



Australian Government

Department of the Prime Minister and Cabinet

Office of the National Data Commissioner

Data Availability and Transparency Bill 2020

Exposure Draft

Consultation Paper
September 2020



Data Availability and Transparency Bill 2020 Exposure Draft Consultation Paper

© Commonwealth of Australia 2020

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 Availability and Transparency Bill 2020 Exposure Draft Consultation 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:

<https://www.datacommissioner.gov.au/form/contact>

Minister's Foreword



If the Australian Government is ever to live up to the expectations of Australians and realise the full potential of its public service, it must make better use of the data it already holds. The promise of digital government is built on better use of data. Data informs decisions makers by ensuring they make better decisions. Data improves service delivery by removing unnecessary friction and pain points. Data is critical to deliver public services that meet the expectations of Australians and equally essential for building a stronger, more prosperous country.

Data and digital technology has been fundamental to the Australian Government's response to the ongoing COVID-19 pandemic and the 2019-2020 bushfire crisis. Navigating these challenges has forced government to adapt and respond. Data has played a key role in determining the size, scope and scale of responses. Whether accessing services wholly online instead of queuing at a Centrelink or using facial verification technology to quickly provide disaster payments to Australians who have lost everything in bushfire affected areas, data has been crucial for getting support to those who have needed it.

Now more than ever, it is clear that we need to get better at using the information we already collect, instead of asking the same questions again and again. For too long, there has been a lack of a consistent and clear framework for making good use of data. We need to make sure the information the government collects and holds can be accessed in a safe and timely way to respond to the needs of Australians. We need to accelerate this Government's commitment to creating a seamless digital experience for the Australian public, now and into the future.

I am confident that the Exposure Draft of the Data Availability and Transparency Bill 2020 provides a strong foundation to enable this seamless experience.

Over the past two years, the Australian Government has continued to actively engage with the public to seek views on this Bill and its policies. We have listened and learned from your experiences to ensure data is used for the right reasons and in ways that deliver public benefit. We remain committed to ensuring the Bill is developed in way that respects the needs and perspectives of many in the community, including the research community, the not-for profit sector, businesses and the public.

Transparency and accountability are strong features of this Bill. It is important citizens know how the Government uses data and what safeguards protect data when it is shared. It is also important that there is strong oversight of the way government data is shared and used. The Bill will establish this oversight and good governance practices. It will also establish an independent National Data Commissioner to uphold the safeguards embedded in this scheme.

My sincere thanks to those who have been on this journey with us over the past two years to develop this legislation. I encourage you to read the Exposure Draft of the Bill and supporting materials to find out more about this Bill. Your feedback will be important to get this important reform right.

A handwritten signature in black ink that reads "Stuart Robert".

The Hon. Stuart Robert MP

Minister for the National Disability Insurance Scheme

Minister for Government Services



Statement From the National Data Advisory Council

The Data Availability and Transparency Bill is an important milestone in the journey to modernising government data sharing and use. The National Data Advisory Council is pleased to see that consultation leading up to the development of this Bill champions exemplar practices in public policy making.

The National Data Advisory Council has been part of this journey since the beginning, and has contributed to the development of the legislation with our views as experts across privacy and data driven organisations, consumer groups, academics and industry. While we provide a range of perspectives on data sharing, we share a common motivation: ensuring data held by the public sector is used in ways that benefit Australians, safely and responsibly. A key part of our role is to provide a sounding board for the interim National Data Commissioner to find the right balance between streamlining the sharing and use of data while addressing privacy and security concerns.

Since our inaugural meeting in March 2019, we have discussed the policy framework underpinning this Bill and its impact, and examined the data sharing reforms from our individual perspectives. Whether it was the ethical use of data or benefits from consumer perspectives, we have challenged positions, debated solutions, and offered new insights.

As a council reflecting a range of perspectives, we appreciate that data initiatives need to acknowledge and take steps to, address, community concerns around privacy and fairness. The Office of the National Data Commissioner has gone to great lengths to engage with stakeholders with a wide range of perspectives, and where possible they have used these views to shape their legislation. We have also noted the transparency with which they have operated, taking care to communicate their work and to listen to stakeholders.

A rigorously safe, streamlined, transparent and accountable framework for sharing data between government agencies and the private, research and non-profit sectors can deliver significant benefits to the Australian community. The National Data Advisory Council looks forward to our continued engagement with the Office of the National Data Commissioner as we move to the next steps in this journey. We also believe this paper and the draft legislation provide another opportunity for the community to engage with this important work.

The National Data Advisory Council

Prof Nicholas Biddle

Dr Alan Finkel

Dr Joshua Meltzer

Ms Ellen Broad

Dr David Gruen

Prof Sallie Pearson

Ms Angelene Falk

Mr Paul McCarney

Ms Lauren Solomon

Contents

Minister's Foreword	i
National Data Advisory Council.....	iii
1. Overview	6
1.1. Modernising, maximising and safeguarding data use will deliver benefits to Australians.....	6
1.2. Reforms target inconsistencies in sharing data	7
1.3. The Data Availability and Transparency Bill enables safe and consistent data sharing practices	8
1.4. The legislation is informed by an ongoing public conversation.....	8
1.5. How to read this document and associated material.....	9
1.6. Have your say and next steps	9
2. The Data Availability and Transparency Bill: A summary.....	10
2.1. Key concepts of the data sharing scheme	11
2.2. The data sharing scheme in practice	12
2.2.1. The accreditation framework controls entry into the data sharing scheme	13
2.2.2. Sharing is only authorised for data sharing purposes.....	14
2.2.3. The data sharing principles are a risk management framework for safe data sharing	14
2.2.4. Data sharing agreements formalise the terms and conditions of a data sharing project	15
2.2.5. The National Data Commissioner will be empowered to oversee the scheme	15
2.2.6. Periodic review of the Bill and its operation	16
3. The Data sharing scheme in practice.....	18
3.1. Ensuring sharing data is in the public interest.....	18
3.2. Projects must observe applicable ethics processes	19
3.3. Consent is necessary unless it is unreasonable or impracticable to obtain.....	20
3.4. Data provided to individuals for validation and control	21
3.5. Protecting the rights and interests of Aboriginal and Torres Strait Islander peoples.....	21
3.6. Data may be used for commercial applications when it is in the public interest.....	22
3.7. Security of the data sharing scheme.....	23
4. Conclusion and next steps.....	24
4.1. Implementing the legislation through Guidelines, guidance and operational systems.....	24
Appendix A.....	25

1. Overview

The Exposure Draft of the Data Availability and Transparency Bill 2020 (the Bill) is a step towards modernising the use of data held by the Australian Government. This consultation paper provides an overview of the materials presented as part of the consultation on the Exposure Draft.¹ Submissions on the Bill and associated materials are requested by 6 November 2020 for the Office of the National Data Commissioner to consider ahead of Parliamentary consideration.

1.1. Modernising, maximising and safeguarding data use will deliver benefits to Australians

The Australian Government is committed to modernising how we use public sector data. Improving how we share and use this data will benefit Australians through more effective government policies, programs, and service delivery, and through improved research outcomes.

The 2019–2020 bushfire season demonstrated that the need for a safe, modern, and streamlined approach to data sharing is more pressing than ever. In its interim observations published on 31 August 2020, the Royal Commission into Natural Disaster Arrangements noted that improving the availability, quality, and comparability of natural disaster information could improve policy and decision making during times of disaster, and improve the delivery of recovery services.²

The data reforms presented in the draft Bill are an opportunity to establish a new framework that can proactively assist in designing better services and policies. The reforms encourage our academics and the research community to innovate and find new insights from public sector data without having to go through stifling and vague bureaucratic processes when working with data custodians.

In 2016, the Productivity Commission set out recommendations to unlock the full potential of public sector data in Australia.³ The Australian Government agreed change was necessary and committed to reforming the Commonwealth data system, including establishing a National Data Commissioner and new data sharing legislation.⁴

In 2018, the Office of the National Data Commissioner was established in the Department of the Prime Minister and Cabinet. Ms. Deborah Anton was appointed as the interim National Data Commissioner to develop and progress whole-of-government reforms to realise the benefits envisaged by the Productivity Commission.

Since its establishment, the Office of the National Data Commissioner's key task has been to develop legislation to overcome existing legislative barriers and enable a streamlined, safe, accountable, and transparent pathway to share data. This consultation paper provides an overview of the elements of the legislation, including the Bill and associated materials, for your views.

