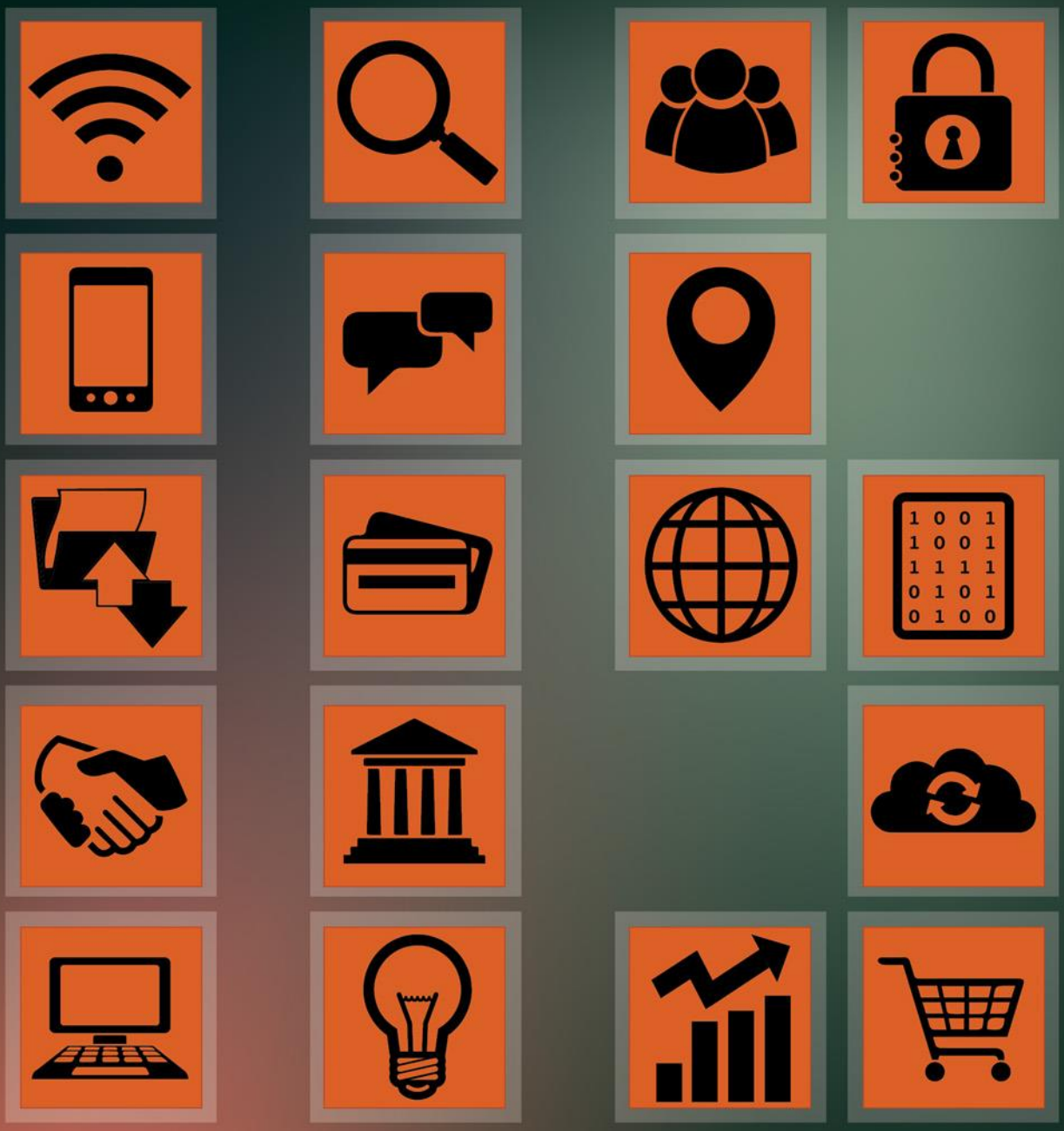

Privacy Impact Assessment – Data Availability and Transparency Bill 2020

For: Office of the National Data Commissioner, Department of the Prime Minister and Cabinet

Date: 26 February 2021

Table of Contents

Document Information

Client	Office of the National Data Commissioner, Department of the Prime Minister and Cabinet
Document purpose	To report on the privacy impact assessment of the Data Availability and Transparency Bill
Client Details	Website: https://www.datacommissioner.gov.au
Consultant details	Information Integrity Solutions Pty Ltd Website: https://www.iispartners.com Email: inquiries@iispartners.com Contact: Mike Trovato, Managing Director Mobile: +61 404 880 793

Document Version

Version	Date	Author	Notes
1	20/02/2020	IIS	Draft PIA #2 based on draft Bill, incorporating ONDC feedback and stakeholder consultations to ONDC for comment
2	06/09/2020	IIS	PIA #2 based on updated draft Bill and Explanatory Memorandum, incorporating ONDC feedback
2.1	08/02/2021	IIS	Draft PIA #3, including further revision based on the Bill and Explanatory Memorandum as introduced to Parliament
3	08/03/2021	IIS	PIA #3, incorporating ONDC feedback

1. Executive summary

The Office of the National Data Commissioner, Department of the Prime Minister and Cabinet (ONDC) engaged Information Integrity Solutions Pty Ltd (IIS) to conduct a privacy impact assessment (PIA) on the Data Availability and Transparency Bill (DATB), formerly known as the 'Data Sharing and Release Bill'.

This version of the PIA assesses the Bill as introduced to the Parliament on 9 December 2020. An earlier version of the PIA assessed a draft of the Bill as it stood on 4 September 2020. For the purposes of clarity and continuity, this report retains the relevant analysis and recommendations that were made on the earlier draft Bill and notes where recommendations have already been addressed.

Governments already use and share public sector data for many different purposes. The problem the DATB addresses is that, for many reasons including impediments in law and culture, the amount of data being shared is relatively small, meaning that opportunities are being missed.[1]

The new legislation, to be overseen by the National Data Commissioner (NDC), will provide an alternative pathway for government departments and agencies to share data in a consistent, safe and secure way. Data sharing under the DATB is expected to deliver tangible public benefits, innovation and efficiencies in the areas of: delivery of government services; informing government policy and programs; and research and development.

The range of data that could be shared is very wide. Not all the datasets would include personal information or de-identified information about individuals. Where they do, privacy risks could arise and must be considered.

The processes so far to develop the legislation recognise that 'maintaining trust with the Australian community is fundamental to realising the full potential of this national asset'.[2]

IIS acknowledges and welcomes the considerable work that has gone into designing privacy within the DATB. The extensive consultation, and the obvious responsiveness of the ONDC to listening and finding ways to enable both privacy protection and data sharing, are reassuring.

1.1 IIS overall view

This PIA considered if the elements of the Data Sharing Scheme set out in the Bill would provide for a reasonable, necessary and proportionate approach to privacy.

IIS assesses the overall privacy risks in the Data Sharing Scheme as potentially high.

---

[1] Productivity Commission, *Data Availability and Use Inquiry Final Report* (8 May 2017), available at <https://www.pc.gov.au/inquiries/completed/data-access#report>.

[2] Australian Government Data Sharing and Release Legislative Reforms Discussion Paper, September 2019, p 11.

Data sharing of the sort that the DATB would authorise, where it involves personal information, carries high inherent privacy risks. It could involve large volumes of data used in a new context, removed from the settings in which the information was originally collected. It will be taking place in a rapidly changing technological and social environment and in an expansive and distributed system with many players.

Privacy risks for individuals could include:

- Mishandling of personal information, including risk of re-identification or data breaches
- Loss of control – individuals don't know what is happening with information about them, might not have a choice and might not in any event support the use
- Personal information is used in new ways that are unexpected, unwelcome, disadvantageous, or harmful.

These are serious issues and go to the heart of the community's willingness to support data sharing.

IIS considers that the DATB framework is strong. Its layers of defence have the potential to work together to identify and carefully manage privacy risks associated with any data sharing project.

The change in the name of the Bill, which no longer includes 'release' and emphasises 'transparency' is significant. The DATB is about sharing public sector data within a rigorously controlled environment. The open release of data remains a separate activity and subject to existing frameworks and control.

The 'layers of defence' in the DATB framework include that:

- All participants in the Data Sharing Scheme must be accredited and data can only be shared with Accredited Users
- Entities in the Data Sharing Scheme must maintain privacy law coverage
- Data may only be shared for delivery of government services, informing government policy and programs, and research and development. Enforcement related purposes, including compliance, law enforcement and national security, are excluded
- Data sharing proposals must address the public interest in the sharing and must consider applicable ethics processes
- Data sharing is not mandatory – the DATB would give Data Custodians the authority to share and the obligation to first make sure data sharing is safe
- Data sharing must be governed by detailed, publicly available Data Sharing Agreements specifying the data to be shared for what purposes and must address the five Data Sharing Principles
- There is regulatory oversight by the National Data Commissioner (NDC), who will have a range of powers and the ability to seek civil and criminal penalties where data sharing fails to comply with the DATB.

While the framework is strong, its elements alone will not be sufficient to protect privacy; whether it stands up to the task will critically depend on its implementation and assurance.

Some of the DATB's strengths come with corresponding weaknesses. The DATB takes a high-level principles-based approach. It provides clear signposts but not, by any means, roadmaps. The fact that many of its key terms and concepts are not defined or detailed in the Bill was worrying to the stakeholders IIS consulted for the PIA. The limited purposes and inclusion of public interest and ethics concepts were welcomed but at the same time raised questions about what could be encompassed under the terms and who gets to decide. Stakeholders worried that shared data could be used with potentially privacy invasive technologies – including artificial intelligence or automated decision-making systems – or in unacceptable commercial activities or with unacceptable entities.

IIS shares many of these concerns. However, it is also satisfied that provided the high-level directions in the DATB are supported by clear, detailed and consistent rules, standards and guidance, the privacy impact of the DATB should be reasonable and proportionate. The Data Sharing Scheme and the principles on which it is built must also be supported by an independent and well-resourced regulator, strong assurance mechanisms, clear lines of accountability, effective compliance and where needed, strong enforcement and remediation if individuals are harmed. Again, the indications on these matters are positive but will be subject to effective implementation.

1.2 Recommendations

IIS has made one recommendation based on its analysis of the 9 December 2020 Bill.

Summary	Rationale	Recommendation
A. NDC to be given more scope for action in the accreditation process for non-corporate Commonwealth bodies	While it may be reasonable to streamline the accreditation process for non-corporate Commonwealth bodies, there must still be a process for assessing those bodies' data handling practices and arrangements against the accreditation criteria. If the NDC cannot seek evidence to support an accreditation application or refuse an accreditation application, the whole framework is weakened.	Amend the Bill to: • Enable the NDC to seek evidence from a non-corporate Commonwealth body to support their application for accreditation • Enable the NDC to refuse to accredit a non-corporate Commonwealth body when there are sufficient grounds for doing so

IIS made 13 recommendations in its PIA of the 4 September 2020 draft Bill, identifying the steps we consider are needed to ensure the DATB can deliver an approach that will enhance data sharing while strengthening data privacy and security protections.

For this report, IIS has updated Recommendation 8 in response to public submissions made on the exposure draft of the Bill. We have also highlighted in green the recommendations that have already been addressed in the latest Bill.

The ONDC's response to the recommendations is at Appendix A.

