and have developed a template Data Sharing Agreement which we will soon pilot with some government agencies.



#### Proposed mandatory terms of the Data Sharing Agreements

##### WHO IS SHARING AND RECEIVING DATA UNDER THE AGREEMENT

The agreement will identify the entities involved in sharing data, including Data Custodian(s), Accredited Users and any Accredited Data Service Provider (if applicable).

##### WHY IS DATA BEING SHARED

Data sharing under the legislation is only authorised for specific purposes and the terms of the agreement will need to describe in detail how the data sharing meets the purpose test and include any other safeguards that ensure the purpose is authorised.

##### WHAT DATA IS BEING SHARED

A detailed description will describe the data shared under the agreement, safeguards to protect data including its treatment and how the outputs will be handled. The terms will also identify the legislation under which the data was originally collected, any secrecy provision overridden by the Data Sharing and Release legislation and any other responsibilities and liabilities parties are subject to.

##### HOW WILL DATA BE PROTECTED AND RISKS MANAGED

The agreement will describe the agreed safeguards applied across all the **Data Sharing Principles** and how risks will be managed. Where necessary the agreement will address requirements of the Protective Policy Security Framework and any other legislative requirements, including obligations under the *Privacy Act 1988*.

##### WHEN WILL THE DATA SHARING OCCUR

The agreement will specify its duration, any review requirements, the process for amendments and what happens to data after the agreement ends (such as de-identification or destruction).

We welcome your views on these terms and any additional matters you consider essential for building trust through transparency.

## 5.4 Public registers of Accredited Users and Accredited Data Service Providers

The National Data Commissioner will maintain a register of accredited data users and accredited data service providers. The register will be made publicly available so Data Custodians can verify whether those requesting data have already demonstrated their ability to safely and competently handle data.

We are still working out what details will be published in the registers, but it will include information Data Custodians can verify about data users and service providers before entering into Data Sharing Agreements.

## 5.5 Annual reports on the data sharing system

The National Data Commissioner will publish an annual report on the operation and integrity of the data sharing system.

The Data Sharing and Release legislation will require Data Custodians, Accredited Data Service Providers and Accredited Users to provide information to the National Data Commissioner to assist in the preparation of the annual report. The Office of the National Data Commissioner will likely request information about the number of Data Sharing Agreements entered into, information on unsuccessful requests for data and outcomes achieved through greater sharing. These matters will be set in guidance from the Office of the National Data Commissioner.

We think annual system-wide reporting will be a tool for the National Data Commissioner to champion benefits of data and provide positive examples of where greater sharing has led to real-world changes.

Annual reporting on the system will also allow the National Data Commissioner to identify the parts of the system that need more support to share data. For example, Data Custodians may be repeatedly denying requests for data because they may be unsure if it meets the purpose test under the Data Sharing and Release legislation. The National Data Commissioner could issue more tailored guidance to assist Data Custodians to make better assessments of such purposes.


Annual reports will allow the National Data Commissioner to identify Data Custodians that remain unwilling or unable to share data for reasons that are not legislative. Cultural barriers, lack of skills and limited resources were identified by the Productivity Commission as reasons that prevent the maximum benefits of public sector data being realised. Evidence in annual reports will allow the National Data Commissioner to intervene at a systems level and work with government, Data Custodians, Accredited Users and Accredited Data Service Providers to address these barriers.

## 5.6 Data breach scheme

We are currently considering what kind of data breach scheme is necessary to safeguard the Data Sharing and Release legislation. Identification and mitigation of risks associated with data breaches is an important step in safeguarding the system. A breach would be the sharing, release or use of public sector data contrary to the Data Sharing and Release legislation.

The Notifiable Data Breaches Scheme in the *Privacy Act 1988* will continue to apply to personal information shared under the Data Sharing and Release legislation. Under the Notifiable Data Breaches Scheme individuals will continue to receive notification of any real or suspected data breaches involving personal information so they can take action to mitigate the risks. The Data Sharing Agreements may include details of Notifiable Data Breach obligations, including a data breach response plan.

The Data Sharing and Release legislation requires a different kind of notification scheme for the vast range of data falling outside the *Privacy Act 1988* notifications scheme. For example, we are considering options to ensure appropriate protection and notification of breaches involving sensitive data that is not personal information, such as data that is of a legally privileged, commercial-in-confidence, security classified, or environmental nature. We will continue to engage on what the breach notification scheme may look like in the coming months.



**The National Data  
Commissioner will  
provide guidance,  
advice, advocacy  
and regulation of  
the data system.**

# 6. THE NATIONAL DATA COMMISSIONER'S OVERSIGHT OF THE DATA SYSTEM

## 6.1 Key Points

1. The Office of the National Data Commissioner will be an independent statutory authority, responsible for overseeing, regulating and advocating for the use of the Data Sharing and Release legislation.
2. The Office of the National Data Commissioner will embed a philosophy of continuous listening, learning and improving in its work and practices.
3. The National Data Commissioner will provide oversight and control of system-wide risks, taking a graduated enforcement approach for improving compliance with the law.
4. The National Data Commissioner will build trust in the system by accrediting users and data service providers to participate in the data sharing and release system. Accreditation will standardise and streamline existing processes.
5. Accreditation criteria will cover three core principles: skills and capability to protect, manage and use data; privacy standards if handling personal information; and effective governance to manage and use data.
6. The Data Sharing and Release legislation will enable the National Data Commissioner to ensure the accountability and integrity of the data sharing system.