1 Exposure Draft of the Bill available at <http://www.datacommissioner.gov.au/exposure-draft>

2 Interim observations available at <https://naturaldisaster.royalcommission.gov.au/publications/interim-observations-1>

3 Productivity Commission's Data Availability and Inquiry report available at <https://www.pc.gov.au/inquiries/completed/data-access#report>

4 Government's response to the Productivity Commission's recommendations available at <https://dataavailability.pmc.gov.au/>

The National Data Advisory Council was established in 2019 to provide advice to the National Data Commissioner on ethical data use, community expectations, technical best practice, and industry and international developments.⁵ Members represent a broad cross-section of perspectives, covering government, business, academia, and community interests. The Council members are data industry leaders with a strong understanding of the Australian and international data landscape.

Since its establishment, the Office of the National Data Commissioner has also been working to improve practices around governance and management of data. This includes providing guidance for applying data sharing principles,⁶ standardised data sharing agreements⁷ to build consistency, and the release of Foundational Four⁸ data practices to improve data capabilities.

1.2. Reforms target inconsistencies in sharing data

Government agencies have often taken a black-and-white approach to data access and use, whereby agencies have kept some data in-house ('closed') or have made non-sensitive data publicly available ('open').

Data is also 'shared' with trusted users with controls in place, but often in an ad hoc manner or with inconsistencies across government. Reforms to data sharing can enable data to be as open as possible and as closed as necessary.⁹

Keeping data **closed** can at times provide the strictest protections for privacy and security. However, in many circumstances, it is possible to manage the risks of sharing to unlock the potential of data. We have heard

from many stakeholders that some data has more value – including to the data custodians themselves – when it is able to be shared. There are also significant risks to the community when data is not shared: closed data risks research not using the best or most relevant information, government policies not being targeted where they are most needed, and citizens finding it difficult and laborious to access government services. Closed data also keeps the Australian public in the dark about what the government does with the data it collects and holds.

Releasing data **openly**, through data.gov.au or other websites, has economic and social benefits, as anyone can access and use this data to analyse, innovate, and develop tools that have public value.¹⁰ Before being released, privacy and security risks must be addressed – open data cannot be retracted or protected against future uses and misuses, and for some data, it is never appropriate to be open.

When data is **shared**, access is granted to users in a controlled manner, for example, under memoranda of understanding or through contracts. Currently, sharing is done in an ad hoc manner, with users potentially having to establish their credentials every time they interact with the system. Sharing is subject to legislative protections and the individual agencies' interpretations of them. Often interpretations are not revisited as technology evolves and community expectations around reasonable use and reuse of data change.

This sharing space is ripe for reform. Modernising the safeguards and regulating the sharing space can enable Australians to benefit from better services, policies, programs, and research.

5 More information on the National Data Advisory Council including current membership are at <https://www.datacommissioner.gov.au/about/advisory-council>

6 Guide to applying the data sharing principles are at <https://www.datacommissioner.gov.au/resources/sharing-data-safely-package>

7 A draft data sharing agreement template has been released <https://www.datacommissioner.gov.au/resources/draft-data-sharing-agreement-template>

8 Foundational Four is a guide to managing data effectively <https://www.datacommissioner.gov.au/resources/foundational-four>

9 The Australian Research Data Commons (ARDC) also noted the principle adopted by the European Commission to keep data "as open as possible but as closed as necessary," see: <https://ardc.edu.au/news/research-data-rights/>

10 The 2015 Australian Government Public Data Policy Statement directs agencies to make all non-sensitive data open by default to maximise the benefits of government data.

1.3. The Data Availability and Transparency Bill enables safe and consistent data sharing practices

The Bill creates an accountable and transparent data sharing scheme for the Australian Government to safely share public sector data by providing controlled access to the right people, for the right reasons, where safeguards must be in place.

The Bill will not undermine or invalidate existing data sharing arrangements that are working successfully for all participants. Rather, the Bill will provide an alternative pathway to share data where it is currently prevented by secrecy provisions or where it simplifies existing pathways. In such cases the Bill provides greater consistency, streamlines access, and provides accountability and transparency to build and maintain community trust.

“The Bill will not undermine or invalidate existing data sharing arrangements that are working successfully for all participants. Rather, the Bill will provide an alternative pathway to share data where it is currently prevented by secrecy provisions or where it simplifies existing pathways.”

Recent events have brought the need for this Bill into clear focus: data is crucial to effectively manage, respond to and learn from crises. By sharing data more readily, the Australian Government can use the wealth of data it holds to deliver timely and better targeted services to those in need. It means different government services are able to pre-populate information, saving citizens time and effort; policies and programs are fit for purpose and unintended consequences are reduced;

and researchers are able to help shape government policies and better understand their impact.

The Bill streamlines sharing by overriding secrecy provisions and non-disclosure prohibitions on sharing.¹¹ It introduces consistent accountabilities and safeguards so public sector data is only shared with accredited users when it is appropriate and safe to do so. The integrity of the data sharing scheme is enhanced by establishing the role of a National Data Commissioner to provide oversight of the scheme and advocate for better practices in sharing and releasing data. All data sharing participants are responsible and accountable for keeping data safe under the Bill, including data custodians and users.

These responsibilities include strong privacy safeguards for personal information, such as the protections of the Australian Privacy Principles and the notifiable data breaches scheme under the *Privacy Act 1988*.

1.4. The legislation is informed by an ongoing public conversation

The Bill and supporting materials are the result of more than two years of extensive engagement during which we listened, learned, and improved the policies that underpin the legislation. We spoke to hundreds of stakeholders, released an Issues Paper,¹² and a Discussion Paper,¹³ received 187 public submissions, hosted 76 roundtable forums, and convened 11 co-design workshops across the Australian Public Service. While we recognise not all views can be reflected in the draft Bill, the Bill aims to strike an appropriate balance between the many competing perspectives and the objectives of the data reforms.

We embedded ‘privacy by design’ in the approach taken to develop this Bill to strengthen protections for individuals’ privacy. Privacy formed part of the policy design from the start and privacy impacts were considered throughout. We commissioned two independent Privacy Impact Assessments (PIA) to ensure we considered privacy from the inception

¹¹ The Bill contains some exclusions from the override, including for contractual arrangements that prevent sharing.

¹² Issues Paper available at <https://www.datacommissioner.gov.au/resources/2018-issues-paper>

¹³ Discussion Paper available at <https://www.datacommissioner.gov.au/resources/discussion-paper>

of policies to the drafting of the Bill. The first PIA¹⁴ focused on the broad framework for sharing and identified its strengths and weaknesses to make eight recommendations that we adopted in the draft Bill. The second PIA, published alongside this paper, assesses whether we have implemented the policy framework into legislation successfully. Our responses to the recommendations made in this PIA are at Appendix A.

Aboriginal and Torres Strait Islander peoples' perspectives were important when drafting the Bill. We consulted with Aboriginal and Torres Strait Islander peoples, together with the National Indigenous Australians Agency (NIAA), to ensure the data reforms considered their data sovereignty concerns and worldviews on data collection and use. This is discussed more in Section 3.5.

This consultation period is another opportunity to make our views heard and help shape these important reforms.

1.5. How to read this document and associated material

This Consultation paper provides a summary of the legislation and accompanying legal and technical documents. Some stakeholders will dive straight into the Bill and Explanatory Memorandum for details, but others may need a map, this Consultation Paper, to navigate the materials.

This summary draws on and should be read in conjunction with the following documents:

1. The exposure draft of the Data Availability and Transparency Bill and the supporting draft Explanatory Memorandum.
2. The exposure draft of the Data Availability and Transparency (Consequential Amendments) Bill 2020 and the supporting draft Explanatory Memorandum.
3. The exposure draft of the Data Availability and Transparency Regulations 2020 and the supporting draft Explanatory Statement.
4. The draft second independent Privacy Impact Assessment and Department of the Prime Minister and Cabinet's response.
5. The discussion paper seeking your feedback on developing the accreditation framework to support the Bill.

These documents are all available on the Office of the National Data Commissioner website at www.datacommissioner.gov.au

1.6. Have your say and next steps

We want to hear your views on the Bill, Regulations, and the accreditation framework. Our consultation period runs for eight weeks and is an opportunity for you to provide formal written submissions to the Office through our website (www.datacommissioner.gov.au). Submissions are due by 6 November 2020, and we encourage you to get in touch early.

To support this feedback process, the Office will host a series of webinars to provide information and answer questions. Please check the website¹⁵ for further details.

Following consultation on the Exposure Draft of the Bill, we will make necessary amendments to the Bill, Regulation, and Explanatory Materials, before presenting to Government for its consideration prior to introduction into Parliament. The Bill will be operational once it receives Royal Assent from the Governor-General. A National Data Commissioner will then be appointed to oversee and regulate the data sharing scheme.

There will also be opportunities to have your say as we operationalise the Bill.

¹⁴ Privacy Impact Assessment of the framework available at <https://www.datacommissioner.gov.au/resources/2019-privacy-impact-assessment>

¹⁵ To find out more about information sessions, please visit <http://www.datacommissioner.gov.au/exposure-draft>

2. The Data Availability and Transparency Bill: A summary

The Exposure Draft of the Data Availability and Transparency Bill 2020 (the Bill) establishes a new data sharing scheme to modernise how the Australian Government shares data.