Summary	Rationale	Recommendation
1. Align accreditation requirements with APP 1 and give regard to OAIC advice on privacy governance and management	It will be important that the standards for privacy and security in the accreditation framework are consistent with the Privacy Act and APP framework, as the sharing scheme is open to a wide range of possible entities with different privacy governance approaches, experiences and capabilities.	Align accreditation framework requirements with 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.
2. Ensure that accreditation involves regular assurance that standards are being met	The effectiveness of accreditation in protecting privacy depends not only on its associated rules, standards and guidance, but also on a strong assurance process that confirms Data Scheme Entities are doing the right thing. An assurance process with oversight of compliance is necessary to ensure the integrity of the Data Sharing Scheme.	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.
3. Draft DATB to effectively exclude sharing for compliance and assurance purposes	The current draft of the DATB precludes 'enforcement related purposes', which are intended to include compliance and assurance. These terms do not appear in the definition as such. This could lead to confusion; for example, about whether compliance is seen as an intrinsic part of the delivery of government services rather than an enforcement related activity. While the Explanatory Memorandum provides this intent, it would be preferable for this to be indicated in the DATB.	Ensure that the DATB is drafted in such a way that there is no doubt that 'precluded purposes' include compliance and assurance. The Explanatory Memorandum and supporting guidance material should also make clear that compliance and assurance activities are precluded.
4. Articulate meaning of permitted purposes in Explanatory Memorandum	In addition to the proposed principles and controls in the Data Sharing Scheme, there is value in restricting the definition and interpretation of permitted purpose under the draft DATB, so as to arrest function creep and expansive uses that go beyond community expectations.	Address the expected data sharing purposes in the Explanatory Memorandum, 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.
5. Provide guidance on the ethics process in appropriate circumstances	The draft DATB anticipates the possible need for ethics consideration to support appropriate data sharing. Existing ethics frameworks and guidelines would not necessarily apply to all data sharing processes under the Scheme. There is	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: • Involving sensitive information

Summary	Rationale	Recommendation
	value in the NDC providing guidance on this matter.	• 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.
6. Provide guidance on how consent operates in the Data Sharing Scheme	The concept of consent has been well-defined by privacy law and guidance, albeit poorly implemented in practice. Data sharing raises new challenges and considerations for consent. There is value in the NDC providing guidance on this matter.	Specify, in the EM, guidelines and other guidance material, matters such as: • 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.
7. Specify 'privacy' in the NDAC's advisory functions	The NDAC will play a critical role in guiding the NDC on strategic matters. Those matters should include ensuring a balanced approach to privacy that foregrounds respect for individuals and rigor in personal information protection. The NDAC is in a position to monitor and advise on the privacy impacts of the Scheme as a whole and the accumulating privacy impact of data sharing under the Scheme. Without an explicit requirement for the NDAC to advise on privacy, there is a risk that privacy considerations are sidelined in strategic discussions about advancing data availability.	Specify the matters that NDAC is to advise on in the Bill, including: ethics; balancing data availability with privacy protection; and trust and transparency.
8. Review effectiveness of the NDC support, staffing and operating model	The NDC's ability to carry out its role in the Data Sharing Scheme will depend in part on the level and nature of resources available to them. In particular, the NDC plays an important role in monitoring compliance with the Scheme and	Review effectiveness of the NDC support and staffing model and the performance of its functions 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

Summary	Rationale	Recommendation
in first statutory review of the Act	complaint handling – privacy protections embedded in the DATB will only be as strong as the enforcement, oversight and assurance measures in place. There is also an open question as to how the NDC will perform the dual role of being an advocate for data sharing and a regulator enforcing compliance. The effectiveness of the NDC's independence, level of resourcing and performance of its dual advocate/regulator role should be subject to early review.	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.
9. Develop and publish a regulatory action plan	The NDC's oversight and monitoring role will be crucial to the effective implementation of the Data Sharing Scheme as it relates to privacy. It will be operating in a fast-moving regulatory and technological environment. Having a well thought-out and publicly-available regulatory action plan helps to facilitate, and signal the importance of, the NDC's oversight and monitoring role.	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: • 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.

Summary	Rationale	Recommendation
10. Individuals to have access to simple arrangements for addressing privacy complaints and issues	Data sharing will be taking place in a complex system, involving parties that may not be previously known to individuals. As the entity responsible for ecosystem governance, the NDC should work with the OAIC to ensure that individuals have easy access to a mechanism for dealing with privacy complaints, queries and issues without being passed around or getting lost in the system.	Work with the OAIC and other privacy regulators to ensure: • 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).
11. Measure and report on individuals' interaction with the Scheme	As the Data Sharing Scheme exists to benefit the community, the NDC, in consultation with the OAIC, should monitor how individuals are being affected from a privacy standpoint. Measuring individuals' interactions with the Scheme – for example, number and nature of privacy complaints – will allow the NDC to address the Scheme's shortcomings and make continuous improvements.	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: • 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).
12. Allow for shortening the period for review of the Act and make reviews public	The draft DATB proposes that the Act is to be reviewed no later than every ten years after commencement, with an initial review three years after commencement. The regular ten-year review interval is very long considering the dynamic technological and social environment in which data sharing will occur.	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. Subsequent reviews should formally consider whether the next review should

Summary	Rationale	Recommendation
		occur sooner than 10 years, taking into account: • 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. The reviews of the Act and the government responses should be made public.
13. Conduct public awareness campaign about the Data Sharing Scheme	The Data Sharing Scheme is a very significant change to the way data sharing will occur in Australia. With any initiative that touches on the (potential) sharing of personal information, it is important to build social licence and trust among the community. Public awareness to promote the Scheme and allay concerns should occur well before it enters into operation.	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: • 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.

The recommendations follow the relevant discussion in the body of the report and can be summarised under four broad themes:

1. Issues not addressed elsewhere in the Bill
    - **Recommendation 2** – Ensure that accreditation involves regular assurance that standards are being met

2. Building on existing expectations of the Bill
    - **Recommendation A** – NDC to be given more scope for action in the accreditation process for non-corporate Commonwealth bodies
    - **Recommendation 3** – Draft DATB to effectively exclude sharing for compliance and assurance purposes
    - **Recommendation 4** – Articulate meaning of permitted purposes in Explanatory Memorandum
    - **Recommendation 7** – Specify 'privacy' in the NDAC's advisory functions
3. Giving clarity in translating the various aspects of the Scheme into practice
    - **Recommendation 1** – Align accreditation requirements with APP 1 and give regard to OAIC advice on privacy governance and management
    - **Recommendation 5** – Provide guidance on the ethics process in appropriate circumstances
    - **Recommendation 6** – Provide guidance on how consent operates in the Data Sharing Scheme
    - **Recommendation 8** – Review effectiveness of the NDC support and staffing model in first statutory review of the Act
    - **Recommendation 9** – Develop and publish a regulatory action plan
4. Future-proofing the privacy impact of the Bill
    - **Recommendation 10** – Provide individuals with access to simple arrangements for addressing privacy complaints and issues
    - **Recommendation 11** – Measure and report on individuals' interaction with the Scheme
    - **Recommendation 12** – Allow for shortening the period for review of the Act and make reviews public
    - **Recommendation 13** – Conduct public awareness campaign about the Data Sharing Scheme.

2. Introduction

2.1 PIA objectives and audience

IIS was engaged to provide a systematic assessment of the DATB to identify the impact that the Bill might have on the privacy of individuals, and to make recommendations for managing, minimising or eliminating that impact.

The focus of the PIA was to provide a well-informed, independent, and holistic review of the DATB's privacy approach, including whether the elements of the proposed Data Sharing Scheme provide for a reasonable, necessary and proportionate approach in the current policy context.

IIS considered the text of initial and then revised versions of, the DATB along with its Explanatory Memorandum (EM) – essentially the Bill is intended to encourage more, and safe, data sharing to achieve potential benefits to the public. Safe data sharing includes proactive consideration of privacy and privacy protection that is built into the sharing processes.

More information about the PIA scope and IIS's methodology is at Appendix B.

2.2 Privacy risks arising in the data sharing context

IIS accepts the public interest in sharing data to deliver benefits to the community and economy. Needless to say, that public interest must be balanced against a range of other interests including privacy. By privacy, we mean: a person's right to live without intrusions into their personal life by government or business, along with their right to be free from arbitrary or unreasonable surveillance or monitoring. PIAs are a baseline tool for addressing incremental encroachments on civil liberties but must be matched with leadership and strategic management of risks.

Privacy impacts often grow from incremental expansions in data collection and use that each, alone, appear reasonable or harmless – rather than from concerted efforts to trample privacy. It is therefore encouraging that the ONDC has, so far, taken a considered approach to privacy. The DATB and Data Sharing Scheme create certain specific privacy risks that IIS took into account during its analysis and which the ONDC should continue to monitor during project development and implementation.

Key overarching privacy risks are set out in the table below along with existing measures in the DATB.

Broad privacy risk	Description	Existing risk mitigation
Function creep	Information collected for one purpose slowly being used for other additional unintended purposes over time, outside the expectations of individuals.	Purpose requirement, prescribing and excluding allowable purposes for data sharing. Sharing exclusions specified in regulations including exclusion of My Health Record and COVIDSafe App data from the Scheme.

Broad privacy risk	Description	Existing risk mitigation
		Exclusion from the Scheme of intelligence agencies and data originating from them. Data Sharing Agreements limiting use to agreed purpose. Oversight and global view of arrangements by NDC.
Lack of transparency	In the digital age, data handling and data flows are increasingly invisible to individuals.	Consent requirement under Data Sharing Principles. Data Sharing Agreements to be published. Breach notification provisions. ONDC working with OAIC on notice.
Individual loss of control / lack of choice	As entities more seamlessly and effortlessly move data around, there is a greater risk that individuals lose control over how their information is handled and shared.	Consent requirement under Data Sharing Principles. Robust monitoring, oversight and avenues for complaint handling. Public interest test under the Data Sharing Principles. Ongoing consultation with community stakeholders on Scheme design.
Development of detailed profiles of individuals	As data is drawn together, linked and integrated, the risk increases that an entity can build up detailed and rich profiles of individuals.	Purpose requirement, prescribing and excluding allowable purposes for data sharing. Data Sharing Agreements limiting use to agreed purpose. Data minimisation via the 'reasonably necessary' limitation.
Risk of harm for vulnerable people	Vulnerable people, such as victims of domestic abuse or people with a public profile who require more stringent privacy protection, may find that increased data sharing exposes them to a greater risk of harm due to possible information misuse or unauthorised disclosure.	Consent requirement under Data Sharing Principles. Accreditation requiring security standards be met. Data Sharing Principle requiring appropriate protection of data. Data minimisation via the 'reasonably necessary' limitation (potentially resulting in de-identification of datasets). Data Sharing Agreements limiting use to agreed purpose. APP 11 (and other privacy law equivalents) requiring reasonable steps to protect personal information.

Broad privacy risk	Description	Existing risk mitigation
Data breach, misuse and loss, or subject to unauthorised access	Sharing data multiplies copies of data and necessarily increases the risk profile of the entities holding it. (The inverse of this is 'if you don't hold it, you can't be breached') Data sharing may also enable the creation of 'data honeypots' that are attractive to hackers for the richness of the data they contain.	Accreditation requiring security standards be met. Data Sharing Principle requiring appropriate protection of data. Data minimisation via the 'reasonably necessary' limitation. APP 11 (and other privacy law equivalents) requiring reasonable steps to protect personal information. Breach notification provisions.

2.3 How to read this report

Section 1, the Executive Summary, sets out IIS' overall conclusions about the privacy impacts of the DATB and the Data Sharing Scheme it establishes and flags the nature of recommendations IIS makes to mitigate risks identified.

Section 2 (this section) and Appendix B, sets out information about the PIA.

Section 3, and Appendix C, provide information about the background to the DATB and its provisions.

Section 4 gives an overview of issues stakeholders raised in consultations for this PIA.

IIS's detailed analysis, findings and recommendations are in sections 5-9. These sections consider whether the provisions do have an impact on privacy and whether changes are needed to the DATB itself, whether an issue should be addressed in the EM, or in other mechanisms available under the DATB, such as regulations, rules, standards, or guidelines or in the implementation of the DATB.