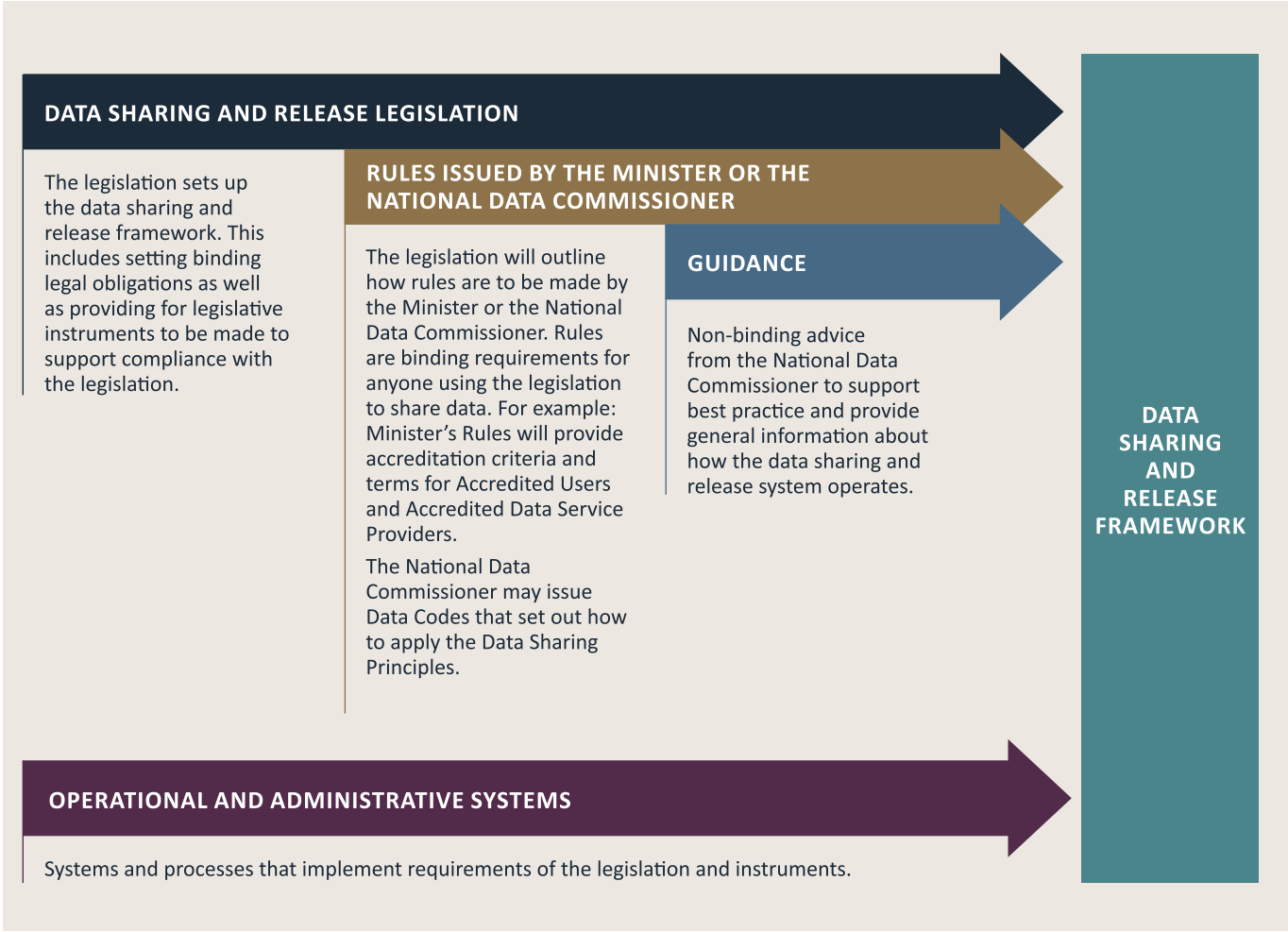
## 6.2 Objectives and functions of the National Data Commissioner

Throughout our consultation, we heard support for the National Data Commissioner both overseeing and being a champion for the data sharing system. Reflecting those views, the National Data Commissioner's objectives are to:

- promote the use and reuse of public sector data
- enhance the integrity of the public sector data system
- engage with the community and build trust about use of public sector data
- apply the Data Sharing and Release legislation in a consistent and effective manner.

To achieve these objectives, the Data Sharing and Release legislation will empower the National Data Commissioner to provide guidance, advice, advocacy and regulation of the system. These functions are enabled through all components of the data sharing and release framework, including the legislation, rules and guidance as well as operational systems (Figure 6).

Figure 6: Data Sharing and Release framework



Guidance to support best practice data sharing and release

Under its guidance function, the National Data Commissioner will support best practice data sharing, release and use and facilitate compliance with the Data Sharing and Release legislation. The Commissioner will identify areas where binding and non-binding guidance is necessary to improve the system through annual reporting and consultation with users, the National Data Advisory Council and other experts.

Binding guidance issued by the National Data Commissioner will be in the form of Data Codes that are legislative instruments. Anyone operating under the Data Sharing and Release legislation will need to abide by these Codes. The Codes will set particular requirements to ensure entities abide by their responsibilities. This additional clarity is important as it supports entities to interpret and apply the principles-based legislation and ensures flexibility as technology evolves. In the first instance, the National Data Commissioner intends to develop a Data Code on handling sensitive data, including personal information, consistently with the Data Sharing Principles established under the Data Sharing and Release legislation.



Non-binding guidance issued or endorsed by the National Data Commissioner will describe the best-practice in sharing or releasing data. Non-binding guidance is intended to help government agencies meet their legislative obligations without being overly prescriptive and may provide more background information such as how processes work in practice. For example, the National Data Commissioner has recently released best-practice guidance on applying Data Sharing Principles to help government agencies apply safeguards that are fit for purpose. Entities must have regard to best practice guidance issued by the Commissioner but are not legally bound by it.

To develop these materials, the National Data Commissioner will draw on existing resources and expertise from government agencies such as the Australian Bureau of Statistics, the Office of the Australian Information Commissioner and the National Archives of Australia.<sup>28</sup>

### **Advice to the Minister and government on the public sector data system**

The National Data Commissioner will be empowered to advise the Minister and relevant entities on the operation of the data sharing system. The National Data Commissioner may also be required to provide advice to government agencies and Ministers under other pieces of legislation.

Under this function, the National Data Commissioner will provide advice, where required, on legislative proposals that interact with the Data Sharing and Release legislation. This could include providing scrutiny comments on Exposure Draft legislation, appearing before Senate Committee Inquiries and consultations with government agencies as they develop and implement legislation.

### **Advocate for cultural change in data sharing and release**

The legislation will also empower the National Data Commissioner to advocate for proper management and greater use, reuse and release of public sector data. This may be via participation in relevant public and private forums, projects, consultations or inquiries. Advocacy will be an important function to achieve cultural change and drive best practice across the data system. Given the cultural barriers and reluctance to share and release public sector data, the National Data Commissioner will focus on providing certainty and clarity where needed, to best achieve and drive sustainable cultural change.

### **Regulate the public sector data sharing system**

A large part of the National Data Commissioner's role will be to provide regulatory oversight of the data sharing system. Effective regulation is a tool to build integrity and trust in the system.

Accreditation and regulatory enforcement are two mechanisms for oversight. Accreditation helps provide assurance for anyone wanting to operate within the Data Sharing and Release system. Our approach to accreditation is outlined in Section 6.3.

Enforcement involves education and actions to help improve compliance with the law. The National Data Commissioner will take a graduated approach to regulatory enforcement by applying proportional responses that deter future non-compliance. This is discussed further in Section 7.5.

---

28 Such as OAIC guidance on de-identification and the Protective Security Policy Framework.

## 6.3 Oversight through accreditation

Throughout our consultations we heard that establishing trust between those requesting data and the Data Custodian was critical to successful negotiations. Accreditation, along with transparency measures discussed in Chapter 5, is an important mechanism for building trust. It can provide assurance not only to Data Custodians, but also the community that organisations and individuals with whom data is shared are competent and trustworthy.

The National Data Commissioner will be able to effectively regulate the system through accreditation, by restricting access to public sector data by revoking or amending accreditation.

Accreditation has been an area of considerable discussion over the last year. You asked us to ensure the processes for accreditation are clear and to help streamline the system. We heard suggestions that accredited individuals shouldn't have to re-start the accreditation process if they change employers. You also asked us about the duration of accreditation and how it would vary for different types of accredited bodies. There was also some confusion about the role the private sector could play in the system, including how they could be accredited under the scheme.

We are continuing to address these questions and concerns. We are seeking a balance that streamlines the system, so it is not onerous or overly bureaucratic while ensuring the accreditation is trusted and respected by Data Custodians and the community.