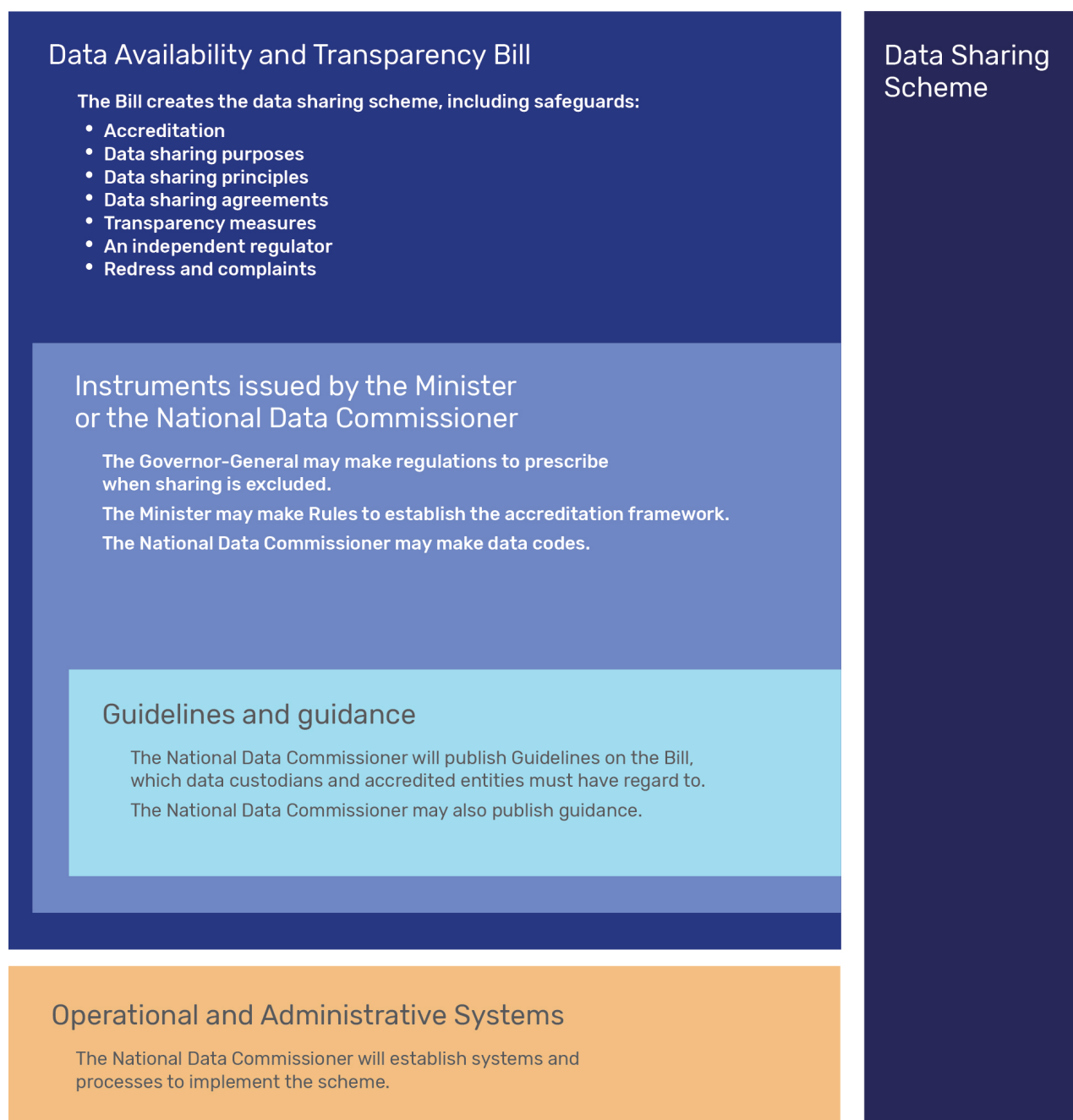
The Bill creates a scheme of controlled access ('data sharing') to public sector data. This scheme includes a system of safeguards to manage risk and streamline sharing processes and establishes an independent regulator for its oversight. The Bill takes a principles-based approach to data sharing, providing parties with the flexibility to tailor sharing arrangements, and allowing the scheme to evolve in line with technology and community expectations. Modernising the approach to sharing public sector data will empower the Government to deliver effective services and better informed policy and programs, and support research and development.

The Bill aims to:

- promote better availability of public sector data
- enable consistent safeguards for sharing public sector data
- enhance integrity and transparency in sharing public sector data
- build confidence in the use of public sector data, and
- establish institutional arrangements for sharing public sector data.

The Bill, in taking a principles-based approach, is supported by secondary legislative instruments, Guidelines, and guidance to provide details on the use of the scheme (see Figure 1). The Regulations, Rules, and Data Codes are legal instruments that are subject to Parliamentary scrutiny. The Bill gives specific powers to the Minister to issue rules and the National Data Commissioner to issue codes that detail how to apply the legal provisions. Guidelines and guidance to use the scheme provide another layer of prescriptive detail that participants need to consider when sharing data under the scheme. The National Data Commissioner will also set up operational and administrative systems to implement the scheme and support the effective streamlining of data sharing processes.

Figure 1 – Components of the data sharing scheme established by the Bill



2.1. Key concepts of the data sharing scheme

The Bill will **authorise sharing of public sector data by data custodians with an accredited user, only for the permitted data sharing purposes and only if effective safeguards are in place.**

“The Data Availability and Transparency Bill will **authorise sharing of public sector data by data custodians with an accredited user, only for the permitted data sharing purposes and only if effective safeguards are in place.**”

The Bill provides an optional and alternative **authority** for the Australian Government to share public sector data.¹⁶ The authority is considered optional as there is no obligation to share; and alternative as existing pathways may continue to be used to authorise sharing where they are working effectively for all parties. Data **sharing** means providing controlled access to data and does not include open data release.

Public sector data is data lawfully collected, created, or held by or on behalf of a Commonwealth body.

A Commonwealth body¹⁷ is the **data custodian** of public sector data that they control and have the right to deal with. Data custodians must establish they have the authority to enter into a data sharing arrangement for the data they wish to share. This may include a consideration of the conditions under which the data were collected, including other laws, conditions of collection, or contractual arrangements.

To access data under this scheme, users must be **accredited** by the National Data Commissioner through Rules established by the Minister. Accreditation streamlines access by ensuring users meet requirements on security, privacy, governance, and technical skills and capabilities. The Bill also allows the Commissioner to accredit experts as **accredited data service providers** to help share data safely, making use of contemporary tools and techniques. Accredited data service providers must meet the accreditation criteria set by the Minister in rules.

Permitted data sharing purposes for sharing data are for delivery of government services, to inform government policy and programs, and for research and development. The Bill does not authorise sharing for **precluded purposes**, including enforcement-related purposes, for example for law enforcement, compliance, and assurance purposes. It also precludes sharing for a purpose related to, or that prejudices, national security. National security is defined as Australia's defence, security, international relations, or law enforcement interests. While these precluded purposes are considered

legitimate functions of government, they are more appropriately managed through existing pathways with their oversight and redress mechanisms.

The Bill provides layers of **safeguards**, including the data sharing principles, which are based on an internationally recognised framework for managing risks associated with sharing data.¹⁸ The principles guide how risks are assessed and managed and must be applied to each data sharing project across five dimensions (projects, people, data, settings, and outputs).¹⁹

A **data sharing agreement** formalises the data sharing arrangements, including detailing what safeguards are in place. The National Data Commissioner will publish details of the agreement to build transparency and accountability in the data sharing scheme.

The National Data Commissioner will **oversee** the scheme and report annually on its integrity and operation. The Commissioner will also educate and promote good data practices, including data management and governance.

2.2. The data sharing scheme in practice

The Bill ensures data is only shared if prescribed conditions are met. It includes layers of safeguards to build trust in the data sharing scheme and its operation, including:

1. an **accreditation framework** to control entry into the data sharing scheme and establish users' and service providers' data capability
2. **data sharing purposes** to ensure data sharing is in the public interest
3. **data sharing principles** to ensure data sharing is done safely
4. consistent **data sharing agreements** to set legally binding requirements for data sharing

¹⁶ Some exclusions to this override are provided in the Bill and the Draft Regulations to Data Availability and Transparency Bill 2020.

¹⁷ Commonwealth body includes commonwealth agencies and companies under the *Public Governance, Performance and Accountability Act 2013*, and some other entities including officers and Norfolk Island authorities covered by the *Freedom of Information Act 1982*.