2.4 Glossary

Term	Expansion or definition
Accredited Entity	Accredited user or ADSP
Accredited User	An entity accredited under the accreditation framework as an Accredited User
ADSP	Accredited data service provider
AIA	Accredited Integrating Authorities
APP Guidelines	Office of the Australian Information Commissioner *Australian Privacy Principle Guidelines* Combined 2019
AFP	Australian Federal Police
APPs	Australian Privacy Principles in the Privacy Act

Term	Expansion or definition
Data Custodian	A Commonwealth body that holds public sector data and – apart from the DATB (when enacted) – has the right to deal with it.
Data Scheme Entity	A collective term for all participants in the Data Sharing Scheme, that is Data Custodians, Accredited Users and Accredited Data Service Provider
Data Sharing Principles Guide	The Department of the Prime Minister and Cabinet Best Practice Guide to Applying Data Sharing Principles
Data Sharing Scheme	The Data Sharing Scheme means the Bill, and the regulations, rules, data codes and guidelines made under it
DATB	The Data Availability and Transparency Bill, formerly known as the Data Sharing and Release Bill
Discussion Paper	Data Sharing and Release Legislative Reforms Discussion Paper, September 2019
EM	DATB Explanatory Memorandum
FOI Act	*Freedom of Information Act 1982*
IIS	Information Integrity Solutions Pty Ltd
June 2019 PIA	Galexia Privacy Impact Assessment on the Proposed Data Sharing and Release (DS&R) Bill and Related Regulatory Data Sharing Scheme, 28 June 2019
NDAC	National Data Advisory Council
NDC	The National Data Commissioner under the DATB
NHMRC	National Health and Medical Research Council
OAIC	Office of the Australian Information Commissioner
ONDC	Office of the National Data Commissioner, Department of the Prime Minister and Cabinet
PIA	Privacy Impact Assessment
PM&C	The Department of the Prime Minister and Cabinet
Privacy Act	*Privacy Act 1988* (Cth)

3. About the DATB

Following recommendations from the Productivity Commission in 2017, the Federal Government took steps to strengthen arrangements for public sector data sharing. This culminated in the establishment of the ONDC within the Department of the Prime Minister and Cabinet (PM&C) and drafting legislation, the DATB. The Bill was introduced into the Parliament on 9 December 2020. This PIA assesses the DATB as introduced and associated arrangements. Appendix C offers contextual information about the process so far. This section gives a brief outline of the DATB. It also outlines the privacy strengths of the Data Sharing Scheme in its current form.

3.1 Overview of the DATB

The DATB essentially translates the policy positions outlined in the *Australian Government Data Sharing and Release Legislative Reforms Discussion Paper*, September 2019 (the Discussion Paper) into a legislative framework. There are some key changes, which arose from the ONDC's review of submissions and further consultations with stakeholders, since the Discussion Paper was released. These are outlined in Section 3.2.

The DATB, if enacted, would establish a consistent, safe pathway for agencies and trusted users to share public sector data for specified purposes. In doing so, it aims to promote better availability of public sector data and streamline data sharing, overcoming complex legislative barriers and outdated secrecy provisions.[3] Importantly, the DATB will work alongside other existing information handling obligations under the *Privacy Act 1988* (the Privacy Act), the *Archives Act 1983* and so on.

The DATB aims to formalise a framework for sharing public sector data. The framework largely rests on four broad requirements to data sharing:

- **Accreditation** – Data sharing is conditional on entities being accredited under the DATB's accreditation framework.
- **Data Sharing Purposes** – The data sharing is reasonably necessary for one of three specified purposes and is not for a precluded purpose.

  Data Sharing Principles – The data sharing meets the requirements of the five Data Sharing Principles.
- **Data Sharing Agreement** – The data sharing occurs under a Data Sharing Agreement between the Data Scheme Entities.

If those four requirements are met, and the proposed data sharing is not excluded by any other clauses in the DATB, then the data sharing is 'authorised' and may proceed. That said, the DATB does not compel data sharing and data custodians may decline a request to share data under the '*No duty to share*' clause despite DATB requirements being met.

[3] The Discussion Paper, p 1.

More information about the DATB, including background, the significance of changes the DATB could facilitate, and the key participants is at Appendix C.

3.2 Changes to policy positions since the Discussion Paper

Following consultation associated with the September Discussion Paper, the ONDC has changed its policy position in a few areas. Those changes have been incorporated into the first Data Sharing Principle in the DATB and, for data sharing projects, require that:

- Any applicable processes relating to **ethics** are observed (see Section 6.4)
- Any sharing of the personal information of individuals is done with the **consent** of the individuals, unless it is unreasonable or impracticable to seek their consent (see Section 6.5)
- Data Sharing Agreements must detail the **public interest**, including for any commercial applications arising as a result of data sharing (see Section 6.10 on Data Sharing Agreements and Section 6.1.5 on commercial activities).

In addition, IIS understands that the NDC will not be supported by a separate office. Instead, the NDC will be located within PM&C and staffed by PM&C staff. The Bill contains measures to preserve the independence of the NDC, to ensure the Commissioner is adequately supported and to avoid actual and perceived conflicts of interest. The PIA considers the possible impact on privacy outcomes of this arrangement at Section 7.4.2.

3.3 Privacy strengths of the Data Sharing Scheme

The ONDC has considered privacy throughout the legislation drafting process and the DATB contains a range of features aimed at enhancing the privacy settings of the Scheme. These include:

- **Coverage of the Privacy Act or equivalent**
  Data Scheme Entities must 'maintain coverage' and comply with the Privacy Act or an equivalent privacy regime in relation to their handling of personal information under the Data Sharing Scheme.
- **Purpose limitation**
  The DATB prescribes permitted and precluded purposes for sharing. Sharing for enforcement related purposes or national security purposes is excluded from the Scheme. Sharing may only proceed if the purpose of the sharing is specifically permitted. This sets appropriate limits on disclosure and reduces risks of function creep.
- **Data minimisation**
  The DATB requires that only data reasonably necessary to contribute to the purpose be shared. This lines up with collection limitation provisions in the Privacy Act and reduces privacy impacts where personal information is involved.
- **Privacy safeguards**
  The Data Sharing Principles contain a number of requirements that strengthen the privacy settings for the Scheme. These include requirements relating to ethics, consent and

identifying the public interest in sharing. They also oblige Data Scheme Entities to ensure sharing occurs in a controlled environment and that data is protected.

- **Sharing with Accredited Users rather than release to the world at large**
  Privacy risks are lessened by sharing occurring between known and trusted parties. While there is value in open release of data, the stakes can be much higher and privacy risks more difficult to mitigate, notwithstanding de-identification efforts. Under the DATB, data users and service providers must be accredited. IIS understands that accreditation will require entities to meet standards for security and privacy of data, though the level of such standards is still under development.
- **Data Sharing Agreements**
  Data sharing is governed by agreements between the Data Custodians and the Accredited Users. Agreements formalise the data sharing purpose and Data Sharing Principle requirements.
- **Restrictions to 'on-sharing'**
  The DATB prohibits Accredited Users from further sharing or release of data they receive under the Data Sharing Scheme except in specified circumstances and subject to strict requirements.
- **Data breach notification**
  The DATB sets out the intended interaction with breach notification obligations under the Privacy Act – essentially it aims to ensure data breach obligations are maintained and that it is clear which Data Scheme Entities' are responsible for which aspects of data breach handling and notification. Data Scheme Entities must also keep the NDC informed about data breaches involving personal information. The NDC would also receive notifications and respond to data breaches involving non-personal information.
- **Enforcement and complaint handling**
  The DATB gives the NDC monitoring and investigative powers, along with a range of enforcement powers including the ability to seek injunctions and civil penalties from a court, issue infringement notices and enter into enforceable undertakings. The Bill also provides for complaint handling; the focus here is on the Data Scheme Entities. Individuals would still pursue privacy complaints via the Privacy Act or other equivalent privacy legislation.

In addition, IIS finds that the ONDC has taken a responsive consultative approach to the development of the Data Sharing Scheme. It has adjusted its approach in accordance with recommendations made in last year's *Privacy Impact Assessment on the Proposed Data Sharing and Release (DS&R) Bill and Related Regulatory Framework* (June 2019 PIA), and in accordance with stakeholder feedback.

3.4 Community support for data sharing

ONDC asked IIS to consider if the DATB is likely to have community support.

3.4.1 Gauging community support and fostering trust

The Productivity Commission explored the question of community support for data sharing and reuse in some detail in Chapter 3 of its inquiry report.

IIS will not repeat the detail of those findings here but observes the following key points:

- The community generally does not view information sharing between departments as a major threat to privacy.[4] The OAIC's 2017 Australian Community Attitudes to Privacy Survey also indicated that government departments were the third-most trusted type of entity (when it came to their handling of personal information).[5]
- Anecdotal evidence suggests that most people expect that different parts of government share data; overseas studies show that people overestimate the extent of information sharing that is already occurring within government.[6]
- Individuals would, however, like to maintain a level of control over their information; they expect governments to share their data with their consent, only when strictly necessary, and to be transparent about their data handling processes.[7]
- Individuals tend to support data sharing between government entities provided they have a degree of control over their data and the benefits of sharing are evident; the onus is on government to communicate these benefits effectively.[8]

These points indicate a certain level of trust in government and comfort in relation to data sharing between public sector agencies, provided certain conditions are met. However, there may be less comfort in relation to:

- Data sharing with private sector entities
- Release of data more widely (rather than between Accredited Users)
- Commercialisation of data, particularly where the public benefit of the data use appears to be eclipsed by notions of 'profiteering' (discussed further below at Section 6.1.5).

It is also worth noting that attitudes to privacy are in flux, correlating with rapid technological change (including data analytics, artificial intelligence, online technologies). For example, the community response to the My Health Record indicates that sentiment can rapidly change for the worse. In its inquiry, the Productivity Commission pointed out (and IIS concurs) that '[a]ll development of data practice – whether in the private sector or public sector – must take the creation and preservation of understanding and trust as its first consideration.'[9]

---

[4] See Productivity Commission, *Data availability and use: Inquiry report*, no. 82, 31 March 2017, p 123.

[5] 58% of respondents said they trusted state and federal government departments, see OAIC, *Australian Community Attitudes to Privacy Survey 2017 Report*, section 1.0.

[6] Id at 4, p 123.

[7] Ibid.

[8] Ibid.

[9] Id, p 122.

3.4.2 Safeguarding social licence

Questions of social licence can be difficult to gauge for projects like the Data Sharing Scheme which involve detailed arrangements. Initial community concerns may be alleviated through further explanation of requirements for data sharing, good governance and security settings including credible assurance processes. IIS finds that there are three possible flashpoints for building or damaging social licence:

- **During policy and legislative development**
  Parts of the community may feel that they have lost control of the debate, that change is occurring against their will and that they have no voice in the proceedings. IIS finds that the ONDC has taken (and continues to take) steps to address this risk through taking an open and responsive approach to policy development, involving successive consultations with stakeholders, and successive PIAs.
- **At the point that legislation is passed or implemented**
  When legislation is passed and the Data Sharing Scheme becomes operational, there may be a second wave of concern. Media coverage may raise awareness (or concern) amongst a wider segment of the community not previously involved or aware of the Scheme. The ONDC must be prepared to engage in a public awareness raising campaign prior to implementation to address and allay community concern. This would include making information available in plain English that explains the Scheme and what it involves.
- **The first time something goes wrong (in the form of a breach or sharing outside community expectations)**
  This is a point where a project can suffer significant loss of social licence. The Scheme will significantly reduce this risk through applying the data minimisation principle and using de-identified data as much as possible. Otherwise, resiliency is the best approach, which involves having robust breach response and recovery arrangements – including engaging the Australian Cyber Security Centre (ACSC) – in place. IIS notes that a combination of provisions in the DATB allow both for mitigating security risks and dealing with (and reporting) a breach should it occur. Strong enforcement also has a role to play in demonstrating to the community that the NDC and all other scheme participants take privacy seriously and that there are consequences for poor practices.