It is critical that we get this right. There are existing models that we can learn from, including how the Australian Bureau of Statistics currently provides access to data via the DataLab or how researchers are able to access population-based health data via the Sax Institute's Secure Unified Research Environment (SURE). The Office of the National Data Commissioner is consulting government agencies, including those who perform data integration as Accredited Integrating Authorities<sup>29</sup> and experienced groups from the research sector and State and Territory Data Analytics Centres to develop criteria and processes for accreditation. We will seek your views on the processes and criteria alongside the draft Data Sharing and Release legislation.

In line with the principles-based approach to legislation, the accreditation criteria will be provided in legislative rules issued by the responsible Minister. Putting the criteria in legislative rules means the legislation will not be overly prescriptive and provides flexibility to tune the system and address new and emerging risks. Empowering the Minister to make these rules, rather than the National Data Commissioner, provides an added level of accountability and transparency.

The accreditation rules will address core principles contained in the legislation, including:

- skills and capabilities to protect, manage and use data
- privacy standards, if handling personal information
- effective governance to manage and use data.

The Minister's rules may also cover any other matters considered necessary for ensuring the system is safeguarded against new and emerging threats.

The National Data Commissioner will also be able to make rules or provide guidelines on the implementation or other matters necessary to administer accreditation.

### Skills and capabilities to protect, manage and use data

The accreditation criteria in the rules will require that suitable skills and capabilities be demonstrated to ensure that data is protected, effectively managed and safely used. The specific criteria will be dependent on the type of accreditation sought. For example, organisations will have to demonstrate they have access to physical infrastructure capable of secure data use, while individual users within the organisation will have to undergo training that ensures they have the skills to protect, manage and use data.

---

<sup>29</sup> Accredited Integrating Authorities undertake high risk data integration projects involving Commonwealth data for statistical and research purposes. [https://toolkit.data.gov.au/Data\\_Integration\\_-\\_Accredited\\_Integrating\\_Authorities.html](https://toolkit.data.gov.au/Data_Integration_-_Accredited_Integrating_Authorities.html).



### **Privacy standards, if handling personal information**

You told us to consider specific criteria for accreditation for those handling personal information. We think having such criteria will demonstrate a commitment to privacy and will help ensure personal information is handled consistently with the Australian Privacy Principles or their equivalent. This means accreditation could require demonstrating privacy coverage under the Commonwealth *Privacy Act 1988* or equivalent. The Office of the National Data Commissioner is working with relevant stakeholders on the design of the privacy coverage model.

### **Effective governance to manage and use data**

Effective governance includes having the right organisational authority, policies and administrative processes in place to support accountability and good decision making in data management and use. Effective governance benefits all parts of the organisation and improves safe data practices. We heard strong support for accreditation criteria that take these processes and arrangements into consideration.

## 6.4 Operational framework for accreditation

We are proposing to accredit two sets of entities in our system: data users (Accredited Users) and data service providers (Accredited Data Service Providers).

### Accredited Users

An organisation or an individual who may access public sector data.

We have heard support for ensuring that where individuals within an organisation are given access to data, there is a process to accredit both the organisation—to ensure they have appropriate processes and procedures in place to protect the data—and the specific individuals within the organisation—to ensure they are fully aware of their responsibilities when handling public sector data.

The research sector in particular, noted that Data Custodians currently rely on different processes to assess individuals who request access to data. This assessment can take a long time if the Data Custodian does not have an easy way to establish individuals' credentials. We think accreditation of individuals and organisations could help bridge this gap.

The Data Sharing and Release legislation will enable accreditation at two levels—organisations and individuals. The accreditation criteria in the rules will then set out the facilities, processes and governance required for organisations to be Accredited Users, and the set of skills and training and affiliation required to be an accredited individual.

Under the Data Sharing and Release legislation, a Data Custodian will only be able to enter into a Data Sharing Agreement with an Accredited User organisation and will only be able to share data with accredited individuals within that organisation.

This dual-level accreditation will provide independent system-wide assurance to Data Custodians when assessing data requests, so that each Data Custodian won't have to go through the process each time of having to assess base-level skills and capabilities, governance practices and security risks.

### Accredited Data Service Providers

An organisation that meets technical and capability requirements to provide data services to Data Custodians.

In our Issues Paper, we raised how 'Accredited Data Authorities' could be used to meet market demand and support Data Custodians to safely share and release data. We heard broad support for the model and its purpose, but not the name. You told us you did not agree with the name Accredited Data Authorities because 'authority' implied they were the experts and authority on data, which was not the intention.

Instead, the Office of the National Data Commissioner will accredit organisations from public, private and research sectors as 'Accredited Data Service Providers' to assist Data Custodians to make decisions about data sharing under the Data Sharing and Release legislation.

- Data Custodians *may* use Accredited Data Service Providers to undertake sharing and release on their behalf (including related services such as cleaning data, providing secure access and safely storing datasets).
- High risk integration projects *must* be done by Accredited Data Service Providers to ensure existing protections around data integration are maintained and strengthened. The Office of the National Data Commissioner will provide more guidance on what is 'high risk data integration.'<sup>30</sup>

If a Data Custodian chooses to use an Accredited Data Service Provider to undertake data sharing or release on their behalf, then that arrangement will need to be outlined in a Data Sharing Agreement. The Data Sharing Agreement will identify exactly what services and what decisions, the Accredited Data Service Provider will undertake on behalf of the Data Custodian. Data Custodians and Accredited Data Service Providers will have joint legal responsibility for managing the data sharing, with the Data Custodian retaining responsibility for overseeing the Data Sharing Agreement and ensuring the terms are met. This is consistent with the *Privacy Act 1988* and the general principles of contract management.

<sup>30</sup> The identification of high risk integration projects will take into account the existing administrative framework for Accredited Integrating Authorities for high risk integration <https://statistical-data-integration.govspace.gov.au/topics/risk-framework>.



The Data Sharing system and legislation build on and will eventually overtake existing arrangements for data integration involving Commonwealth data for research and statistical purposes (the Commonwealth Arrangements<sup>31</sup>). The transition will occur over time, so existing arrangements made to enable data integration will continue unless the entities involved choose to instead authorise and enable sharing under the Data Sharing and Release legislation. New integration projects will be able to take advantage of the streamlined data sharing opportunities under the Data Sharing and Release legislation. Existing Accredited Integrating Authorities will need to be accredited as Accredited Data Service Providers under the Data Sharing and Release legislation. This process will take into account documents tendered during the Accredited Integrating Authority accreditation process to cut down on duplication.

## Accreditation Process

The rules will set out different accreditation criteria for Accredited Users and Accredited Data Service Providers. In both cases, we will apply the same core principles (see Section 6.3), and, in both cases, we are working towards the same goal of streamlining processes and building trust in the capacity of people who can access data under the Data Sharing and Release framework.

Accredited Data Service Providers will be organisations, whereas accreditation of users will be at both the organisation and individual level.

Organisations applying for accreditation as an Accredited User or Data Service Provider will have to provide evidence they meet the accreditation criteria. Organisations will have to provide evidence of the necessary infrastructure and governance structures to manage and use data safely.