¹⁸ Based on the Five Safes framework (Desai, T., Ritchie, F., & Welpton, R. (2016). *Five Safes: Designing data access for research*).

¹⁹ See the guide to applying the data sharing principles are at <https://www.datacommissioner.gov.au/resources/sharing-data-safely-package>

5. strong **transparency mechanisms** and effective **oversight** by the National Data Commissioner, and
6. The Bill, and its operation, will be reviewed periodically to ensure it remains fit for purpose.

2.2.1. The accreditation framework controls entry into the data sharing scheme

The accreditation framework facilitates participation in the data sharing scheme by users and data service providers from different sectors such as government, business, academia, think tanks, and not-for-profit sectors.

Accreditation will control entry into the data sharing scheme, serving as a safeguard to provide:

- visibility and regulation of participants in the data sharing scheme
- transparency and accountability of accredited entities through public registers
- a consistent and reusable process for entities to enter the scheme and request public sector data, and
- information to support data custodians when making decisions about sharing data.

Accreditation will be established through multiple legal mechanisms. The Bill provides the National Data Commissioner with the power to accredit entities, regulate their activities, and place conditions on, suspend or cancel accreditation.

The accreditation framework will be established through Rules by the Minister responsible. It will provide for types of accreditation, assessment criteria, and details about the process, duration, and conditions of accreditation.

The Bill and Rules will also be accompanied by Guidelines and guidance to support participants to apply for, manage, and maintain their accreditation. The National Data Commissioner may also issue codes in the future if necessary to clarify accreditation requirements in practice.

More detail about the key elements of the accreditation framework, including types of accreditation, proposed criteria, application and assessment process, and public registers, can be found in the discussion paper on the accreditation framework.



2.2.2. Sharing is only authorised for data sharing purposes

The Bill authorises sharing for three data sharing purposes – for delivery of government services, to inform government policies and programs, and for research and development:

- **Government services** are government activities that provide coordinated and structured advice, support, and services to individuals. Sharing data for this purpose could enable improved designs of systems, engagement, and processes involved in the delivery of services, including improving user experiences through simplified or automated systems like pre-filled forms and reminders to submit or verify details.
- Sharing data to inform **government policy and programs** is a broad purpose that could help enable the discovery of trends and risks to inform public policymaking, enable modelling of policy and program interventions, and provide a holistic understanding of cross-portfolio impacts and ‘wicked problems’; that is, intersectional problems which are complex in nature and for which no single solution exists.
- Sharing data for **research and development** includes activities to advance knowledge and contribute to society. Sharing for research and development will enable academics, scientists, and innovators in the public and private sectors to access public sector data to gain insights that could enhance Australia’s socio-economic wellbeing.

While the permitted data sharing purposes are intentionally broad, the precluded purposes are specific and use existing legal concepts to limit the permitted purposes as required. The Bill precludes the sharing of data for national security purposes, including activities to prevent domestic terrorism or espionage, and for purposes that would prejudice national security,

such as terrorism or espionage. The Bill also precludes data sharing for enforcement-related purposes, such as law enforcement, policing, compliance, and assurance activities (see also Section 2.1 on precluded purposes). The Minister may prescribe additional precluded purposes in rules to address future risks. The Minister could only narrow the existing scope and is unable to authorise new purposes for sharing.

The Bill excludes sharing that would infringe intellectual property rights or international agreements, or where intelligence agencies²⁰ or their data are involved.

The Bill excludes the sharing of operational data and evidence before courts, tribunals, and certain agencies with oversight or integrity functions to protect the independence and confidentiality of their core functions. Some legislative provisions have also been excluded from the Bill’s override to preserve protections around, for example, national security, My Health Records and COVIDSafe app data (see also the exposure draft Data Availability and Transparency Regulations).

“Some legislative provisions have also been excluded from the Bill’s override to preserve protections around, for example, national security, My Health Records and COVIDSafe app data.”

2.2.3. The data sharing principles are a risk management framework for safe data sharing

The data sharing principles are a risk management framework to assess risks of sharing data and identify ways to manage those risks. The data sharing principles must be applied to each data sharing project.

The principles are:

- **Project Principle:** data is shared for an appropriate project or program of work, including consideration of the public interest, and ethics, while maintaining strong privacy safeguards.

20 Domestic intelligence agencies include the Australian Secret Intelligence Service, the Australian Secret Intelligence Organisation, the Australian Geospatial-Intelligence Organisation, the Defence Intelligence Organisation, the Australian Signals Directorate, and the Office of National Intelligence.

- **People Principle:** data is made available only to appropriate persons, who have the right training and skills.
- **Setting Principle:** data is shared in an appropriately controlled environment, which is safe and secure.
- **Data Principle:** appropriate protections are applied to the data, including applying the data minimisation principle so only the required data is shared.
- **Outputs Principle:** outputs are as agreed, and appropriate for future use.

The Bill requires the data custodian and users to be satisfied that, when the principles are considered as a whole, the risks associated with sharing data are appropriately managed. The controls under each of the principles can be 'dialled up' or 'dialled down' as necessary to manage risks and provide safe data sharing.

2.2.4. Data sharing agreements formalise the terms and conditions of a data sharing project

Data sharing agreements are a key governance and transparency measure. They set out the terms and conditions for projects under the data sharing scheme. All sharing arrangements under the Bill must be recorded in a data sharing agreement that includes a set of minimum mandatory terms. These standardised terms will support greater consistency and clarity of obligations and reduce the need for complex negotiations.

Data custodians can add additional terms to the agreement, however, the National Data Commissioner may not be able to enforce them.

The agreements can be changed or updated, for example, to include additional accredited users or to address changes in the scope of a project. Variations will need to be reported to the National Data Commissioner, and responsibilities to apply safeguards to manage overall risk will continue to apply.

Information from data sharing agreements will be published by the National Data Commissioner in a register to support transparency and oversight of the scheme. The register will provide insight into what data is being shared, with whom and for what benefit, and how safeguards are being applied.²¹

The National Data Commissioner will have regulatory oversight of data sharing agreements, and powers to monitor and enforce compliance with participants' responsibilities under this Bill.

2.2.5. The National Data Commissioner will be empowered to oversee the scheme

The Bill empowers the National Data Commissioner with advice, guidance, regulatory, and advocacy functions to oversee the scheme. The Commissioner will promote better sharing and release of public sector data by driving cultural change and supporting capability building among data scheme entities. The Commissioner will also accredit entities to build trust in the system, and standardise and streamline existing processes.

The National Data Commissioner has a range of regulatory powers available to monitor and enforce compliance with the Bill, similar to other Australian government regulators. The Commissioner can respond to complaints or raise their own investigations if they have reasons to suspect a breach of the scheme.

The Bill enables the Commissioner to take a graduated approach to regulatory enforcement and publish process guidance on how they will apply their powers. Following an investigation, the Commissioner could give recommendations, accept and enter into enforceable undertakings, issue written directions, issue infringement notices, seek injunctions, or seek civil or criminal penalties from a court.

As a statutory office holder, the National Data Commissioner will be independent in performing and exercising their powers and functions. The Commissioner will be supported by public servants of the Department of the Prime Minister and Cabinet (the Department), and contractors and consultants where appropriate.

21 A draft data sharing agreement template has been released <https://www.datacommissioner.gov.au/resources/draft-data-sharing-agreement-template>

To avoid potential regulatory conflict when regulating the Department, the Bill ensures that only the Commissioner exercises regulatory authority over the Department. The Bill requires the Department to provide adequate staffing to the Commissioner to perform its functions, and that the Commissioner has discretion in the performance of their role.

The Bill establishes a National Data Advisory Council as a source of expertise, to support the Commissioner through advice on ethical data use, community expectations, technical best practice, and industry and international developments. Members of the Council are appointed by virtue of their depth of experience and expertise relevant to the data sharing scheme.

Complaints, redress, and merits review

Taking a no-wrong door approach to handling complaints, the Commissioner will work collaboratively with other oversight and integrity agencies to ensure the appropriate body handles a complaint. The Bill includes a scheme-specific complaint mechanism for data scheme entities to complain to the National Data Commissioner about actual or suspected breaches of the Bill by another data scheme entity.

Merits and judicial review will be available for decisions made by the National Data Commissioner such as accreditation decisions. Existing avenues for redress are unaffected, such as complaints to the Ombudsman about the actions of Australian Government agencies and complaints to the Australian Information Commissioner under the *Privacy Act 1988* where a suspected mishandling of personal information has occurred.

The Bill does not provide for merits review of data sharing decisions by data custodians. Data custodians' sharing decisions will be capable of challenge through judicial review channels, such as the *Administrative Decisions (Judicial Review) Act 1977*. If decisions are made using data shared under the Bill that impact individuals, existing merits review avenues apply. For example, if an output that exited from the data sharing scheme is subsequently used to pursue a compliance action against an individual under another law, then merits review under that law will be available to review such decisions.