It is IIS's view that the various risks identified here could well be addressed by various elements of the DATB. IIS makes some specific comments on the DATB's impact on the 'safety net' for individuals in Section 8 and its transparency measures and approach in Section 9. We also consider, and this is a strong thread through this PIA, that whether or not the community will support data sharing authorised by the DATB will depend on how it is implemented by all of the players.

4. Consultation with stakeholders

This PIA forms one part of the privacy by design and privacy impact assessment process.

The ONDC has already conducted an extensive consultation process to test and develop the policy settings for the Bill. This culminated in the Discussion Paper, which set out issues identified in the consultations to that point and proposed the parameters for the proposed Data Sharing Scheme. IIS drew on the detailed information in the Discussion Paper and reviewed key submissions responding to the Discussion Paper to inform its findings in this PIA.

IIS also consulted with selected privacy regulators and privacy/community advocates who had previously participated in consultations on the draft DATB. The aim was to test IIS's preliminary findings and recommendations and to identify additional issues, if any. In the limited time available, not all invited parties were able to participate. A list of participants can be found at Appendix B.

The consultations were based on a consultation document, and information IIS provided about the issues we had identified and our indicative recommendations. The groups consulted noted the difficulty in commenting without having seen the draft DATB and expressed a common wish to have the opportunity to provide further comments once the final version of the draft DATB is released for public consultation.

IIS notes issues raised in submissions that were clearly of significant concern to the submitters. These points included deficiencies in the Privacy Act and whether the Data Sharing Scheme should be included under the Privacy Act, rather than establishing a separate regulator (the NDC). While acknowledging the possible impact on privacy, IIS did not address these issues, as they were out of scope for this PIA.

Although IIS took into account comments made during consultations in making its findings, the views expressed in the PIA are IIS's and are not intended to represent the views of stakeholders.

Positives and strengths identified by the stakeholders include:

- Commendation on the level of consultation that has been conducted
- Potential for strong privacy protections within the framework
- Endorsement of the way the Bill is intended to interact with existing legislation and the offence provisions provided in the enforcement powers
- Supportive of the way consent has been framed.

4.1 Issues raised in consultation

Participants raised concerns related to the following areas.

Issues stakeholder were keen to see addressed in the DATB:

As noted, stakeholders IIS consulted had not had the opportunity to see the DATB. Some of the issues raised have been addressed in the DATB. In other cases, the DATB takes a different

approach. IIS considered the issues in the body of the PIA (references to the relevant provisions of the PIA are noted):

- Agreement that public interest should be considered, however there was concern regarding who gets to decide the public interest and what it will mean, and whether these points should be in the primary legislation or the EM (see Section 6.6)
- The meaning of other terms, including 'ethics' (see Section 6.4)
- A preference for regulations rather than principles to ensure responsibility for actions (see Section 6.2)
- The specific details of the accreditation criteria that will be used (see Section 5.5)
- Specification for who will decide what is reasonably necessary (see Section 6.1.2)
- Greater clarity and particularity around permitted purposes, especially commercial purposes to be applied consistently and promote community confidence (see Section 6.1)
- More clarity around commercial uses, and a suggestion to conduct a PIA specifically on this issue (see Section 6.1.5)
- The community may still be uncomfortable with certain types of commercial entities that have vast or powerful data holdings using public sector data, even if they can meet the criteria (see also Section 6.1.5)
- A preference for commercial entities to be legislatively bound to the NDC's regulatory and enforcement powers rather than under rules and regulations, strengthening the NDC's powers (see Section 7)
- The role of de-identified data and limits of its ability to make data anonymous (see Section 6.8)
- Strong support to include privacy in the objects of the Bill or alternatively in the EM, to enable sustainable innovation (see Section 5.4)
- There should be more frequent review of the legislation (see Section 9.1).

IIS understands that there will be public consultation on the DATB before it is introduced to Parliament and stakeholders will then have the opportunity to consider these issues again.

Issues and risks stakeholders identified for the implementation of the DATB:

A number of the issues stakeholders raised in this area are canvassed in this PIA, in particular in relation to the NDC's role, the level of resourcing made available to the NDC, and the implementation approach. In many cases whether or not the issue or risk eventuates would only be apparent as the Data Sharing Scheme is implemented. IIS assumes that such issues would be the subject of NDC monitoring and the proposed statutory reviews of the legislation. Issues identified included:

- Having a robust ethics framework that is beyond reproach, in particular regarding how automated decision making is treated as a downstream use case of the data and how data can be used as a tool for discrimination and a way to have assurance over such uses

- Level of and ability for the ONDC to monitor, audit and provide assurance of Accredited Entities, including their technologies, as well as accountability in case of misconduct or non-compliance
- Potential for the rapid advances and the rise in use of artificial intelligence or automated decision making, and risks of downstream use, falling outside the scope of permitted purposes or the potential the use of these technologies may provide for unintended insights or uses of data, suggesting the need to preclude their use
- Having sufficient security testing of the risks in data sharing before sharing commences
- Managing the inherent conflict of interests in the NDC's role to encourage data sharing and to oversee and regulate data sharing – preferably the OAIC would oversee the data sharing arrangements to ensure privacy is taken into consideration and protected
- Awareness of the importance of data sharing for the purposes of research, however these data may be published (i.e. in a research paper or journal) and eventually used for commercialisation
- Concerns over whether there will be controls around collateral use of the data once it has been shared, to minimise scope creep
- Concern as to the efficacy of the data minimisation requirement, notwithstanding overarching support for it
- Ensuring that the framework is supported by a strong implementation plan
- Need for the NDC to work with OAIC in relation to accreditation framework and provide for NDC interrogation of applicants' self-assessed claims that they meet the criteria.

5. Findings and recommendations – Interaction with privacy law, objects clause and accreditation

This section and Section 6, discuss aspects of the DATB framework and its impact on privacy.

IIS considers that the DATB framework is strong. Its multi-layered and coherent set of requirements should facilitate data sharing while allowing for privacy to be considered and protected. The DATB is designed to operate alongside, and not replace or overlap with, the Privacy Act. However, IIS has identified areas which could be strengthened, or to which the NDC should pay particular attention.

5.1 Interaction with the Privacy Act

When reviewing the privacy impacts of the DATB, it is important to understand that the Data Sharing Scheme will not operate in a vacuum. Existing protections provided by the Privacy Act and its APPs continue to apply. The DATB makes clear that all entities participating in the Data Sharing Scheme must 'maintain privacy coverage' either under the Privacy Act or comparable state or territory law. Entities participating in the Data Sharing Scheme will still be required to follow APPs concerning privacy policies, privacy collection notices, data quality, security, data disposal, access and correction, as they do at present.

IIS finds that the approach of ensuring the APPs (or comparable principles) apply creates an important baseline for personal information protection. This PIA, therefore, avoids recommending changes to the DATB that would duplicate protections otherwise already available under the Privacy Act.

The DATB interacts with the Privacy Act when personal information is shared. When Accredited Users receive personal information from a Data Custodian this would be a collection for Privacy Act purposes and subject to APP 3. Accredited Users would need to consider, for example, whether the collection was reasonably necessary or directly related to their functions and activities. APP 3 allows indirect collection of personal information where this is authorised by law as it would be under the DATB. The DATB additionally requires that sharing of the personal information of individuals be done with the consent of the individuals, unless seeking consent is unreasonable or impracticable.

The DATB also interacts with the Privacy Act by virtue of the latter's 'required or authorised by law' exceptions in APP 6. This means, for example, that secondary uses and disclosures of personal information authorised by the DATB are permitted under the Privacy Act.[10] This exception is critical to enabling the Privacy Act to interact with a range of other legislation. That said, it is incumbent on legislative drafters to take a cautious approach; poorly drafted or needlessly broad 'authorisations' for additional data use can have significant ramifications for privacy. IIS finds that the ONDC has taken a cautious approach and this is evident in the DATB which contains a number of privacy safeguards (in particular, the Data Sharing Purpose and Principles which we discuss further in Section 6).

[10] Privacy Act, Schedule 1, APP 6.

5.2 Privacy coverage model

As part of the package of measures in the DATB which go to privacy protection, Data Sharing Entities are required to maintain privacy coverage. This provision applies regardless of the nature of the organisation or whether they are state or territory bodies. It is an important protection.

The privacy coverage provisions make clear that nothing in the Bill affects the operation of the Privacy Act in relation to a Data Scheme Entity that is an APP entity.[11] All other Data Scheme Entities must ensure that for activities under the DATB:

- The Privacy Act applies, for example, via the Privacy Act's opt-in provisions, or by possible regulations meaning that state authorities and instrumentalities can be treated as entities for the purposes of the Privacy Act),[12] or
- A law of a State or Territory applies that provides for all of the following:
    - Protection of personal information comparable to that provided by the APPs
    - Monitoring of compliance with the law
    - A means for individuals to seek recourse if their personal information is mishandled.

This follows the approach outlined in the Discussion Paper for 'equivalent privacy protections'.[13] The equivalency requirements do not include data breach notification requirements. This would have posed difficulties as State and Territory privacy laws do not currently include this protection. The DATB builds in separate privacy protection here.

During this PIA process, IIS suggested the ONDC make a finding on equivalence for each state and territory to remove doubt about which privacy laws maintain coverage. Subsequently, the EM has been drafted to include a clear statement about equivalency. It states that at the time of drafting, New South Wales, Victoria, Queensland, Tasmania, the Australian Capital Territory, and the Northern Territory have relevant privacy laws that meet DATB equivalency requirements.

5.3 DATB approach to data breaches

The Data Sharing Scheme includes provisions for managing data breaches. Under the DATB a data breach is defined as 'unauthorised access to, or unauthorised sharing or unauthorised release of, the data; [or] the data is lost in circumstances where there is likely to be unauthorised access to, or unauthorised sharing or unauthorised release of, the data.'[14] A DATB data breach could involve any type of shared data, including personal information.

---

[11] Section 6 of the Privacy Act defines 'APP entity' as an agency or organisation. Other provisions then rule out some organisations.

[12] Privacy Act, ss 6F and 6EA.

[13] Discussion Paper, p 31.

[14] DATB Bill, cl 35.

The data breach provisions in the DATB are part of the protective framework. They ensure that any mishandling of data by any Data Scheme Entity is dealt with appropriately and transparently, and that responsibilities for data breach handling are clear. The provisions are not intended to replace or diminish the data breach provisions in the Privacy Act. In particular, Data Custodians remain responsible for obligations under Part IIIC of the Privacy Act, although they can allocate some or all of these responsibilities to an Accredited User via the Data Sharing Agreements if the Accredited User is also an APP entity.

Should the Accredited User not be an APP entity, then the Data Custodian is the holder of the personal information for the purposes of notification to the OAIC. In such cases, the Accredited User must notify the Data Custodian of a breach involving personal information so that the Custodian may meet its breach notification obligations under the Privacy Act. This would mean that amongst other things, that breach notification provisions in the Privacy Act would continue to apply to data shared under the DATB even if the Accredited Users is a state or territory body.

IIS considers this provides for a strong protective framework.

We have one observation from a privacy impact perspective. The definition of data breach in the DATB is different to the definition in the Privacy Act, and the terms address different issues.[15] The ONDC advised that the DATB definition of data breach is modelled on the Privacy Act definition to ensure alignment between the schemes. Some adjustments have been necessary to reflect differences between the schemes ('disclosure' is a Privacy Act concept, whereas the DATB relies on concepts of 'sharing' and 'release').

5.4 Interaction with the *Freedom of Information Act 1982* (Cth)

The FOI Act will not apply to data shared under the Data Sharing Scheme. Specifically, agencies will be exempt from the FOI Act in relation to a document that comprises ADSP-enhanced data or that was shared under the authority of the Bill. The EM to the Data Availability and Transparency (Consequential Amendments) Bill 2020 (which will amend the FOI Act) states that this exemption from the FOI Act 'is intended to preserve protections for data under the principal Bill. The principal Bill creates a controlled environment for sharing, where data unsuitable for release […] may be safely accessed by appropriate persons for purposes in the public interest.'[16]

Without this exemption, there may be a risk that 'data shared under the scheme for a permitted purpose such as policy or research could be accessed by any person for any purpose (including precluded purposes under the principal Bill).[17]

While data shared under the authority of the Bill will be exempt from FOI, other copies of the data held by a data custodian will be subject to the FOI Act as they are currently because those copies are held

[15] Privacy Act, s 26WE: a notifiable data breach involves unauthorised access to, or unauthorised disclosure of, the information and it would be reasonable to conclude the breach could result in serious harm to individuals.