Accredited individuals will have a simpler process: needing to be vouched for by an Accredited User organisation and undertake training provided by the Office of the National Data Commissioner. Individuals will need to pass a test to show they have completed and understood the training.

We are proposing that accreditation would be valid for five years for organisations and three years for individuals. Accredited Users will be required to notify the National Data Commissioner of any changes in circumstances impacting their accreditation status. Once accredited, users will also be required to maintain their obligations to remain accredited.

The National Data Commissioner, in considering applications from potential Accredited Users and Accredited Data Service Providers, will also take advice from the National Intelligence Community on potential threats to national security.

Once the legislation passes, the Office of the National Data Commissioner will take a staged approach to implementation commensurate with resources and reflective of agreed priorities.

## 6.5 Accountability

The Data Sharing and Release legislation will enable the National Data Commissioner to ensure the accountability and integrity of the data sharing system. The legislation will be designed to operate alongside existing accountability and privacy systems, such as the *Privacy Act 1988*, *Freedom of Information Act 1982* and the Protected Security Policy Framework.

Consultation showed broad support for a National Data Commissioner to ensure the integrity of the data sharing system. However, clarification and further information were sought on:

- the types of mediation, complaints and appeals mechanisms in the legislation
- how these would look in practice
- where accountability and responsibility would fall in a data sharing agreement.

The legislation will contain a range of accountability mechanisms (complaints, merits review and judicial review), which operate alongside existing mechanisms, as discussed in Section 7.6. A comprehensive complaints mechanism will also be included in the legislation to ensure an avenue of redress is always available.

31 Details on Commonwealth arrangement for data integration can be found at [https://toolkit.data.gov.au/Data\\_integration\\_-\\_Commonwealth\\_Arrangements.html](https://toolkit.data.gov.au/Data_integration_-_Commonwealth_Arrangements.html)



**The National Data  
Commissioner will  
take a graduated  
enforcement approach,  
applying proportional  
responses to deter  
future noncompliance.**

## 7. WHEN THINGS GO WRONG

### 7.1 Key points

1. The Data Sharing and Release legislation will provide an alternative pathway to share data, where it is currently prevented by a secrecy provision or where it is simpler than existing pathways.
2. Where there is an existing secrecy or non-disclosure provision, the legislation will provide limited statutory authority to share data.
3. If the data sharing is not in accordance with the purpose test or the Data Sharing Principles, the data sharing will rebound to the original secrecy provision.
4. The legislation will include offences and penalties for situations where additional protections may be needed, including where there is not an original secrecy provision, called 'gap coverage.'
5. The National Data Commissioner will regulate the system in a manner that promotes trust, taking a graduated enforcement approach applying proportional responses to deter future non-compliance.
6. Merits review will be provided for decisions made by the National Data Commissioner.
7. Complaints mechanisms will be available to Data Custodians, Accredited Users and Accredited Data Service Providers.
8. Existing merits review and complaints avenues will continue to operate.

### 7.2 Offences under the Data Sharing and Release legislation

#### Rebound approach reinstates offences under the original secrecy and non-disclosure provision

The Data Sharing and Release legislation will provide limited statutory authority to override Commonwealth secrecy and non-disclosure legislative provisions. The override will only apply if sharing is for an authorised purpose and appropriate safeguards are in place. We heard words of caution related to overriding secrecy and non-disclosure offences, as some penalties associated with secrecy and non-disclosure provisions were considered fit for purpose.

In response to these concerns, we have designed an offence approach preserving the secrecy and non-disclosure provisions' penalties and protections. If data is shared for purposes that are not authorised, or if safeguards are not applied correctly under the Data Sharing Principles, the Data Sharing and Release legislation authority will fall away and the original offences and penalties will apply. We are calling this the 'rebound approach.'

The Data Sharing Agreement will point to the legislation and rebound penalties so Data Custodians, Accredited Users and Accredited Data Service Providers are aware of the consequences if something goes wrong.



### **Gap coverage offers additional protection when offences under other legislative provisions are inadequate**

Our system is creating new data sharing and risks. New data sharing will create datasets and instances of sharing not protected by existing offences and penalties. We are introducing new offences and penalties to cover those situations. For example, relatively benign data can become sensitive when integrated with other data to create a new enriched dataset. The original ‘benign’ data may not have attracted offences or penalties under existing secrecy and non-disclosure provisions. The Data Sharing and Release legislation will contain additional protections to address this gap, called ‘gap coverage’.

Under gap coverage, integrated data inherits the protections (such as secrecy provisions) of its source datasets.<sup>32</sup> If one or more of the source datasets were subject to a non-disclosure provision, the integrated dataset would be subject to that provision (or provisions) in the event of a breach. If not, the penalties of the Data Sharing and Release legislation apply to protect the data.

### **When is an offence committed under the Data Sharing and Release legislation?**

The Data Sharing and Release legislation will propose the following offences as a breach of legislation:

- unauthorised sharing, release and use of data
- unauthorised uses of data created under Data Sharing and Release legislation
- providing false or misleading information to the National Data Commissioner
- failure to take reasonable steps to implement safeguards, as agreed in Data Sharing Agreements.

The legislation will also consider offences for non-compliance with any of the following:

- accreditation conditions or other legislated requirements
- a rule (including a Data code) issued under the Data Sharing and Release legislation
- a direction from the National Data Commissioner.

---

<sup>32</sup> In some circumstances data may be derived to an extent that means the original secrecy provision no longer applies.

We think the above offences approach to secrecy and non-disclosure provisions in other legislative schemes maintains and strengthens existing protections. We welcome your views on whether they are appropriate and could be improved further.

### 7.3 Penalties for breaching Data Sharing and Release legislation

In the Issues Paper we asked if penalties for breaching the Data Sharing and Release legislation should be strict liabilities. We consulted the Attorney General's guide to offences and agreed strict liability can be appropriate in some regulatory regimes, especially in public health, but only where the penalty does not include imprisonment or exceed 60 penalty units. Proposed criminal penalties for breaching the Data Sharing and Release legislation will exceed this level.

We also heard use of strict liability could improve trust but would shift the culture in the Australian Public Service to be even more risk-averse and unwilling to share data.

Penalties for breaching these offences will be proportionate and consistent with comparable existing provisions, including in the *Privacy Act 1988* and the *My Health Records Act 2012* (as amended). Penalties will not be strict liabilities to ensure benefits of data can be realised through a culture of responsible data sharing.

The rebound approach and gap coverage of offences will provide for multiple penalties to be applied, but it will be for a court to determine the proportion of liability and quantum of penalties. Where there are multiple pieces of legislation involved, a court will check that the final total penalty is appropriate for the conduct as a whole, considering overlaps between offences to avoid punishing a person multiple times.

We welcome views on whether these penalties balance the appropriate level of deterrence for wrongdoings, while also ensuring entities can confidently operate under the Data Sharing and Release legislation.

### 7.4 What about defences?

The Data Sharing and Release legislation will not introduce any new defences. Instead, existing defences under other legislation may be relevant, including good faith defences under the *Freedom of Information Act 1982* and specific exemptions under Commonwealth secrecy laws.