The National Data Commissioner will not be able to overturn a decision not to share data as there is no duty to share using the Bill. However, as part of their annual reporting, the Commissioner could seek to identify reasons for such denials and improve guidance to resolve any uncertainty leading to those decisions.

Registers

Making information publicly available and being transparent about the operation of the data sharing scheme and who is using data for what purposes helps build public trust and confidence. The Bill requires the National Data Commissioner to publish registers of data sharing agreements, accredited users, and accredited data service providers.

Publishing information about the participants accredited in the data sharing scheme and the data sharing projects can also support greater discovery of public sector data and how it is used to drive innovation. It can uncover what data already exists, and reduce the need to collect it multiple times.

2.2.6. Periodic review of the Bill and its operation

The Data Availability and Transparency Bill is drafted as principles-based to remain relevant and adaptable to evolving technology and public expectations. The Bill, legislative instruments, Guidelines, and guidance will be reviewed periodically to ensure the data sharing scheme operates as intended, and to provide an opportunity for improvement.

As a new scheme impacting data across government, the Bill will be reviewed three years after commencement which could assess its effectiveness. Periodic reviews will then occur every ten years from commencement to address emerging issues, with reports to be tabled in Parliament.

The National Data Commissioner will report annually on the operation of the data scheme and address any systemic issues to protect data while encouraging its greater sharing and use.

The data sharing principles in practice at the Australian Bureau of Statistics

The data sharing principles are based on the Five Safes Framework already guiding several agencies to safely share data. Below illustrates how data sharing principles (in the form of Five Safes Framework) are currently being applied in practice at the Australian Bureau of Statistics (ABS). These practices can guide data custodians in providing access to data under the proposed legislation.

The Multi-Agency Data Integration Project (MADIP) is a secure data asset combining information on healthcare, education, government payments, personal income tax, and population demographics to create a comprehensive picture of Australia over time. Authorised government and non-government researchers can access MADIP data for approved research projects. Recent projects have produced insights into a wide range of government policy areas – for example, income growth, suicide prevention, welfare dependence, and educational attainment.

The ABS is responsible for combining MADIP data, providing access to authorised users via highly secure ABS systems, and safeguarding privacy in collaboration with its partners. The ABS provides access to MADIP data through the Five Safes Framework (equating to the data sharing principles) to effectively manage risk and maximise the use of shared data.

Safe Projects (Project Principle): The ABS assesses each project proposal to ensure it will deliver public value, is not for compliance or other regulatory purposes and that the data is suitable to meet the analytic requirements. The project is approved by each of the relevant data custodians (including the provision of Public Interest Certificates) and an ABS manager.

Safe People (People Principle): Each individual named on projects must undertake mandatory ABS DataLab safe researcher on-boarding before they are provided access. This includes a half-day face-to-face interactive training, focused on the shared responsibility for maintaining data confidentiality, as well as security protocols and expectations when using ABS microdata data. The user must pass a quiz on their understanding of the training. All users sign documents agreeing to

use the data responsibly and uphold confidentiality, including conditions of use from data custodians. Sanctions, including legal penalties, a suspension, or access ban may be applied if users do not abide by their responsibilities. Each individual must belong to an organisation that has a Responsible Officer Undertaking in place with the ABS.

Safe Settings (Setting Principle): Access to the MADIP data is provided through the ABS DataLab. This is a closed system within the ABS IT environment with controls including secure login using two-factor authentication, logging, and auditing of activity, role-based data access (data is accessed on a 'need to know' basis in accordance with the requirements for approved projects) and the researchers cannot import or export data. Users are also made aware of their responsibilities around physical access environments and data security through the DataLab training. Access is only supported within Australia.

Safe Data (Data Principle): No direct identifiers are provided to users and only those MADIP variables that are approved and necessary for the project are provided. The data is prepared to ensure information is not likely to enable the identification of the individual or organisation. As part of DataLab training, users understand their obligations for responsible use of data, including not attempting to re-identify individuals or organisations.

Safe Outputs (Outputs Principle): All outputs are vetted and approved by an ABS officer before removal from the DataLab to ensure no data is released in a manner that is likely to identify an individual or organisation. The outputs must also be consistent with the stated aims and expected outcomes in the project proposal. The outputs must also meet any data custodian requirements, including broad confidentiality and any project-specific conditions. Users are trained in their obligations with regards to outputs as well as good practice in preparing outputs that are non-disclosive. No unit records are released from the DataLab.

3. The data sharing scheme in practice

In September 2019, the Office of the National Data Commissioner released a Discussion Paper presenting our policy thinking and sought views about arising issues in data sharing. Key areas included:

- ensuring sharing data is in the public interest
- the requirement for consent unless unreasonable or impracticable
- adherence to ethics processes to determine the merits of a project
- protecting the rights and interests of Aboriginal and Torres Strait Islander peoples
- the public interest derived from commercial applications of data sharing, and
- maintaining the security of the scheme.

Submissions and forums with stakeholders across the country helped shape our policy thinking, but we recognise more needs to be done. As we operationalise the data sharing scheme, greater clarity will be provided in these areas. Here we provide a summary of what we have heard on the above issues and our approach to addressing them. The Office of the National Data Commissioner will continue engaging further as we operationalise the data sharing scheme, including as we prepare the Guidelines and guidance to help participants operate effectively in the scheme.

3.1. Ensuring sharing data is in the public interest

The desire to serve the public interest underpins the Australian Government's drive to better share and use public sector data through the Data Availability and Transparency Bill 2020 (the Bill). A common query about the data sharing scheme is how it will define when sharing is in the public interest. The term 'public interest' is not defined in the Bill because it is an evolving concept.²² There is no universally accepted approach to measuring the public interest, but there is agreement that transparency and consultation in the process are vital for building trust and accountability.

The Bill requires data scheme participants to describe how the public interest is served by the sharing before any sharing can commence. The transparency requirements in the Bill support scrutiny of the scheme by the public and the National Data Commissioner. The data sharing agreements – which will capture how all of the safeguards are applied – will be published on a public register. This transparency promotes accountability across the scheme, putting the onus on decision-makers to demonstrate to the public how the public interest is served by the sharing.

Community expectations around public interest are subjective and change over time. This gives data

²² The Australian Law Reform Council in its 2014 report on "Serious Invasions of Privacy in the Digital Era" made a case against defining public interest, stating that defining public interest could "be overly general or overly confined and inflexible" as well as be unable to respond as "community expectations of privacy changes over time". The report is available at <https://www.alrc.gov.au/publication/serious-invasions-of-privacy-in-the-digital-era-dp-80/8-balancing-privacy-with-other-interests/meaning-of-public-interest/>

custodians and users flexibility in how they evaluate the public interest that is served by a particular project as community expectations evolve. However, it also gives them a greater responsibility to be aware of the implications of the project and to be sensitive to current community expectations.

Evaluating public interest of a project needs to cover multiple domains, and data scheme participants must consider how the public interest is served across each of them. This will include a consideration of the potential benefits and risks to the economy, public health, the environment, and overall social wellbeing. The evaluation also has to pay attention to the risks and benefits for individuals and businesses as well as population groups, including vulnerable communities. The risks of not sharing should also form part of this evaluation.

Special care should be taken when assessing the public interest where sharing involves the private sector or vulnerable groups. While there may be short term benefits of sharing such as increased jobs in a particular sector, the sharing may also lead to an unfair competitive advantage to certain businesses. Likewise, some proposed sharing may appear to benefit the wider community, but may be at the expense of vulnerable groups. Public interest assessments need to outline these risks and benefits and explain how they have been weighed against each other.

Such a process inevitably requires subjective judgements to be made, and the scheme requires custodians to apply and demonstrate rigour in this process.

The National Data Commissioner will be responsible for providing guidance to help data scheme participants evaluate and articulate how the public interest is served by a particular project. Guidance on applying the data sharing principles under the Bill will clarify how the Project Principle is applied to assess and demonstrate public interest. During the consultation period, we invite comment on the position that the public interest is served by good public policy delivered by effective institutions in line with community expectations and norms and welcome views on what matters the most to you when it comes to evaluating the public interest of a project.

“We welcome views on what matters the most to you when it comes to evaluating the public interest of a project.”

Importantly, the requirement to demonstrate public interest is not the only safeguard determining whether data should be shared for a particular project. The Project Principle also requires data scheme participants to consider the ethics of a project (see also section 3.2) and to seek consent from individuals unless unreasonable and impracticable (see also section 3.3). In addition, ensuring the security of the data being shared is a requirement of both the accreditation framework and the settings principle within the data sharing principles (see section 3.7).