[16] Data Availability and Transparency (Consequential Amendments) Bill 2020, EM, [20].

[17] Ibid.

outside the scheme. In addition, outputs will also be subject to the FOI Act (where they are held by an agency covered by that Act). In this way, the data on either side of the sharing – pre-shared data and post-share output – is FOI-able. It is only the controlled data sharing environment that is removed from the remit of the FOI Act.

If an output is released under FOI, it exits the scheme. PM&C clarified that only the copy released to the FOI recipient exits the scheme and not the copy still held by the accredited user. This means that all the protections contained in the Bill continue to apply to the accredited user, regardless of whether or not the output was subject to FOI access.

IIS has not identified any privacy risks in the interaction of the FOI Act with the Bill, as proposed.

5.5 Principle-based law

Like the Privacy Act, the DATB takes a principles-based approach to regulation which allows it to be flexible, to apply in diverse circumstances, and to accommodate rapidly evolving technologies. However, experience with principle-based law tells us that entities will need guidance and assistance to give certainty as to how to apply the law in practice. The NDC has an important role to play in this respect. IIS outlines actions we believe NDC can take to help entities, including through supporting guidance (see Appendix D) and monitoring the Scheme as a whole (see Section 7.4.3).

In line with the principles-based approach, many key concepts in the DATB are not defined and carry their ordinary meaning. The ONDC pointed out that this is common legislative drafting that aims to facilitate smooth interaction of the DATB and other laws. The ONDC has also drawn on existing definitions in other laws to facilitate this smooth interaction.

IIS accepts this reasoning. Every effort should be made to reduce friction points with other legislation. That said, the NDC must take steps to ensure terms are applied as intended and are not read down over time. Indeed, lack of detail on the meaning of key terms was a theme in submissions to the Discussion Paper and was a concern raised by the organisations IIS consulted for the PIA. While this PIA focuses on the DATB, IIS identifies (in Appendix D) terms and other core concepts that need further explanation in the EM and/or supporting guidance material developed by the NDC.

5.6 DATB objects

The objects of the DATB are:

- 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 use of public sector data
- Establish institutional arrangements for sharing public sector data.

These objects do not specifically mention privacy protection or assurance, though enabling consistent safeguards and enhancing transparency of data sharing do advance privacy outcomes. During its analysis, IIS considered whether respect for privacy should be explicitly mentioned in the objects

clause. While the Data Sharing Scheme's scope is broader than personal information, personal information or de-identified information could be involved. Inclusion of privacy protection in the objects clause might allay community concern about the Scheme's posture towards privacy.

One submission to the Discussion Paper suggested that there should be some mention of privacy, and balancing this with other interests, as is currently the case in the objects clauses of a number of privacy laws. Introducing a specific focus on privacy could also off-set the concern in another submission that the NDC's role in advocating for data sharing could possibly conflict with protecting individuals' privacy interests.

During the PIA process, IIS suggested to the ONDC that privacy be brought into the objects clause or, at a minimum, be mentioned in associated supporting explanation in the EM. Through successive iterations of the Bill, the objects clause has remained the same, however the EM has been updated to explicitly refer to privacy. It states that the Bill's stated 'objectives encourage greater sharing of public sector data with robust safeguards to protect privacy and data security while enhancing integrity and transparency to build community confidence.' IIS has opted not to recommend amendment to the objects clause. However, in our view this makes it all the more important for other mechanisms that aim to ensure privacy is considered at a strategic level in management and oversight of the Scheme. In particular, the National Data Advisory Council (NDAC) has a role to play in encouraging ongoing consideration of privacy and the cumulative privacy impact of the Data Sharing Scheme as a whole. See Section 7.1.1.

5.7 Accreditation of Data Scheme Entities

Data sharing is also conditional on entities being accredited, which is intended to create another layer of assurance to support safe data sharing. The DATB itself does not limit the types of organisations that can apply for accreditation; they could be Commonwealth agencies, state or territory bodies, academic institutions, not-for-profit and for-profit private sector organisations, or overseas bodies.

5.7.1 Accreditation of Commonwealth bodies

Under the Bill's accreditation framework, the NDC accredits entities that wish to collect and use scheme data or who wish to become an ADSP. Entities must provide evidence that they meet accreditation criteria and then the NDC decides whether to accredit the entity.

This approach, however, will not apply to (non-corporate) Commonwealth bodies. Under the Bill, the NDC 'must' accredit Commonwealth agencies if they apply – there is no discretion to refuse accreditation. Nor are such agencies obliged to provide any evidence to support their application for accreditation. According to the EM, '[t]his approach recognises that non-corporate Commonwealth bodies meet the accreditation criteria as they are subject to relevant Australian Government policies and frameworks, and to ongoing oversight by Ministers. Relevant measures at the time of introduction include, but are not limited to, the Australian Government's Protective Security Policy Framework (PSPF), the Privacy Act, and the Australian Public Service (APS) Code of Conduct. These measures

ensure non-corporate Commonwealth bodies protect, manage, and use public sector data appropriately.'[18]

There is no doubt that Commonwealth bodies are subject to a range of policies and frameworks that regulate their data handling practices (including on privacy and security) and that this should be taken into account when accrediting entities under the scheme. However, under the proposed framework, if an agency has recently sustained a serious data breach (e.g., that is notifiable under the Privacy Act),[19] the NDC has no discretion to refuse accreditation. Nor is the NDC empowered to seek evidence that the agency has rectified the issue that caused the breach. According to the OAIC's most recent data breach statistics, Australian Government agencies entered the top 5 industry sectors to notify data breaches for the first time, notifying 6% of all breaches.[20]

Possible counterarguments include: that accreditation is one of several protections under the Bill and should be understood in that wider context; that it does not authorise any data sharing – entities must still formalise a data sharing agreement; and that data custodians must still assure themselves that accredited entities have appropriate arrangements in place before sharing. IIS accepts that such measures offer important protections, but they will work most effectively in concert with accreditation rather than as a stand-in for any gaps. Accreditation is fundamentally a preventative measure but, as currently formulated, risks operating as a reactive one (where something must go wrong before the accreditation framework is activated – for example, by suspending accreditation). It plays a different role to the Data Sharing Principles and Data Sharing Agreement but an important one and will be critical to ensuring that all entities are up-to-the-mark, so to speak, with their data handling arrangements.

Under the proposed framework, non-corporate Commonwealth bodies cannot fail accreditation. This is counter to the idea of accreditation as an independent assessment process that then acts as a form of trust mark and provides assurance to others that the entity meets defined standards or criteria. The fact that Commonwealth agencies are subject to policies and frameworks that indicate that they are already likely to meet accreditation criteria may justify a streamlined accreditation process, but there must still *be* a process and the NDC must have the discretion to refuse accreditation if the circumstances demand it.

Recommendation A – NDC to be given more scope for action in the accreditation process for non-corporate Commonwealth bodies

Rationale

While it may be reasonable to streamline the accreditation process for non-corporate Commonwealth bodies, there must still be a process for assessing those bodies' data handling practices and arrangements against the accreditation criteria. If the NDC cannot seek evidence

[18] DATB, EM, December 2020, [384].

[19] Under the Privacy Act, serious data security breaches must be notified – the Act defines these as breaches that are 'likely to result in serious harm' to any of the affected individuals; see *Privacy Act 1988,* s 26WE.

[20] OAIC, *Notifiable Data Breach Report: July-December 2020*.

to support an accreditation application or refuse an accreditation application, the whole framework is weakened.

IIS recommendation

Amend the Bill to:

- enable the NDC to seek evidence from a non-corporate Commonwealth body to support their application for accreditation
- enable the NDC to refuse to accredit a non-corporate Commonwealth body when there are sufficient grounds for doing so.

5.7.2 Accreditation criteria

The Bill establishes a set of accreditation criteria which includes the following:

- the entity is able to manage scheme data accountably and responsibly
- the entity has designated an appropriately qualified individual to be responsible for overseeing the management of scheme data
- the entity is able to apply the data sharing principles
- the entity is able to minimise the risk of unauthorised access, sharing or loss of scheme data
- the entity is committed to continuous improvement in ensuring the privacy and security of scheme data
- the entity is able to comply with an accredited entity's obligations under the data sharing scheme
- the entity's participation in the data sharing scheme would not pose concerns for reasons of security (within the meaning of the *Australian Security Intelligence Organisation Act 1979*)
- any additional criteria prescribed in the rules.

Aside from being very high-level, the accreditation criteria cover key areas of concern, in IIS's view. It is reassuring to see criteria related to privacy and security and such criteria should remain in any future iterations. For such criteria to be meaningful, however, they will need to be spelled out in more detail in the rules or supporting guidance material. For example, what does 'continuous improvement' in relation to privacy and security mean in practice, and does it include third-party audit and assurance?

PM&C confirmed that accreditation criteria will be supported with further detail in the Rules, which will outline types of evidence the entity will need to provide as part of their application. In addition, ONDC will publish guidance, guidelines and advice when the scheme comes into effect that will break down the types of evidence and materials that will be accepted as a part of the accreditation process.

It will be important that the standards for privacy and security are consistent with the Privacy Act and APPs. Security standards in particular will be important and should be risk based and tailored to what is 'reasonable in the circumstances to protect the information'. The approach to privacy governance

will also be a critical protection. Again, this is an area where given the wide range of possible organisations, their privacy governance approaches, experience and capabilities could also vary widely. IIS considers that in these circumstances, it would be useful to incorporate the OAIC's work on privacy governance, including privacy management plans and the Privacy (Australian Government Agencies – Governance) APP Code 2017 into the rules or associated accreditation framework.[21]

The NDC should consult the OAIC and other privacy regulators in Australia on the development of accreditation rules to ensure alignment with the privacy obligations and standards. The ONDC observed that existing requirements under s 17 of the *Legislation Act 2003* (Cth) require rule-makers to be satisfied that any consultation that is appropriate and reasonably practicable has taken place before a legislative instrument is made. IIS has therefore refrained from making a formal recommendation in this regard. We do, however, wish to record here our view that consultation with the OAIC on accreditation rules is appropriate and should be, in the circumstances, reasonably practicable.

Recommendation 1 – Align accreditation requirements with APP 1 and give regard to OAIC advice on privacy governance and management

Rationale

It will be important that the standards for privacy and security in the accreditation framework are consistent with the Privacy Act and APP framework, as the sharing scheme is open to a wide range of possible entities with different privacy governance approaches, experiences and capabilities.

IIS recommendation

Align accreditation framework requirements with 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.

5.7.3 Assurance that entities are complying with accreditation criteria and conditions

The effectiveness of accreditation also depends on a strong assurance process. While most Data Scheme Entities are likely to do the right thing, compliance with accreditation obligations cannot be taken for granted. An assurance process with oversight of compliance is necessary to ensure the integrity of the Data Sharing Scheme. This is a process that needs to be conducted, or at least overseen, by the NDC.

[21] See OAIC guidance on privacy management frameworks, available at <https://www.oaic.gov.au/privacy/guidance-and-advice/interactive-privacy-management-plan-for-agencies/> and <https://www.oaic.gov.au/privacy/privacy-registers/privacy-codes-register/australian-government-agencies-privacy-code/>.

IIS notes that overall industry practice is lacking in terms of third-party assurance for data handling. However, this is slowly shifting. For example, IIS has observed that some Australian public sector agencies with data sharing initiatives have become more active in seeking audits of participants' data practice.