We heard arguments in favour of creating a good faith defence to protect Data Custodians from criminal liability if they genuinely (in good faith) but mistakenly believed the sharing of data was authorised by the Data Sharing and Release legislation. In assessing options, we found the existing good faith defences under the *Freedom of Information Act 1982* may be relied on for sharing data under the Data Sharing and Release legislation.

The *Freedom of Information Act 1982* could provide immunity from criminal liability and certain forms of civil liability where a Data Custodian shares data and genuinely (albeit mistakenly) believes this was authorised by the Data Sharing and Release legislation. This immunity would not be available if the Data Custodian was driven by wrong or indirect motives such as personal malice, gaining a benefit or an objective not authorised under the Data Sharing and Release legislation.

We found including new defences could water down existing penalties in the rebound approach (see section 7.2) and could lead to negligence in applying safeguards when sharing data. Introducing a new good faith defence in the Data Sharing legislation risks fostering a culture of 'near enough is good enough' when it comes to information security.

Other defences under the *Criminal Code Act 1995* may apply.

## 7.5 Approach to enforcement

### A fair, independent and accountable regulator

The National Data Commissioner will regulate the system in a manner that promotes trust, guided by the following principles:

- Fairness—be consistent, proportionate and efficient.
- Independence—be trusted, impartial and objective, free from undue influence.
- Accountability—be transparent, open to scrutiny and operate responsibly.

The National Data Commissioner’s regulatory functions will include:

- accrediting users and data service providers, including providing an internal review of accreditation decisions made by the National Data Commissioner
- handling complaints from Accredited Users, Accredited Data Service Providers and Data Custodians about the Data Sharing and Release system
- monitoring compliance with the Data Sharing and Release legislation, including conducting assessments and investigations
- determining breaches of the legislation
- enforcing the legislation and imposing penalties.

The National Data Commissioner will be granted regulatory powers necessary to enforce the legislation, including monitoring and investigatory measures. They will work closely with existing regulators, collaborating on and transferring matters as appropriate. The National Data Commissioner will apply a regulatory approach focused on enabling voluntary compliance by prioritising capacity building in the first instance, then deterrence and finally enforcement (see Figure 7).

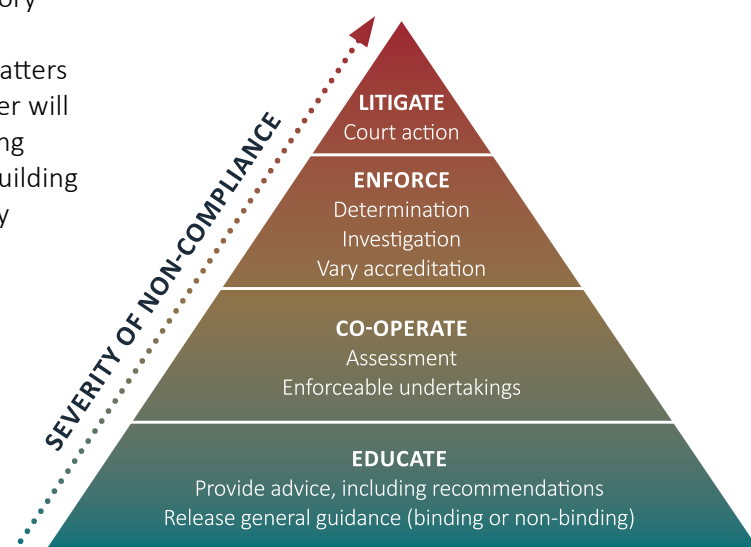
### Graduated enforcement approach

When planning for and responding to non-compliance, the Office of the National Data Commissioner will apply a graduated enforcement approach<sup>33</sup> that applies proportional responses that are likely to deter future non-compliance. Enforcement measures will be applied on a case-by-case basis, considering context and risk.

Education will be used to manage accidental or non-intentional non-compliance with negligible to minor impacts. Co-operation functions will generally be used to prevent, deter or address non-compliance with relatively low impacts that are ongoing or due to careless or opportunistic non-compliance. Enforcement actions will generally be administrative measures used against non-compliance, which is careless or opportunistic, with moderate impacts. Finally, in response to serious or continued non-compliance, the Office of the National Data Commissioner may litigate, pursuing civil or criminal penalties through court action.

The graduated enforcement approach will drive a culture that focuses effort on identifying important problems and tailoring actions to suit the problem. It is an outward-looking tactic, rather than an inward-looking one. The model relies on the National Data Commissioner’s discretion and its effectiveness will be contingent on the National Data Commissioner’s willingness to escalate matters when necessary.<sup>34</sup>

**Figure 7:** The Office of the National Data Commissioner’s enforcement approach



<sup>33</sup> This model is a combination of John Braithwaite’s ‘pyramid of interventions’ and Malcolm Sparrow’s ‘risk-based approach’.

<sup>34</sup> *Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry*.



## Annual priorities

When the legislation commences, the National Data Commissioner will identify annual priorities and have a work plan for the Office's first year of operation. This will include a focus on capacity building under its guidance function, in order to encourage uptake of the legislation in its first year of operation. Enforcement, when it occurs, will use an escalation approach that seeks to encourage voluntary compliance. In the first year of operation, these annual priorities and work plan will be published on the Office of the National Data Commissioner's website shortly after the commencement of the legislation. Subsequently, annual priorities will be developed with and included in the National Data Commissioner's annual report and published on its website.<sup>35</sup>

Annual regulatory priorities for the Office of the National Data Commissioner's first year of operation will reflect areas where uncertainty, complexity, or risk of non-compliance were identified during legislative development.

The Office of the National Data Commissioner will work to ensure that risks and concerns from these focus areas are addressed both in the drafting of the legislation, and preparation of other materials ahead of its commencement. This will be strengthened by a regulatory approach that minimises the residual risk of non-compliance and reviews the effectiveness of the legislation, particularly in these priority areas.

The Office of the National Data Commissioner will publicly announce a shortlist of priority areas, maintaining the longer list for internal prioritisation purposes.

## 7.6 Making a complaint, reviewing a decision, or seeking redress

You told us it was important that the system include avenues for individuals to raise issues or ask for decisions to be reviewed. In response, we are developing different approaches based on the entity making the complaint or seeking review.