3.2. Projects must observe applicable ethics processes

A consideration of the ethics of a project plays an important role in determining the merits of a particular use of data. It also evaluates whether the project is in the public interest in a way that balances the interests of individuals and broader society and reduces potential impacts on vulnerable communities.

Where an ethics process is currently mandated, that mandate will continue to apply to projects under this Bill. The Project Principle requires that applicable processes relating to ethics are observed and projects have regard to their recommendations. This means sharing projects such as those involving human-centred data may need to undergo an ethical review to identify and weigh up their risks and benefits. Such reviews facilitate mitigation or minimisation of the risk and severity of possible physical or psychological harm, discomfort, or inconvenience to data subjects that may arise through data collection, use, analysis, and publication.

Many research institutions have long-established institutional ethics committees, processes, and norms to help provide this assurance. These should continue to be leveraged by data scheme participants where possible.

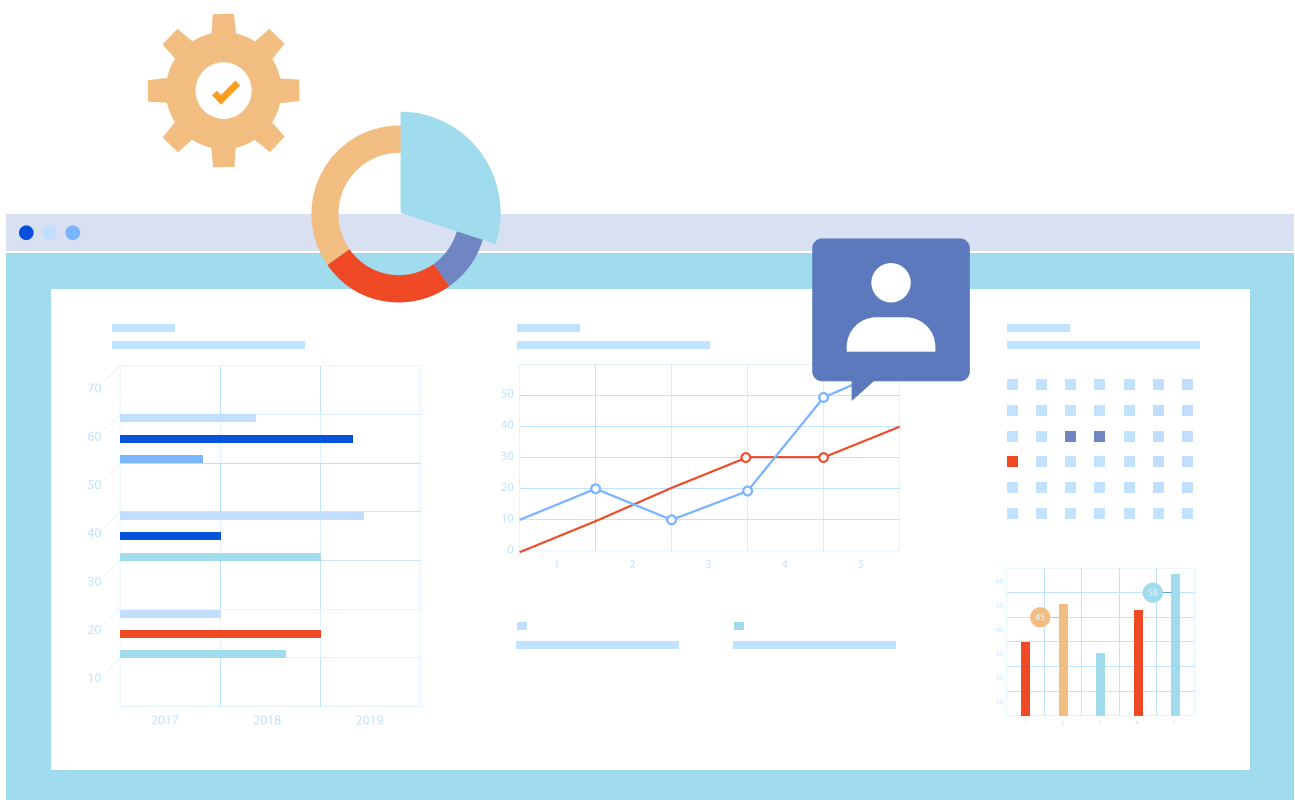
The applicable form of ethics review will depend on the kind of project. Some projects may be reviewed by data custodians themselves, while others may require formal review by a Human Research Ethics Committee (HREC) registered with the National Health and Medical Research Council (NHMRC).²³

Before sharing data, data scheme entities should consider seeking independent advice on the ethical implications of the project and how to mitigate identified risks. Details of any ethics considerations and observed processes will be documented in the project's data sharing agreement.

The National Data Commissioner may provide further guidance on relevant ethics processes, or direct data custodians or users to seek advice from experts for projects with complex ethical considerations.

3.3. Consent is necessary unless it is unreasonable or impracticable to obtain

The data reforms have been developed using a privacy by design approach, which has considered the role for consent. We have undertaken two independent privacy impact assessments, which have developed and support our approach to consent (see 2020 Privacy Impact Assessment of the Bill, section 6.5). Under the Project Principle, any sharing of personal information is done with the consent of the individuals, unless it is unreasonable or impracticable to seek their consent. The consent standard of 'unless unreasonable and impracticable' is modelled on the *Privacy Act 1988*.



23 Data scheme entities can refer to the NHMRC's National Statement on Ethical Conduct in Human Research, available at <https://www.nhmrc.gov.au/about-us/publications/national-statement-ethical-conduct-human-research-2007-updated-2018>

We heard about consent in public submissions on our Issues and Discussion Papers, in roundtable forums held across Australia, from the public service, and in conversations with stakeholders. Conversation ranged from the positive around the value of consent in sharing and using public sector data; to caution that while consent can be used to protect privacy it should not be applied as the only privacy protection; to the risks of inadequate consent being used instead of protecting privacy. We heard other concerns with consent, including that there are currently inconsistent consent practices in Australia, and requiring consent for all data sharing could lead to biased data that delivers the wrong outcomes.

As a result of these conversations and in recognition of the important role consent plays in government data handling, the consent requirement has been elevated into the Bill. In the Discussion Paper, we had proposed only having the requirement in guidance on the application of the data sharing principles.

For projects where data scheme entities do not seek consent, other safeguards outlined by the data sharing principles can be dialled up to protect privacy. Other privacy-enhancing measures include using de-identified data where possible and undertaking a privacy impact assessment as required under the Australian Government Agencies Privacy Code. Information about a project, whether the project requires consent and what other privacy safeguards have been adopted, will be recorded and published in the data sharing agreement.

Anyone who suspects misuse of their personal data or that a privacy breach has occurred can make a complaint to the Privacy Commissioner. The National Data Commissioner could also launch their own investigations to address any systemic failures in the data sharing scheme or in applying safeguards to protect personal information.

3.4. Data provided to individuals for validation and control

In 2020, we have acutely felt the need for the Government to have access to up to date information to deliver timely and reliable services to people. The Bill enables government agencies to share data to inform

service delivery, such as pre-filling forms. In practice, this could mean that those affected by the 2019-2020 bushfire season and the COVID-19 pandemic can receive eligible government services quickly and easily in a time of need, without having them provide the same information many times over to different government agencies.

The Bill allows accredited users to provide individuals and businesses with data about themselves. The data custodian and the accredited user would need to agree to the sharing in the data sharing agreement, and it must be consistent with the permitted data sharing purposes and data sharing principles. Individuals and businesses receiving their own data do not need to be accredited by the National Data Commissioner. Once data has been provided to the individual or business, they are in control of their data and can provide it to whomever they choose to, outside of the Bill's protections.

By allowing participants to provide data to individuals and businesses, the Bill allows government agencies to check the accuracy of data. In most cases, this sharing will likely occur to facilitate service delivery, such as pre-filling forms for individuals and businesses applying for government services. Individuals and businesses may choose to provide validated data to agencies for precluded purposes, such as assurance and compliance. This is similar to how the current myTax scheme operates: individuals are provided with prefilled information the ATO gathers from a range of sources, which the individual then checks and provides to the ATO to determine compliance with tax laws.

3.5. Protecting the rights and interests of Aboriginal and Torres Strait Islander peoples

We heard a range of views around greater sharing of data about Aboriginal and Torres Strait Islander peoples throughout the development of the Bill. Views expressed covered issues including appropriate ethics processes, data sovereignty, and data governance, and questions about who benefits from the value created from data about Aboriginal and Torres Strait Islander peoples and cultures. We also heard views on obtaining consent,

including questions of best practice and of obtaining free, prior, and informed consent (FPIC) under international human rights standards.