More significantly, IIS notes the conditions imposed by the US Federal Trade Commission in its recent US$5 billion court order against Facebook that include:[22]

- Monitoring third party compliance with Facebook's terms through measures including 'ongoing manual reviews and automated scans, and regular assessments, audits or other technical and operational testing at least once every twelve (12) months'
- Engaging 'qualified, objective, independent third-party professionals… who (1) uses procedures and standards generally accepted in the profession; (2) conducts an independent review of the Mandated Privacy Program…'

This is a benchmark that will likely be repeated and become standard operating procedure.

The Bill contains some provisions that require accredited entities to report certain information to the NDC. For example, they must report on any changes in circumstances that may affect accreditation and assist the NDC in the preparation of the annual report. Furthermore, the Explanatory Memorandum notes that for the first accreditation criteria ('entity is able to manage scheme data accountably and responsible'), evidence to demonstrate this could include 'information about… audit and review.'[23] While those provisions are important, they do not necessarily involve a regular, recurring obligation on entities to confirm or demonstrate ongoing compliance with the terms of their accreditation.[24]

Recommendation 2 – Ensure that accreditation involves regular assurance that standards are being met

Rationale

The effectiveness of accreditation in protecting privacy depends not only on its associated rules, standards and guidance, but also on a strong assurance process that confirms Data Scheme Entities are doing the right thing. An assurance process with oversight of compliance is necessary to ensure the integrity of the Data Sharing Scheme.

IIS recommendation

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

[22] See FTC vs Facebook, Inc (2019), Stipulated order for civil penalty, monetary judgment, and injunctive relief in the United States district court for the District of Columbia, available at <https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf>.

[23] DATB, EM, December 2020, [402].

[24] See also the Financial Services Council submission which has more detail on audit and review, available at <https://www.datacommissioner.gov.au/exposure-draft/submissions>.

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.

5.7.4 Suspension or cancellation of accreditation

The NDC is empowered to suspend or cancel accreditation where the Commissioner reasonably believes that the entity has: breached their conditions of accreditation, failed to meet the accreditation criteria or breached the Bill itself. However, this provision does not apply to accredited entities that are (non-corporate) Commonwealth bodies. In such cases, it is the Minister who must direct the NDC to suspend or cancel accreditation for those bodies. It is not clear to IIS why Commonwealth bodies are treated differently here. Requiring the Minister to intervene implies a more onerous process for Commonwealth bodies – potentially making it harder for those bodies to be suspended from the Data Sharing Scheme when circumstances demand it.

PM&C explained that this approach provides consistency for the treatment of Commonwealth bodies (who are at other points subject to Ministerial rather than NDC direction, such as in relation to prescription under rules). However, this is not borne out by other accreditation provisions. Most Commonwealth bodies will be accredited by the NDC and even those prescribed by the Minister in rules are still formally accredited by the NDC. Moreover, it is the NDC that imposes conditions (if any) on Commonwealth bodies in relation to their accreditation. IIS notes that the OAIC and other accountability agencies directly regulate Commonwealth bodies, so it is unclear why the NDC should operate under a different model.

IIS's concern is that requiring ministerial direction in these circumstances slows down the process in cases where suspension or cancellation of accreditation may be urgent. The NDC will be the office-holder most equipped to ascertain and determine that suspension may be necessary as they and their office are the authority that is actively monitoring the scheme and receiving (non-personal data) breach notifications. It is unlikely that the Minister will have more or better information at hand to justify automatic deferral of such decisions to them. To be clear, IIS is not against the Minister having the power to direct the NDC to suspend or cancel an entity' accreditation. We only suggest that the NDC be equally empowered to do so without having to await the Minister's go-ahead.

While IIS has decided not to make a formal recommendation, we encourage further consideration of the matter to ensure the Accreditation Framework is sufficiently robust and responsive.

6. Findings and recommendations – Purpose, principles and agreements

The DATB framework takes a principles-based approach. It is characterised by high-level parameters, principles and words that are not defined but take their ordinary meaning. This approach has significant advantages. However, there will need to be clear messages to support the high-level concepts and principles, starting with the EM, and supported by clear rules and guidance to make sure it works in practice as the community would expect.

The section explores each of the key requirements for data sharing.

6.1 Data sharing purposes

The DATB seeks to ensure that Commonwealth data is shared for limited and specified purposes that address areas identified in the various reports as having the potential to deliver public benefit and that are likely to be within community expectations.

These purposes are: delivery of government services; informing government policy and programs; and research and development. There are also requirements that data is only shared where it is 'reasonably necessary' to contribute to the purpose and that the Data Custodian is sure it won't be used for other purposes.

Enforcement related purposes, along with purposes related to national security and any purposes prescribed in rules, are precluded. Regarding purposes prescribed in rules, the draft EM observes that: 'This provision enables the Minister to prescribe additional precluded purposes but not permitted purposes. This approach is intended to manage unintended expansions or interpretations of the data sharing purposes clause, and to ensure the scheme continues to operate as intended and in line with community expectations.'[25] IIS supports this approach.

IIS considers the data sharing purposes (and the formal exclusion of 'precluded purposes') to be an important element of the DATB's layered defence for privacy. However, this is an area where the approach to guidance and implementation could affect privacy outcomes. In particular, the meaning of the terms used, the application of the 'reasonably necessary' requirement (see Section 6.1.2 below), and the scope of the exclusion for enforcement related purposes, will be critical elements in ensuring that data sharing proceeds as anticipated in the purposes.

6.1.1 Preclusion of enforcement related purposes

As recommended in the June 2019 PIA, flagged in the Discussion Paper and raised by a range of concerned stakeholders in response to original proposals in the 2018 Issues Paper, the intention is that the DATB will exclude compliance and law enforcement as purposes for which data can be shared.

[25] Draft DATB, EM, July 2020, [109].

In the various submissions, the June 2019 PIA, and the Discussion Paper, there is discussion of what activities might be included in the terms 'compliance' and 'assurance.' The Discussion Paper suggests that:

> 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.[26]

The June 2019 PIA does not define compliance but notes reasons why (taking account of submissions and the PIA consultants' own views) it should be excluded. These include that: compliance is difficult to define; it necessarily implies identification of, and consequences for, individuals and raising the privacy risk profile of the DATB; the activity is a poor fit for the Five Safes (now reflected in the DATB Data Sharing Principles); data quality and timeliness would be issues; and the quantity of data needed for compliance could undermine or side line the data minimisation principle.[27]

The current DATB excludes 'enforcement related purposes', an exclusion intended to cover compliance related activities. These are defined in the DATB as including detection, investigation, prosecution or punishment of criminal offences, matters detrimental to public revenue, as well as other related matters.

Drafting has drawn on the definition of 'enforcement related purposes' from the Privacy Act rather than create a new legal concept associated with 'compliance'.[28] The use of an existing legal term is expected to provide greater certainty on interpretation given existing commentary and case law. The ONDC considers compliance activities fall within several categories of the 'enforcement related purposes' definition. The Privacy Act definition includes 'prevention' of criminal offences or other breaches of specified laws. The ONDC advised that 'prevention' to the extent that it would involve general policies and programs is consistent with the objects of the DATB, whereas the other activities (detection, investigation, prosecution and punishment) targeting specific individuals and entities are ruled out. Similarly, the exclusion refers to 'detrimental' to the public revenue rather than the broader Privacy Act formulation 'protection' of the public revenue. Again, the intention is to permit general policy and program activities while ruling out those targeting individuals.

IIS is concerned about ongoing uncertainty as to whether compliance and assurance activities are ruled in or out. Without a clear statement to the contrary, there may be a view that compliance is intrinsic to the delivery of government services (a permitted purpose) rather than an enforcement related activity (a precluded purpose).

---

[26] Discussion Paper, p 25.

[27] June 2019 PIA, p 12.

[28] See Privacy Act, s 6.

Recommendation 3 – Draft DATB to effectively exclude sharing for compliance and assurance purposes

Rationale

The current draft of the DATB precludes 'enforcement related purposes', which are intended to include compliance and assurance. These terms do not appear in the definition as such. This could lead to confusion; for example, about whether compliance is seen as an intrinsic part of the delivery of government services rather than an enforcement related activity. While the Explanatory Memorandum provides this intent, it would be preferable for this to be indicated in the DATB.

IIS recommendation

Ensure that the DATB is drafted in such a way that there is no doubt that 'precluded purposes' include compliance and assurance. Amend the Explanatory Memorandum and supporting guidance material to make it clear that compliance and assurance activities are precluded.

Update: The DATB now provides a list of enforcement-related purposes that are precluded purposes. The EM notes that the enforcement-related purposes include a range of detection, investigation and law enforcement activities that would be best carried out under dedicated laws. IIS considers Recommendation 3 to have been addressed.

6.1.2 Meaning of the data sharing purposes

The three purposes for which data sharing can be undertaken were generally, but not universally, accepted in responses to the Discussion Paper. The DATB names these purposes – delivery of government services, informing government policy and programs, and research and development – but does not expand on their meaning or scope. While there are commonly accepted meanings of these words, there can be wide variations in what might be encompassed. As noted above, enforcement related purposes, purposes related to intelligence activities and purposes prescribed in rules are 'precluded' meaning that sharing in aid of those purposes is not authorised. These precluded purposes offset some of the privacy impact of data sharing by establishing appropriate constraints.

Commercial uses and applications could occur under the permitted purposes. This does not mean public data will be sold, but it could mean that commercialisation arises from research and development conducted by an Accredited Entity (see further discussion on commercial activities at Section 6.1.5). This highlights the need for boundaries to the data sharing purposes being clear.

During this PIA process, IIS identified a need for strong signposts in the EM to clarify the meaning of each of the three purposes and 'what is in and what is out.' IIS suggested that this include being transparent about the fact that the purposes could encompass commercial activities. A narrowly defined purpose test working in concert with the Data Sharing Principles should help manage risks of function creep and secondary use of data beyond community expectations.

Recommendation 4 – Articulate meaning of permitted purposes in Explanatory Memorandum

Rationale

In addition to the proposed principles and controls in the Data Sharing Scheme, there is value in restricting the definition and interpretation of permitted purpose under the draft DATB, so as to arrest function creep and expansive uses that go beyond community expectations.

IIS recommendation

Address the expected data sharing purposes in the Explanatory Memorandum, 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.

Update: In line with the advice provided by IIS during the PIA process, the EM now articulates the meaning of data sharing purposes. Therefore, IIS considers Recommendation 4 to have been addressed.

6.1.3 Participation of AUSTRAC, the AFP and the Department of Home Affairs

Data sharing is authorised as long as the conditions in the '*Authorisations to share data'* clause are met and the sharing is not 'excluded'. The '*When sharing is excluded from the data sharing scheme'* clause excludes data sharing involving excluded entities. These are defined in the Bill and include prescribed intelligence agencies. Those agencies cannot participate in data sharing and data originating from those agencies is also excluded from the Data Sharing Scheme.

AUSTRAC, the Australian Federal Police (AFP) and the Department of Home Affairs (as the agency o the Minister administering the *Australian Border Force Act 2015*) are able to participate in the Data Sharing Scheme other than in relation to their 'operational data' which the Bill excludes. These agencies are also subject to the preclusion of data sharing for enforcement related purposes discussed in Section 6.1.3 above.

Given the concerns raised by stakeholders about the use of the Data Sharing Scheme for enforcement and compliance, IIS has particularly examined the participation of AUSTRAC, the AFP and the Department of Home Affairs in the Scheme. We find that the data sharing activities of such agencies are appropriately curtailed by the precluded purposes provisions – so long as the DATB is drafted in such a way that there is no doubt that 'precluded purposes' include compliance and assurance (see Recommendation 3). As pointed out in the EM, data sharing related to law enforcement and national security is 'best performed and managed under dedicated legislation that provides tailored protections and redress mechanisms to ensure procedural fairness.'[29] AUSTRAC, the AFP and the Department of Home Affairs would also be subject to the other protections applying

[29] Draft DATB, EM, July 2020, [108].

to data sharing under the DATB including purpose limitation, data minimisation, Data Sharing Principles, accreditation and Data Sharing Agreements which must be published.