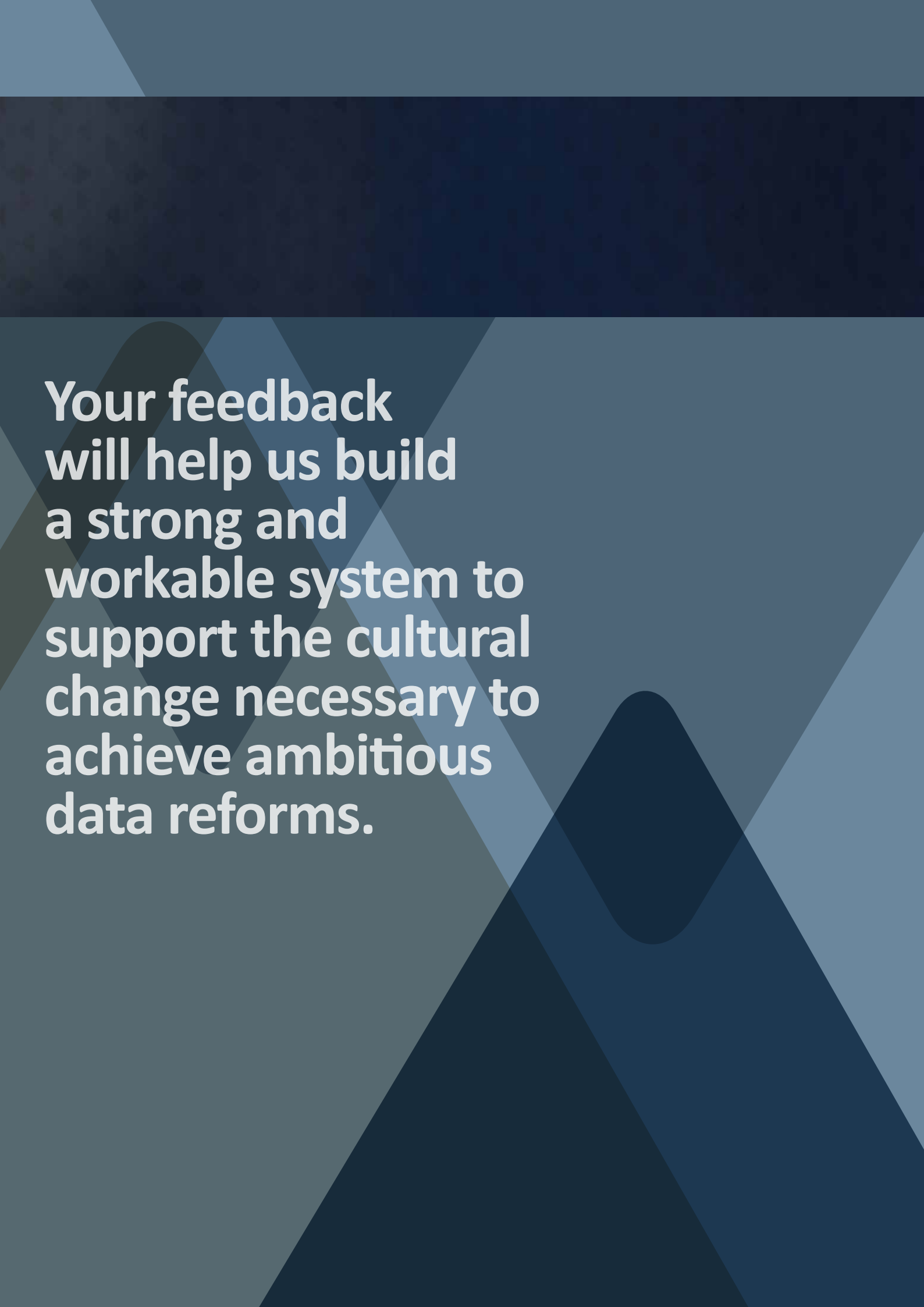
We will include a complaints mechanism for Data Custodians, Accredited Users and Accredited Data Services Providers to raise system-specific complaints with the National Data Commissioner. We will also include merits review and judicial review of decisions made by the Office of the National Data Commissioner. In addition to these new mechanisms, existing avenues, such as complaints under the *Privacy Act 1988* to the Information Commissioner where a suspected mishandling of personal information has occurred will continue.

The Data Sharing and Release legislation will provide internal and external merits review for accreditation decisions. We are also considering whether the National Data Commissioner should be able to issue binding directions to remedy possible breaches of the legislation, or to stop the use of compromised software or data methods. If the National Data Commissioner is able to issue binding directions, they would be merits reviewable.

The Data Sharing and Release legislation will not provide for merits review of data sharing decisions by Data Custodians (for example, decisions to share, the conditions of sharing, or to deny access). Such decisions are best made by Data Custodians who have a greater understanding of the risks and benefits of sharing data.

---

35 Annual reports will be prepared under the requirements of the *Public Governance Performance and Accountability Act 2013*.



**Your feedback  
will help us build  
a strong and  
workable system to  
support the cultural  
change necessary to  
achieve ambitious  
data reforms.**

## 8. WHAT'S THE PLAN FROM HERE?

**The Office of the National Data Commissioner will undertake another round of public engagement following the release of this Discussion Paper. Those consultations will get your feedback on the framework and help us build a strong and workable system to support the cultural change necessary to achieve our ambitious data reforms. You can also provide your views through submissions on this Discussion Paper via our website, [www.datacommissioner.gov.au](http://www.datacommissioner.gov.au).**

We will consider your feedback and update our policy positions to make sure we get it right. In early 2020, we will consult again on an exposure draft of the legislation, including the Data Sharing and Release Bill, Sensitive Data Code, Accreditation Criteria Rules and Explanatory Materials. We will release these documents for public comment for eight weeks and will conduct another round of engagement to hear and incorporate feedback before we finalise the legislation. We are aiming for the Bill to be introduced to Parliament in mid-2020.

---

### **IN EARLY 2020, WE WILL CONSULT YOU AGAIN ON AN EXPOSURE DRAFT OF THE LEGISLATION.**

---

Alongside work to progress the legislation, we are building the foundations and processes for transparent and accountable public sector data sharing. We are working with government agencies to develop effective systems to streamline requests for data and Data Sharing Agreements and searchable registers. We are also developing training and guidance to help government agencies apply the Data Sharing Principles.

It will take time for the data system to mature and for Data Custodians and others to confidently use the new system. We will need to work together to realise the benefits of the new system. The government is committed to maximising the value of public sector data for all Australians.



# ATTACHMENTS

## Attachment A—Key terms

**Accredited Data Service Provider** is an organisation that meets technical and capability requirements to provide data services to Data Custodians.

**Accredited User** is an organisation or an individual who may access public sector data.

**Assurance activities** are considering eligibility, entitlement or liability for government programs and services. For example, an agency checking the data provided on a government form is consistent with data provided elsewhere.

**Collect** is a broad activity that includes gathering, acquiring, generating and obtaining information from any source by any means. This includes directly collecting information from people (e.g. in a survey, Census, or administrative process), creating new information from data already held (e.g. through data integration, or an audit log) and receiving data shared by another entity.

**Compliance activities** are making decisions about whether someone is compliant or not compliant with their legal obligations. This includes activities to identify and prevent fraud against the Commonwealth.

**Data** means any facts, statistics, instructions, concepts, or other information in a form capable of being communicated, analysed, or processed (whether by an individual or by other means including a computer, electronic and automated means).

**Data Custodians** are Commonwealth entities and companies as defined under the *Public Governance, Performance and Accountability Act 2013*, such as agencies and departments, including Commonwealth companies such as Australia Post and NBN. Data Custodians collect or generate public sector data for the purpose of carrying out their functions and have legal responsibility to manage this data. Unlike other entities within the Data Sharing and Release legislative system, Data Custodians do not need to be accredited as they have existing responsibilities over data under contract, government policy and legislation.