The Bill will support the data policies developed by the National Indigenous Australians Agency and require users to adhere to applicable policies and processes when sharing and using data about Aboriginal and Torres Strait Islander peoples. All relevant ethics processes under current arrangements, such as the Australian Institute of Aboriginal and Torres Strait Islander Studies (AIATSIS) Code of Ethics – Guidelines for Ethical Research in Australian Indigenous Studies, will continue to apply and will need to be considered under the Project Principle to demonstrate the public interest of a given project. Similarly, data custodians and users could apply the CARE Principles²⁴ when designing data governance systems as part of applying the safeguards under the Bill.

Data custodians and users can also seek direct advice on methodologies, governance, and protocols for working with Aboriginal and Torres Strait Islander data from a range of government and non-government entities. These could include AIATSIS, the University of Melbourne's Indigenous Data Network (IDN), the Aboriginal and Torres Strait Islander Data Archive (ATSIDA), and Maïam nayri Wingara Aboriginal and Torres Strait Islander Data Sovereignty Collective.

Aboriginal and Torres Strait Islander peoples and organisations could also benefit from using the Bill to seek access to certain data about their communities and cultures, or provide specialised expertise on Aboriginal and Torres Strait Islander data to other accredited users. Having greater access to their data and making their knowledge more available can empower communities to drive better services, policies, programs, and research for collective benefit.

“The layers of safeguards will protect identified personal information from misuse, particularly where businesses may seek to profit from this data.”

3.6. Data can only be used for commercial applications when it is in the public interest

Stakeholders recognised the potential of data sharing to benefit the public but also raised that there is a strong need for oversight when data is shared for commercial applications. A range of approaches to measuring and ensuring public interest were considered, including formal ethics approvals and evidence of proper consideration of the risks and benefits of data sharing projects. This feedback shaped changes in our policy positions.

Data sharing can benefit the public when it is done safely and effectively, such as when public sector data is used to support research to create better products and services for the community. For example, a research project to improve pharmaceutical treatments for heart disease could deliver both profits for the researcher as well as a public health benefit.

The layers of safeguards will protect identified personal information from misuse, particularly where businesses may seek to profit from this data. This does not limit the benefits from using more aggregated data in a safe setting to deliver useful research that is in the public interest. Existing protections around direct marketing, and for competition and consumers, continue to apply. Any data shared under the Bill will also be subject to the standards set in the *Privacy Act 1988* and the *Australian Competition and Consumer Law*.

Where sharing has commercial applications, safeguards in the form of data sharing principles and transparency measures embedded in the Bill work together to authorise projects that deliver public interest, for example, sharing of data results in research outputs that could develop life-saving drugs. In particular, projects must be for permitted data sharing purposes, and have controls applied under the data sharing principles to manage risks. Details of the project and its expected outputs and benefits, will be recorded in a public data sharing agreement. If the public interest of a data sharing project is not satisfied, the authorisation to share does not exist. Section 3.1 describes the factors to consider when

24 CARE Principles for Indigenous Data Governance are available at <https://www.gida-global.org/care>

evaluating public interest. Guidance on applying the data sharing principles under the Bill will assist the data sharing scheme participants to demonstrate the public interest of a project.

The National Data Commissioner may also issue further guidance, directions or data codes, to steer users toward appropriate uses.

3.7. Security of the data sharing scheme

In the current data-driven society, there are genuine concerns about how the security of the data sharing scheme will be maintained as technology evolves. We are increasingly reliant on digital services, and malicious actors can prey on data about individuals and businesses if it is not kept secure. The loss of data through negligent sharing practices, or poor transparency of records about who shared data and for what reasons, further erodes public trust in the Government's ability to keep data safe. Poor practices in some non-government organisations, including universities, businesses, and not-for-profit organisations, could also erode this trust. Without appropriate oversight, data security can be neglected, misused, or mishandled.

The Bill, while being technology-neutral, provides a pathway to ensure security is addressed to an appropriate standard when sharing data. For entry to the data sharing scheme, participants need to be accredited. There are three broad accreditation criteria established by the Bill that cover 1) governance and administrative frameworks, 2) security and privacy of data, and 3) technical skills and capability. The accreditation rules (see Discussion Paper on accreditation framework) will provide the next layer of detail about specific thresholds and requirements that entities must meet to participate in the scheme. As a legislated instrument these can be updated over time and quickly if needed to address a security threat.

The data sharing principles embed another layer of defence to protect data, including the Settings Principle.

The Settings Principle considers whether all parties have taken reasonable steps to ensure data will be used in an appropriately safe and secure environment, i.e. one that minimises the likelihood of unauthorised use, access, or loss of data. Data custodians need to consider the practical controls, in both physical and IT environments that can be put in place to control how data is stored, transferred, and accessed. Controls will depend on whether the entity will be provided access to the data (for example, via a web service, secure facility, or API) or be given the data itself (for example, by download or physical media).²⁵

Above are also reasons for data custodians to consider the use of the data sharing scheme even if an authorisation to share data is not needed. The consistent practices and streamlined framework provides a safe, secure, and trusted alternative to ways in which data is currently shared.

To ensure the security of the scheme continues to receive strong attention, the Office of the National Data Commissioner is also working with other government agencies with expertise in security including those responsible for cybersecurity and national security.



25 See Best Practice Guide to Applying Data Sharing Principles, released March 2019 - <https://www.datacommissioner.gov.au/resources/sharing-data-safely-package>

4. Conclusion and next steps

Better sharing of public sector data can lead to improvements in services, policies, and research outcomes. It can transform everyday life, drive efficiency and safety, create productivity gains, and allow for better government decision making. Recent crises highlight the need to improve the availability of data across the government to improve government policy service delivery during crises. The Exposure Draft of the Data Availability and Transparency Bill 2020 aims to modernise and streamline how public sector data is shared while maintaining strong protections to keep data safe.

We want to hear your views on the exposure drafts of the Bill, Regulations, and the accreditation framework. Your feedback will help us ensure we build a strong and workable scheme that will enable safe, controlled, accountable, and transparent data sharing. Head to our website, where you can register for a webinar for a further explanation of the Bill and accreditation framework, or submit your feedback.²⁶

Following consultation, we will consider your feedback and make necessary amendments to the Bill to make sure we get the reforms right. We will then provide the Bill to the Government for consideration and introduction to the Parliament.

4.1. Implementing the legislation through Guidelines, guidance and operational systems

Our work doesn't stop there. Alongside progressing the legislation, we have continued to work with government agencies to develop effective systems to support the implementation of the Bill. This includes developing training and guidance to help government agencies apply the data sharing principles.

It will take time for the data sharing scheme to mature and for participants to confidently use the new scheme. To support this, we will continue to build the foundations and processes required for transparent and accountable public sector data sharing. We remain committed to continuing to publicly engage as we modernise how public sector data is shared, and to maximising its benefits for all Australians.

26 Feedback can be provided at <http://www.datacommissioner.gov.au/exposure-draft>

Appendix A

Privacy Impact Assessment of the Exposure Draft of the Data Availability and Transparency Bill

The Department of the Prime Minister and Cabinet (PM&C, or the Department) engaged Information Integrity Solutions, led by former Australian Privacy Commissioner Malcolm Crompton, to undertake an independent Privacy Impact Assessment (PIA) on the Exposure Draft of the Bill. Taking an iterative privacy by design approach, this builds on the first independent PIA on the framework. In the PIA, Information Integrity Solutions support the 'layers of defence' in the Bill, including data minimisation and consent requirements, which have the potential to work together to identify and carefully manage privacy risks related to any data sharing project.

Department of the Prime Minister and Cabinet's Response to PIA Recommendations

The Department has made the following responses to the recommendations of Information Integrity Solutions (IIS) in their independent draft Privacy Impact Assessment (PIA) of the Exposure Draft of the Data Availability and Transparency Bill (the Bill), as at **4 September 2020**. The PIA is draft, to allow for update if the Bill is changed following Exposure Draft consultation. The Department will review its responses if the recommendations change.

IIS Recommendation	PM&C Response	PM&C Comments
<p>Recommendation 1: Align accreditation requirements with Australian Privacy Principle (APP) 1 and give regard to Office of the Australian Information Commissioner (OAIC) advice on privacy governance and management.</p> <p>Align accreditation framework requirements with Privacy Act 1988 (Privacy Act) governance requirements (including under APP 1). To do this, consult the OAIC and give regard to OAIC advice on complying with APP 1, establishing good privacy governance and developing a privacy management plan. For example, the accreditation framework could require entities to have a privacy management plan in place that aligns with OAIC's advice.</p>	Agree	The Department agrees and notes that the proposed accreditation framework is being developed in consultation with the OAIC.
<p>Recommendation 2: Ensure that accreditation involves regular assurance that standards are being met.</p> <p>Ensure accreditation rules for Data Scheme Entities contain provisions that require entities to regularly check and confirm their compliance with accreditation obligations. This could take the form of a compliance statement or audit report that confirms compliance, including in relation to personal information handling. The NDC should track and enforce Data Scheme Entities' ongoing assurance requirements.</p>	Agree	The Department agrees and confirms the accreditation framework will include procedures and requirements in relation to maintaining accreditation. The National Data Commissioners powers will also include suspending or cancelling an entity's accreditation.