6.1.4 Commercial activities

In its current form, the DATB allows for commercial applications arising as a result of data sharing provided all provisions of the DATB can be met and are complied with. 'Commercial activities' are not a separate 'permitted purpose'; the data must be used only for one of the three purposes already discussed (delivery of government services; informing government policy and programs; and research and development) and meet the other DATB requirements. IIS also notes that the Data Sharing Scheme does not permit data to be sold and places limits on use and publication of data outputs via the Data Sharing Agreement. By way of example, the EM points out that data could be shared for research and development and a resulting output – such as improved pharmaceutical treatment for heart disease – could return a public benefit to the community as well as profit to the Accredited Users involved.[30]

The possible commercial applications of the outcomes of research and development was an issue of strong discussion and differing views in the consultations related to the DATB and this PIA. Stakeholders raised questions about the very concept of private sector organisations monetising public sector data, about how to assess value to the community, and about the risks, including re-identification of personal information involved. They also raised commercial uses of particular concern including sharing data with private sector organisations for service delivery and the use of shared data or outputs in automated decision making or the development of problematic algorithms in artificial intelligence.[31]

Given these concerns, IIS considered the matter closely. We came to the view that possible commercial applications of the data were adequately checked by the range of protections in place – particularly public interest and ethics requirements but also the Data Sharing Principles more generally, purpose limitation, data minimisation and the requirements contained in Data Sharing Agreements. These create a high bar for sharing to support commercial activities. It is also important to note that use of public sector data for commercial purposes is not prohibited by the Privacy Act – as long as agencies meet the requirements of the APPs in relation to any use or disclosure of personal information. Viewed from this perspective, the DATB adds additional layers of defence to the APPs by requiring Data Sharing Agreements, user accreditation, public interest and ethics requirements and consent (where reasonable and practicable), as a matter of course.

That said, given stakeholder concern about this aspect of data sharing, the issue needs careful oversight and consideration during future legislative reviews of the DATB. Work is needed to provide sufficient reassurance both in the lead up to the introduction of the DATB and during the implementation phase. This could involve detailed guidance on the application of the ethics (see Section 6.4) and public interest requirements (see Section 6.6), and further thinking about possible

[30] DATB, EM, Draft, July 2020, [106].

[31] IIS understands that stakeholders will be afforded further opportunities to consider this issue during public consultation on the draft DATB before it is introduced to Parliament.

commercial use scenarios and their implications, as well as continuous NDC oversight. In addition, the NDAC has a role to play in advising the NDC on data sharing for commercial purposes and meeting community expectations.

6.2 The Data Sharing Principles

The Five Safes Framework has been one of the core building blocks for the Data Sharing Scheme.[32] The ONDC's consultations on its Discussion Paper identified that 'safe' could be seen as an over promise, suggesting that there are no risks in data sharing. The Five Safes are retained as part of the Data Sharing Scheme but are remodelled as the Data Sharing Principles.

The Data Sharing Principles are high-level. They introduce important directions, particularly in relation to ethics, consent, and public interest. The DATB also provides that 'a data scheme entity's sharing of data is not consistent with the data sharing principles… unless the entity is satisfied that each principle is applied to the sharing in such a way that, when viewed as a whole, the risks associated with the sharing are appropriately mitigated.'[33] However, the high-level framing of the principles may create uncertainty about the standards that apply and the meaning of words such as 'appropriate'. Some submissions to the Discussion Paper also expressed concern that it would not be clear that the DATB and the Data Sharing Principles do not displace Privacy Act obligations. This was also a theme in IIS's discussions with stakeholders for this PIA (see Section 4).

To help explain the concepts inherent in the Data Sharing Principles and to assist Data Custodians making decisions under the Data Sharing Scheme, the PM&C prepared the Data Sharing Principles Guide (the Guide).[34] This was available to all stakeholders during the consultation and development processes for the DATB. The Discussion Paper notes that the Guide was developed with local and overseas experts and was well received. IIS agrees that the Guide provides a clearer picture of what is expected. We understand the Guide will be amended when the DATB becomes law, including to take account of changes to the key policy positions underpinning the DATB.

IIS considers that the high-level nature of the Data Sharing Principles poses a privacy risk for the Data Sharing Scheme. IIS appreciates the power and flexibility of principle-based legislation (see Section 5.2). We also appreciate that the principles do not have to do all the work of protecting shared data – they are only one part of the framework, which also includes accreditation of Data Scheme Entities, defined data sharing purposes, transparent and enforceable Data Sharing Agreements, and regulatory support and enforcement powers. They are, however, a critical element.

IIS has considered the detail of the Data Sharing Principles further below. The need for guidance on specific matters is noted in a number of places. IIS understands, and welcomes, that the ONDC is

---

[32] 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. A description of the Five Safes is at <https://www.abs.gov.au/ausstats/abs@.nsf/Latestproducts/1160.0Main%20Features4Aug%202017>.

[33] DATB, cl 16(11).

[34] PM&C *Best Practice Guide to applying Data Sharing Principles* (15 March 2019), available at <https://www.pmc.gov.au/sites/default/files/publications/data-sharing-principles-best-practice-guide-15-mar-2019.pdf>.

already identifying the need for and developing guidance material. As noted, this would include updating the Guide to align with the DATB.

6.3 Project principle – overview

The project principle is that data is shared for an appropriate project or program of work. The principle includes, but is not limited to, the following elements:

- The sharing can reasonably be expected to serve the public interest
- Any applicable processes relating to ethics are observed
- Any sharing of the personal information of individuals is done with the consent of the individuals, unless it is unreasonable or impracticable to seek their consent
- A requirement for the Data Custodians to consider using an Accredited Data Service Provider (ADSP) to perform data services in relation to the sharing.

6.4 Project principle – public interest

The Project Principle requires Data Scheme Entities to ensure that the sharing can reasonably be expected to serve the public interest. This is supported by a corresponding requirement that Data Sharing Agreements include a description of how the public interest is served by the sharing. Consideration of the public interest will support Data Custodian decision-making about whether or not to share data. The ONDC considers this provision to be part of the package of measures – the layered defence – that would allow data to be shared safely, including for commercial activities. Another layer of defence is that the DATB does not compel Data Custodians to share data.

'Public interest' is not defined in the Bill. IIS considered the desirability of introducing a definition. On this point, other laws and jurisdictions were instructive – particularly the FOI Act and the Privacy Act. While these laws play a different role to each other and to the DATB, all regulate the handling of personal information in some circumstances and all contain a public interest element.

The FOI Act applies a public interest test to the release of certain types of records. The Act does not define public interest but does specify factors favouring access in the public interest (s 11B(3)) and factors irrelevant to weighing the public interest (s 11B(4)). The Information Commissioner's FOI Guidelines issued under s 93A of the FOI Act offer further guidance on applying the public interest test.[35] Relevantly, they list interference with an individual's right to privacy as a factor weighing against disclosure.

The Privacy Act seeks to avoid marginal decisions about the public interest for health research by requiring that the public interest in the use of health information in research 'outweighs to a substantial degree the public interest in maintaining adherence to the Australian Privacy Principles'. The Australian Law Reform Commission (ALRC) considered definitions of 'public interest' in its 2014

[35] OAIC Guidelines issued by the Australian Information Commissioner under s 93A of the *Freedom of Information Act 1982*, available at <https://www.oaic.gov.au/assets/freedom-of-information/guidance-and-advice/foi-guidelines/foi-guidelines-combined-november-2019.pdf>.

inquiry into privacy in the digital age.[36] It decided against defining the term, noting, among other things:

> In the UK, the Joint Committee on Privacy and Injunctions concluded that there should not be a statutory definition of the public interest, as 'the decision of where the public interest lies in a particular case is a matter of judgment, and is best taken by the courts in privacy cases'. [37]

In IIS's view, if the public interest requirement is to do the heavy lifting to give public confidence in allowing commercial uses into the Data Sharing Scheme, the factors to be weighed in determining the public interest will need to be credible and transparent. Submissions to the Discussion Paper commented on the need for:

- A strong case to be made when data sets contain personal information and therefore the process to consider the public interest needs to be strong
- Weighing of public interest to include impact on individual privacy
- The public interest to be built into guidance and training.

IIS recommends that the NDC develop detailed guidance, and training material, to assist Data Scheme Entities in weighing the public interest. Such guidance should address factors that may weigh against data sharing, including the public interest in protecting and respecting individuals' right to privacy. The guidance should also give regard to relevant existing frameworks and existing concepts such as the no-harm principle.[38] Given the importance of the public interest requirement, the first statutory review of the Bill and the NDC's Annual Report should report on how the public interest requirement is working in practice.

6.5 Project principle – ethics

The Project Principle also requires that any applicable processes relating to ethics are observed. This provision aims to set further expectations about matters that should be considered when Data Custodians make decisions to share data. It recognises that ethical considerations may arise in data sharing projects, such as those involving possible commercial applications or the participation of private sector organisations. Along with the other layers of defence in the DATB, this provision aims to reassure the community that data will be shared for appropriate purposes and with appropriate safeguards. The ethics component may also offset risks associated with cases where it is 'unreasonable or impracticable' to seek consent (consent is discussed in the next section).

---

[36] ALRC, *Serious Invasions of Privacy in the Digital Era (DP 80)* (2014), available at <https://www.alrc.gov.au/publication/serious-invasions-of-privacy-in-the-digital-era-dp-80/>.

[37] Id, [8.35].

[38] See, for example, the submission of ElevenM to the DATB exposure draft, [30], available at <https://www.datacommissioner.gov.au/exposure-draft/submissions>.

The DATB does not define ethics. It is a broad concept. The Ethics Centre's take on the issue is that an ethical decision is 'the one which best achieves what is good, right and consistent with the nature of the things in question'.[39]

Ethics considerations are often part of frameworks for weighing the public interest in a particular activity. For example, the National Health and Medical Research Council's (NHMRC's) Guidelines under s 95 of the Privacy Act provide a framework for decisions about the collection, use and disclosure of health information for medical research without consent. Recently, 'ethics' has been part of discussions in the private sector about ways to gain and maintain social licence for the increasing use of data analytics.[40]

However, the ethics requirement (which is to consider any applicable framework) is not meant to impose a new formal ethics test, to replace the provisions in the Privacy Act, or to specify the involvement of a particular body such as the NHMRC.[41] What is intended is to assist in good decision-making about what is appropriate and what might have a disproportionate impact, including on privacy. Some Data Custodians will already have a good understanding of existing frameworks and how ethics might be considered. Others will be less experienced.

In IIS's experience, having a systematic framework for thinking about what is and is not acceptable has been helpful for organisations seeking to expand their use of customer data. It could well be helpful in assisting Data Scheme Entities to work within community expectations.

IIS considered whether to recommend reference to a formal process, such as the NHMRC guidelines, where personal information is involved. However, we appreciate that these guidelines would not necessarily be applicable to all data sharing processes. And there could be duplication of effort; for example, many of the matters that must be addressed under the NHMRC guidelines are also included in a Data Sharing Agreement. Apart from any other considerations, whatever an appropriate ethical framework might entail, putting it into legislation would be a fast way to be out of date.

At the same time, IIS considers that the ethics component is less likely to work as a privacy measure and to help build community confidence in the Data Sharing Scheme, if the processes used lack transparency and accountability. As a minimum the NDC should develop guidance on the range of applicable ethics processes and the frameworks that could be applied in particular circumstances, including when reference to an independent external ethics committee would be needed. Where sensitive personal information is involved such as health information, the decision-making process should be through a properly constituted and formal Ethics Committee along the lines set out by the NHMRC. The guidance should also make clear how the ethics component would interact with existing provisions in the Privacy Act.