**Data sharing** means providing controlled access to the right people for the right reasons with safeguards in place.

**Data Sharing Principles** are risk management safeguards applied prior to sharing public sector data under the Data Sharing legislation.

**Data release** means open data that is made available to the world at large

**De-identified information** is when identifiable information has been treated so it is no longer about an identifiable or reasonably identifiable legal person or natural person, as defined in the *Privacy Act 1988*.

**Government policy** is a rule or principle that guides government decisions.

**Government program** means an organised system of services, activities, or opportunities to achieve something.

**Government service delivery** means government activities to provide coordinated and structured advice, support and services to citizens and customers. This includes activities to improve the user experience of service delivery through simplification (e.g. tell us once), automation and proactive engagement.



**Identifiable information** means information about a legal or natural person that is identified or reasonably identifiable. Intended to capture non-corporate entities.

**National security and law enforcement** means activities to protect Australia from threats and to conduct policing activities.

**Personal information** is defined by the *Privacy Act 1988* to mean information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- a. whether the information or opinion is true or not; and
- b. whether the information or opinion is recorded in a material form or not.

**Protected information and restricted information** means information protected by other legislation or security classifications. This is distinct from ‘sensitive information’, defined below.

**Public sector data** is information collected or generated by Commonwealth entities (such as departments) and Commonwealth companies, or through research programs funded by the Australian government. This includes information collected directly from people through surveys and forms (e.g. to enrol in Medicare) as well as data generated internally through administrative or statistical processes. Data collected by the Commonwealth under commercial contracts and international treaties will remain protected by the terms of those agreements, including any limits to sharing.

**Purpose test** is a threshold issue to determine whether public sector data can be shared under this legislation.

**Research and development** means activities to advance knowledge, contribute to society, better public policy by a range of actors including universities and the private sector.

**Sensitive information** as defined in the *Privacy Act 1988*, is a subset of personal information and includes information about an individual’s health, racial or ethnic origin, political opinions, religious beliefs, criminal record, or biometric templates.

**Sensitive data** means information within the definition of ‘sensitive information’ (above) as well as other types of data that are of a legally privileged, commercial-in-confidence, security classified, or environmental nature.

**Output** means any product created from the original data, such as a cleaned or integrated dataset as well as specific outputs and publications including but not limited to tables, infographics, presentations and journal articles.

## Attachment B—Policy Transitions Overview

ISSUES PAPER POSITION	FEEDBACK	DISCUSSION PAPER POSITION
<b>Approach</b>		
<ul style="list-style-type: none"> <li>• Consultation on proposed positions.</li> <li>• Co-design approach internal to government.</li> <li>• Privacy Impact Assessment on legislation.</li> </ul>	<ul style="list-style-type: none"> <li>• Legislative and cultural barriers need to be overcome to realise the potential of public sector data.</li> <li>• Public conversation on data needs to progress.</li> <li>• Public trust in government handling of data is volatile and malleable.</li> </ul>	<ul style="list-style-type: none"> <li>• Engagement aimed at progressing a public conversation about data, rather than focus on legislation only.</li> <li>• Work to ‘ready the system’ for the legislation, including capacity building and data maturity work in the public service.</li> <li>• Public consultation on independent Privacy Impact Assessment on framework, prior to legislation.</li> <li>• Public consultation on the Exposure Draft of the legislation.</li> </ul>
<b>Framework</b>		
<ul style="list-style-type: none"> <li>• The Data Sharing and Release legislation will establish a national scheme for sharing and release of Commonwealth data with all levels of government and the private sector.</li> </ul>	<ul style="list-style-type: none"> <li>• Strong support from all stakeholders for a broad scope.</li> <li>• Support for greater data release, leveraging existing legislative mechanisms.</li> <li>• Government agencies requested ongoing engagement to negotiate exemptions.</li> </ul>	<ul style="list-style-type: none"> <li>• Legislation will provide authority to share data where it is currently prohibited or complex to do so, provided that the purpose test and safeguard requirements are met.</li> <li>• Legislation will not compel sharing or release.</li> <li>• Exemptions for particular government agencies and legislation will be finalised during consultation on draft legislation.</li> <li>• Legislation will be drafted to enable future development into a national system.</li> </ul>
<b>Purpose Test</b>		
<ul style="list-style-type: none"> <li>• The legislation will authorise data sharing for specified purposes with public benefit.</li> <li>• There will be exemptions for national security and law enforcement data.</li> </ul>	<ul style="list-style-type: none"> <li>• Support for some purposes and concerns about others.</li> </ul>	<ul style="list-style-type: none"> <li>• The legislation will authorise data sharing to inform: <ul style="list-style-type: none"> <li>– government policy and programs</li> <li>– research and development</li> <li>– delivery of government services.</li> </ul> </li> <li>• The legislation will not allow data sharing for: <ul style="list-style-type: none"> <li>– national security and/or law enforcement</li> <li>– compliance and assurance.</li> </ul> </li> <li>• We are still considering how to preclude commercial uses not delivering public benefit.</li> </ul>

ISSUES PAPER POSITION	FEEDBACK	DISCUSSION PAPER POSITION
<b>Safeguards</b>		
<ul style="list-style-type: none"> <li>The legislation will require safeguards applied after assessment against the Five Safes Framework, taking into account data, people, setting, outputs and project risks.</li> </ul>	<ul style="list-style-type: none"> <li>General support for principles of the Five Safes Framework.</li> <li>Support for risk framework being adaptable to changes in technology and processes over time.</li> <li>Concerns raised about the management of sensitive information.</li> </ul>	<ul style="list-style-type: none"> <li>The Data Sharing Principles, an evolution of the Five Safes Framework, are technology-neutral.</li> <li>Legislation empowers the National Data Commissioner to issue binding 'Data Codes'.</li> <li>Sensitive data (including sensitive information) subject to additional safeguards as set in a Data Code to be consulted on alongside legislation.</li> </ul>
<b>Interaction with other legislation</b>		
<ul style="list-style-type: none"> <li>Legislation will provide an alternative authority to share data that is otherwise prohibited.</li> <li>Legislation will operate alongside existing data and information management requirements and legislation.</li> </ul>	<ul style="list-style-type: none"> <li>Strong support for maintaining existing safeguards.</li> <li>Clarity sought on interaction with existing legislation and schemes.</li> <li>Support for legislation being consistent with existing privacy legislation.</li> </ul>	<ul style="list-style-type: none"> <li>Existing legislative mechanisms, requirements and obligations will continue to apply. Legislation is authorised by and consistent with the <i>Privacy Act 1988</i>.</li> <li>The legislation will provide a limited statutory authority to share data, overriding other Commonwealth secrecy and non-disclosure provisions.</li> <li>The National Data Commissioner will work closely with other regulators and refer complaints and issues as appropriate.</li> </ul>
<b>National Data Commissioner</b>		
<ul style="list-style-type: none"> <li>National Data Commissioner as a champion and regulator of data sharing.</li> <li>The National Data Commissioner will work closely with other regulators and be advised by the National Data Advisory Council.</li> </ul>	<ul style="list-style-type: none"> <li>Support for the role of the National Data Commissioner to champion and regulate data sharing system, including to promote nationally consistent processes and standards.</li> <li>Clarity sought on interaction with other regulators.</li> <li>Concern to provide appropriate regulatory powers, but not to discourage use of the system.</li> </ul>	<ul style="list-style-type: none"> <li>The National Data Commissioner is responsible for overseeing and regulating the data sharing system, while advocating for and supporting data release, best practice data management and use.</li> <li>Other regulators retain their remits, including the Information Commissioner's regulatory oversight of the <i>Privacy Act 1988</i>.</li> <li>The National Data Commissioner will have regulatory powers to oversee and enforce compliance with the legislation.</li> <li>Offences will not duplicate existing offences, but will include new offences to cover gaps.</li> </ul>