IIS Recommendation	PM&C Response	PM&C Comments
<p>Recommendation 3: Draft DAT Bill to effectively exclude sharing for 'compliance and assurance' purposes</p> <p>Ensure that the DAT Bill is drafted in such a way that there is no doubt that 'precluded purposes' include compliance and assurance. The EM and supporting guidance material should also make clear that compliance and assurance activities are precluded.</p>	Agree	The Department agrees and confirms the drafting of 'enforcement related purpose' includes compliance and assurance activities. Enforcement related purpose is adapted from the same concept in the Privacy Act 1988, which also uses the concept to include compliance and assurance. The draft Explanatory Memorandum makes this intention clear.
<p>Recommendation 4: Articulate meaning of permitted purposes in Explanatory Memorandum (EM).</p> <p>Address the expected data sharing purposes in the EM, giving examples of what would and would not fit within these terms, in particular in relation to compliance. Make clear that private sector organisations could become accredited entities and that any commercial activities must be consistent with the permitted purposes.</p>	Agree	The Department agrees and confirms it has included description of the permitted and precluded purposes in the draft EM.
<p>Recommendation 5: Provide guidance on the ethics process in appropriate circumstances.</p> <p>Specify, in supporting guidance material, when and how a Data Scheme Entity should undertake an ethics process and the nature of the process required. Possible circumstances to consider include cases:</p> <ul style="list-style-type: none"> • Involving sensitive information • Where seeking consent is impracticable or unreasonable • When it is not possible to use de-identified data • Where the sharing would have a commercial application for the Accredited User • Where there may be community concern about the proposed sharing. 	Agree	The Department agrees and will develop guidance to provide advice on ethics.
<p>Recommendation 6: Provide guidance on how consent operates in the data sharing scheme.</p> <p>Specify, in the EM, guidelines and other guidance material, matters such as:</p> <ul style="list-style-type: none"> • The definition and standard for consent (including referring to other authoritative sources where available), • That consent should be the norm for personal information sharing associated with the delivery of government services, • The kinds of sharing purposes that will usually warrant consent, • The kinds of circumstances that justify proceeding without consent. 	Agree	The Department agrees and will develop guidance on how consent operates in the data sharing scheme.
<p>Recommendation 7: Specify 'privacy' in the National Data Advisory Council's (NDAC's) advisory functions.</p> <p>Specify the matters that NDAC is to advise on in the Bill, including: ethics; balancing data availability with privacy protection; and trust and transparency.</p>	Agree	The Department agrees and has added privacy to the NDAC's advisory functions in the Bill, along with a non-exhaustive list of other functions.

IIS Recommendation	PM&C Response	PM&C Comments
<p>Recommendation 8: Review effectiveness of the National Data Commissioner (NDC) support and staffing model in first statutory review of the Act</p> <p>Review effectiveness of the NDC support and staffing model during the first statutory review of the Act. The NDC and the NDAC should be asked to provide input on this issue as part of the review. The review should consider how the model supports or detracts from the ability of the NDC to carry out their statutory functions, including monitoring compliance with the scheme and investigating complaints.</p>	<p>Agree in principle</p>	<p>The Department agrees and confirms the first statutory review after three years of the scheme's commencement will most likely consider the effectiveness of the Bill and data sharing scheme, including NDC operation.</p>
<p>Recommendation 9: Develop and publish a regulatory action plan.</p> <p>Develop and publish a regulatory action plan that specifies the NDC's approach to its oversight and the use of their enforcement powers. The plan should cover matters such as:</p> <ul style="list-style-type: none"> Monitoring the data sharing scheme (including compliance with accreditation conditions, implementation of data sharing purposes, nature and extent of commercial applications, data minimisation, consent practices, breaches involving or resulting from de-identification practices, etc.), Monitoring changes in the operating environment brought about by technological and other change that may impact privacy, Addressing privacy impacts by: issuing new supporting guidance or amendments to existing guidance; issuing a data code; reporting concerns to the Minister; advising the Minister on matters requiring rules; proposing amendments during legislative review; any other appropriate measures, including enforcement against specific Data Scheme Entities. 	<p>Agree</p>	<p>The Department agrees and confirms the Office of the National Data Commissioner will develop a regulatory action plan to support the National Data Commissioner (NDC), once the Bill commences and the NDC becomes the scheme regulator.</p>
<p>Recommendation 10: Individuals to have access to simple arrangements for addressing privacy complaints and issues</p> <p>Work with the OAIC and other privacy regulators to ensure:</p> <ul style="list-style-type: none"> The interface between the data sharing scheme and individuals is simple and effective There are simple and effective mechanisms in place to enable individuals to find information about the data sharing scheme and assert their privacy rights. This may include a 'no wrong door' policy and swift transfer of enquiries or complaints to the appropriate entity (whether that be a data scheme entity or the privacy regulator). 	<p>Agree</p>	<p>The Department agrees and has been working closely with the Attorney-General's Department and the OAIC to avoid regulatory duplication and provide clarity around regulatory remits. The Bill includes mechanisms to enable transfer of complaints and information sharing with the OAIC and other oversight bodies. These mechanisms support the 'no wrong door' approach and facilitate streamlined arrangements between the NDC and other oversight bodies, including the OAIC. The Department will continue to work with the OAIC on implementation of the scheme, including arrangements making use of these provisions.</p>

IIS Recommendation	PM&C Response	PM&C Comments
<p>Recommendation 11: Measure and report on individuals' interaction with the scheme.</p> <p>Work with the OAIC to develop indicators and to measure individuals' interaction with the scheme to check their ability to navigate privacy issues and seek help or remedies. This could include gathering information on the number and nature of:</p> <ul style="list-style-type: none"> • Privacy enquiries the NDC receives, • Privacy inquiries or complaints the NDC transfers to a data scheme entity, • Privacy enquiries the OAIC receives about the scheme, • Privacy complaints the OAIC resolves, • Other metrics that give insight into the operation of the scheme with respect to individuals, • Report metrics in the appropriate annual report (either the NDC or the OAIC). 	<p>Agree in principle</p>	<p>The Department agrees in principle and will implement reporting obligations, including annual reporting. Reporting is intended to cover the interactions of individuals with the data sharing scheme, within legal and other constraints. The Department will work with the OAIC on developing indicators and measures that align with the reporting requirements of the data sharing scheme and with the OAIC's information sharing powers.</p>
<p>Recommendation 12: Allow for shortening the period for review of the Act and make reviews public.</p> <p>Retain the initial review of no later than three years after commencement. The initial review should focus on whether the provisions establishing the data sharing scheme are operating as intended and whether the privacy protections are fit-for-purpose in the present operating environment.</p> <p>Subsequent reviews should formally consider whether the next review should occur sooner than 10 years, taking into account:</p> <ul style="list-style-type: none"> • How the scheme is operating in practice, including any privacy impacts of concern • The changing technology landscape • Amendments to the Act, especially those that significantly expand the scheme or otherwise have the potential to impact privacy. <p>The reviews of the Act and the government responses should be made public.</p>	<p>Agree in principle</p>	<p>The Department agrees in principle. The Bill requires regular statutory reviews to consider the operation of the scheme, including the review requirement. As is evidenced in the transparency mechanisms in the Bill and the transparent nature of the Bill's development, the Department is committed to continuing transparency around its operation. To the extent possible, the Department agrees any review and Government responses will be made publicly available.</p>

IIS Recommendation	PM&C Response	PM&C Comments
<p>Recommendation 13: Conduct public awareness campaign about the data sharing scheme.</p> <p>The NDC, in collaboration with other relevant stakeholders, should conduct a public awareness campaign to promote the data sharing scheme. The campaign should involve multiple channels – such as posters, mail, videos or other multi-media, Data Custodians and other government websites and social media – to maximise reach. The campaign should occur before the launch of the scheme, and should feature easily-accessible information about the following:</p> <ul style="list-style-type: none"> • The benefits that the scheme will bring to individuals and the wider public, • An explanation of potentially concerning (non-)permitted purposes, including commercial activities and compliance/assurance, • An overview of the framework in place to protect privacy and security, • How individuals can ask questions and exercise their rights. 	<p>Agree</p>	<p>The Department agrees and intends to conduct public communications, including undertake digital advertising on the Exposure Draft of the Bill supported by videos and easy to access website content. A public awareness campaign, involving easily-accessible information, will be core to ensuring that the public is aware and informed about the scheme.</p>