## Attachment C—Department of the Prime Minister and Cabinet (PM&C) responses to Privacy Impact Assessment recommendations

PM&C engaged Galexia to undertake an independent Privacy Impact Assessment on the Data Sharing and Release (DS&R) framework. PM&C agreed or agreed in principle to all eight recommendations of the Privacy Impact Assessment.

COMPONENT / APP	GALEXIA RECOMMENDATION	PM&C RESPONSE
<b>Key Policy Position 1: Distinguishing between data sharing and data release</b>	<b>Recommendation 1:</b> Splitting data sharing and data release requirements  The requirements in the Bill for data sharing and data release should be split, so that each activity has its own stand-alone set of requirements, tailored for that activity.	<b>Agree</b>
<b>PM&amp;C agrees</b> with this recommendation and notes that the proposed legislative framework already aligns with it. The framework authorises sharing, and will support but not create a new authorisation for the open release of data—the processes are distinct. Guidance and advice issued by the National Data Commissioner may be applicable to both processes—for instance, the Data Sharing Principles can be used to mitigate risks of both sharing and release—but there will be tailored considerations for each process.		
<b>Key Policy Position 1: Distinguishing between data sharing and data release</b>	<b>Recommendation 2:</b> Enhanced privacy safeguards for data release  If data release is authorised by the legislation, then additional legislated enhanced privacy safeguards for data release will be required. These should include: <ol style="list-style-type: none"> <li>1. An additional public interest test;</li> <li>2. A data custodian veto power; and</li> <li>3. Enhanced sanctions.</li> </ol>	<b>Agree in Principle</b>
<b>PM&amp;C agrees in principle</b> with this recommendation, noting that the DS&R framework will support but not authorise open release of data, as noted in response to Recommendation 1.		
<b>Key Policy Position 2: Compliance activities</b>	<b>Recommendation 3:</b> Exclusion of compliance activities  The Bill should exclude compliance activities related to an individual as an approved purpose for data sharing or data release.	<b>Agree</b>
<b>PM&amp;C agrees</b> with this recommendation. While compliance activities are a valid and important function of government, these activities are most appropriately handled under different legislation. Sharing data for compliance activities may occur under specific portfolio legislation, but will not be authorised by the DS&R framework.		

COMPONENT / APP	GALEXIA RECOMMENDATION	PM&C RESPONSE
-----------------	------------------------	---------------

<b>Key Policy Position 3: Covering the States and Territories</b>	<b>Recommendation 4:</b> Additional Data Breach Notification requirements  The Bill should include a mechanism for imposing a Data Breach Notification requirement where the entities involved operate in a State or Territory where such a requirement does not yet exist.	<b>Agree</b>
---	--	--------------

**PM&C agrees** with this recommendation, which aligns with policy intent that entities participating in the DS&R system will have equivalent privacy obligations, including in relation to notification and mitigation of suspected data breaches.

<b>APP 1—Openness and Transparent Management</b>	<b>Recommendation 5:</b> Improved openness in Privacy Policies about data sharing / release  Agencies and accredited entities should be more open about data sharing and the potential disclosure of some data to external users.	<b>Agree</b>
--	--	--------------

**PM&C agrees** with this recommendation, noting that while transparency and accountability are central to the DS&R framework, Privacy Policies are regulated by the Privacy Act not the DS&R framework. The National Data Commissioner will advocate for more transparency on data sharing, including by working with the Australian Information Commissioner to support best practice and agencies' compliance with the requirements of both systems, such as ensuring entities' Privacy Policies reflect their participation in the DS&R system.

<b>APP 1—Openness and Transparent Management</b>	<b>Recommendation 6:</b> Establish a user friendly public information_resource  The National Data Commissioner and any third party entity that is accredited to receive data or act as a Data Service Provider should be required to maintain a user friendly public information resource that lists: <ol style="list-style-type: none"> <li>1. Core data sharing and data release activities;</li> <li>2. Data sources; and</li> <li>3. A register of data sharing agreements.</li> </ol>	<b>Agree in Principle</b>
--	---	---------------------------

**PM&C agrees in principle** with this recommendation, noting that the DS&R framework will require the establishment and maintenance of a public data sharing agreement register that will contain the recommended information on data sharing under the DS&R system. This means data release and data sharing activities relying on other authorisations will not be covered. As additional accountability measures, the National Data Commissioner will report on data sharing activities in the DS&R system in its annual report, and will advocate for greater transparency on data sharing and release activities more broadly.

COMPONENT / APP	GALEXIA RECOMMENDATION	PM&C RESPONSE
-----------------	------------------------	---------------

<b>APP 3—Collection of solicited personal information</b>	<b>Recommendation 7:</b> Minimisation of data collection  The Bill should ensure that data minimisation is a clear requirement for data sharing. The Bill should include the word ‘only’ in the requirement: e.g. ‘sharing only data that is reasonably necessary.	<b>Agree</b>
---	---	--------------

**PM&C agrees** with this recommendation and has implemented it within the proposed framework. The purpose test incorporates the ‘data minimisation’ concept by authorising sharing of only data that is reasonably necessary to achieve an approved purpose.

<b>APP 5—Notification</b>	<b>Recommendation 8:</b> Improved openness in Notices about data sharing / release  Agencies and accredited entities should be more open in their Notices about the use of data sharing and the potential disclosure of some data to external users. <ol style="list-style-type: none"> <li>1. The National Data Commissioner and the Office of the Australian Information Commissioner should consider the following options:</li> <li>2. Development of a standard Notice template;</li> <li>3. Development of Guidance on when and how to issue Notices;</li> <li>4. A prohibition on using data collected prior to the implementation of effective Notices; and</li> <li>5. Checking Notices for compliance.</li> </ol>	<b>Agree in Principle</b>
---------------------------	--	---------------------------

**PM&C agrees in principle** with the recommendation that entities should ensure Privacy Notices reflect their participation in the DS&R system. However, the Department notes that some agencies’ Privacy Notices already inform people that their data may be shared for government and research purposes, which supports the use and reuse of data for these purposes. As such, option 3 of the recommendation may need further consideration. It should also be noted that Privacy Notices are a matter of compliance with the Privacy Act, so are within the remit of the Australian Information Commissioner rather than the National Data Commissioner. The National Data Commissioner intends to work together with the Australian Information Commissioner to support entities to comply with the respective legislative frameworks and consider the recommended options.