---

[39] The Ethics Centre, available at <https://ethics.org.au/why-were-here/what-is-ethics/>.

[40] See for example, Jacob Metcalf, Emily F. Keller, and danah boyd, *Perspectives on Big Data, Ethics, and Society* (23 May 2016), available at <http://bdes.datasociety.net/council-output/perspectives-on-big-data-ethics-and-society/>.

[41] NHMRC Guidelines under s 95 of the Privacy Act, available at <https://www.nhmrc.gov.au/about-us/publications/guidelines-under-section-95-privacy-act-1988>.

Recommendation 5 – Provide guidance on the ethics process in appropriate circumstances

Rationale

The draft DATB anticipates the possible need for ethics consideration to support appropriate data sharing. Existing ethics frameworks and guidelines would not necessarily apply to all data sharing processes under the Scheme. There is value in the NDC providing guidance on this matter.

IIS recommendation

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:

- 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.

6.6 Project principle – consent

The Discussion Paper noted that 'Consent is one of the most divisive topics we heard about in our consultations'.[42] It canvassed the range of positions on the issue, which vary from seeing individual consent as a pre-requisite to data sharing, to wariness about consent processes as a panacea, to seeing requirements for consent as an impediment to research, potentially undermining public benefits.[43] The position arrived at was:

> '[T]hat the legislation [will] 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'[44]

Following consultations on the Discussion Paper, which again saw a focus on consent, the DATB position, via the project principle, is that 'any sharing of the personal information of individuals is done with the consent of the individuals, unless it is unreasonable or impracticable to seek their consent'.

Consent is now elevated as a first principle, making it more of a positive duty for Data Custodians and Accredited Users to consider what is reasonable and practical in the circumstances. This does not mean that consent will need to be, or should be, sought in all cases where personal information is

[42] The Discussion Paper noted competing views about consent, p 33.

[43] Discussion Paper, pp 7 & 33.

[44] Discussion Paper, p 32, see further p 33.

shared. It is not new in the world of research for consent to be waived under an approved ethics process.

If applied well IIS considers this formulation could strike the right balance.

This view takes into account that by and large it won't be possible to obtain consent in the context of data sharing activities. The information will often have been collected where data sharing was not contemplated, or where it was flagged only as a possibility, with none of the required detail to inform consent. As outlined in the Discussion Paper, there are also circumstances where sharing data only with consent would work against possible research outcomes that would otherwise be in the public interest.[45]

IIS considers that the consent issues for the DATB are different from those in the global discussion where it is now well recognised that notice and consent have failed as a mechanism to empower individuals. Consent has been an abused concept world-wide. The ACCC gave a stark overview of the issues in its 2019 Digital Platforms Inquiry.[46] Similarly, a 2018 article cited the finding in a nation-wide survey on consumer attitudes that people don't read privacy policies and argued that this is rational behaviour in the face of factors such as the inability to negotiate better terms or needing to use a service.[47]

What is being done with consent in the Data Sharing Scheme has to be seen against those concerns. Community confidence in the Scheme is more likely to build, if the circumstances are seen to be different and the levels of protection are seen to be different.

In this regard, IIS notes that even where consent is obtained, the other provisions of the DATB will still apply. Data will still only be shared with Accredited Users in accordance with Data Sharing Agreements. This is a belt and braces approach – consent is not being asked to do all the work. Apart from any other considerations, this potentially takes some pressure off risks such as 'bundled consent' and should allow for real consent in the right circumstances.

As with other elements of the DATB, the consent element provides a signpost rather than a detailed road map.

The challenge will be in making sure that consent only comes into play when individuals have a real choice and are fully informed and, if consent is not reasonable or practical, making the other control processes work well, including by monitoring use and acting against bad practice.

---

[45] Discussion Paper, p 33.

[46] Australian Competition and Consumer Commission, *Digital Platforms Inquiry – Final Report* (June 2019), Chapter 8, available at <https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf>.

[47] Katherine Kemp, *94% of Australians do not read all privacy policies that apply to them – and that's rational behaviour, The Conversation,* (14 May 2018), available at <*https://theconversation.com/94-of-australians-do-not-read-all-privacy-policies-that-apply-to-them-and-thats-rational-behaviour-96353*>.

IIS considers that consent is an area where a lot of help and guidance will be needed, as well as monitoring and assurance. Areas where IIS has identified the need for actions, and which are discussed below, are as follows:

- When should consent come into play
- Meaning of 'unreasonable or impracticable'
- Decisions about 'unreasonable or impracticable'
- Standard of consent.

6.6.1 When consent should come into play

The consent element of the Project Principle would apply to all the permitted data sharing purposes prescribed in the Bill, including delivery of government services.

IIS accepts that there could be good reasons to share information in the absence of consent, particularly where individuals will not have a real choice about the sharing. However, the DATB should not remove real choice when it would otherwise be available. This could be the case, some submissions to the Discussion Paper argued, where delivery of government services is involved.

The Discussion Paper indicated that 'the final purpose (delivery of government services) will involve the sharing of personal information and support better outcomes targeted at individuals no matter what cohort they belong to'.[48] The combination of service delivery and direct contact with the individuals concerned would on its face make it difficult to see why consent would not be a feasible option to authorise sharing the information to provide services to them.

IIS appreciates that there might be circumstances, even with delivery of government services, where there could be a case to proceed without consent. Guidance on application of the Data Sharing Principles, developed in consultation with the OAIC, and with Accredited Users and individuals or their representatives, should make clear the circumstances when consent would be expected and when it might not be reasonable and practical. The NDC should also include monitoring consent approaches in the regulatory action plan.

The PM&C response to the APP 5 recommendation in the July 2019 PIA noted 'that some agencies' Privacy Notices already inform people that their data may be shared for government and research purposes.' It also indicated that notices under APP 5 are within the remit of the Australian Information Commissioner.

IIS notes that poor practice with privacy notices and privacy collection statements results from the conflation by entities of the requirements of APP 1 and APP 5. The Information Commissioner has flagged this as an issue in recent times. IIS understands that the NDC intends to work closely with the Information Commissioner to support compliance, and on any relevant guidance in this area. In

[48] Discussion Paper, p 21.

particular, in preparation for the commencement of the DATB, the NDC and the OAIC should work together to advise agencies on any changes to their collection notices.

However, in IIS view, many of the usual collection (APP 5) notices would not provide either sufficient or clear information to allow individuals to make informed choices about data sharing for government service. IIS sees a need for detailed guidance to ensure Data Custodians provide sufficient information to inform consent in these circumstances. This could be in the APP Guidelines or in specific guidance on the Data Sharing Principles. The NDC should work closely with the OAIC, and privacy regulators in other jurisdictions in developing guidance on consent.

6.6.2 Meaning of 'unreasonable or impracticable'

The DATB concept of 'unreasonable or impracticable' draws on the use of these words in the Privacy Act. These terms appear specifically in sections 16A and 16B, which spell out a range of exceptions to the APPs on collection, use and disclosure of personal information, including where it is 'unreasonable or impracticable' to obtain consent. These are generally for other public interests including law enforcement, but also where health information is collected, used, or disclosed for research.[49]

The term 'unreasonable and impracticable' are not specifically defined in Privacy Act. The APP Guidelines advise that the ordinary meanings of the words would apply, and this will depend on the circumstances. Relevant circumstances for the Data Sharing Scheme outlined in the APP Guidelines include:

- The impact on the integrity or validity of health research
- The number of individuals involved
- The ability to contact individuals, for example because their location is unknown after reasonable enquiries have been made, or if they cannot be contacted for another reason
- The inconvenience, time and cost involved in obtaining consent.

The APPs, or comparable principles, will apply to Data Custodians and Accredited Users and so the relevant guidance would be a source of information to assist in decision-making.

Some Data Custodians will already be experienced in thinking about consent and whether or not it should be obtained. But given the potential for an increased set of participants in the Data Sharing Scheme there is likely to be a need for clear guidance both to help new players and promote good practice and consistency, complemented by a focus in NDC oversight, compliance and enforcement strategy on the approach taken by the new players.

[49] IIS notes that the Bill excludes the operation of ss 16A and16B of the Privacy Act. However, we consider that the NDC guidance on seeking consent when sharing health information should be informed by or based on the OAIC guidance developed for s 16B. For example, the circumstances where consent would be unreasonable or impracticable in a s 16B context may be relevant to the application of the consent mechanism in the Project Principle.

There should also be consistency between the NDC guidance and the APP Guidelines on the meaning and application of 'unreasonable or impracticable'. In addition, as IIS has flagged above, the NDC guidance should start from the premise that would be hard to argue it would be 'unreasonable or impracticable' to seek consent in the context of delivery of government services. If this approach is not already contemplated in the APP Guidelines, IIS recommends that the NDC work with the OAIC to address this.

6.6.3 Decisions about 'unreasonable or impracticable'

As with application of other aspects of the DATB, the Data Custodian would decide whether there was case to share data without consent. They would rely on discussions with Accredited Users and information that would then be set out in Data Sharing Agreements.

IIS understands that guidance on the DATB would indicate that in making consent decisions, Data Custodians can ask for the data sharing to be subject to ethics approval by a 'formal ethics committee approval process'.

In addition, IIS considers that Data Custodians should, if a case is being made against consent, be required to consider why de-identified data would not fit the purpose and why obtaining consent is unreasonable or impracticable. This should be made clear in the NDC's guidance. In addition, the NDC guidance should emphasise that the application of consent under the DATB should be consistent with, and not undermine, Privacy Act requirements. Collection, use and disclosure of health information for research, where consent is unreasonable or impracticable, can be carried out in accordance with guidelines approved under ss 95 and 95A of the Privacy Act.[50]

IIS understands the intention is that this protection and process would remain in place, but it is a matter that is worth spelling out.

6.6.4 Standard of consent

As already flagged, the term consent in the DATB would take its ordinary meaning. The ONDC indicates, and this would be made clear in the EM and guidance, that the consent for the DATB aligns with the Privacy Act and the APP Guidelines. The Guidelines state that valid consent has the following elements:

- The individual is adequately informed before giving consent
- The individual gives consent voluntarily
- The consent is current and specific, and
- The individual has the capacity to understand and communicate their consent.[51]

[50] National Health and Medical Research Council, Guidelines approved under s 95 of the Privacy Act, available at <https://www.nhmrc.gov.au/about-us/publications/guidelines-approved-under-section-95a-privacy-act-1988>.

[51] APP Guidelines, [B.35].

Valid consent is defined in a similar way in the European Union General Data Protection Regulation (GDPR).[52]

As flagged earlier, IIS would agree with sentiments in the wider community that standards of consent very often do not meet these conditions. More needs to be done to ensure the preconditions are met. To date, effective implementation and enforcement has been wanting.

It is possible that there will be less risk of poor privacy practices, and less impact for individuals, in the DATB context. Data Custodians have a range of options by which to share data and would have less need to rely on consent to authorise data sharing activities. The layered approach in the DATB also seems likely to help offset privacy impacts for individuals if the circumstances mean consents given do not meet the standard above. IIS nevertheless counsels a best practice approach to consent. Community acceptance is at risk without this.

IIS considers that there has been so much abuse of the concept of consent that it would be preferable to include the elements of valid consent in the DATB. In addition, the EM should specify the standard of consent expected. The NDC guidelines should also address the issue, including by reference to the APP Guidelines, and the NDC should include oversight of Data Scheme Entities approach to consent in its regulatory action plan.

Recommendation 6 – Provide guidance on how consent operates in the Data Sharing Scheme

Rationale

The concept of consent has been well-defined by privacy law and guidance, albeit poorly implemented in practice. Data sharing raises new challenges and considerations for consent. There is value in the NDC providing guidance on this matter.

IIS recommendation

Specify, in the EM, guidelines and other guidance material, matters such as:

- 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.

[52] OAIC, guidance on the GDPR, available at <https://www.oaic.gov.au/privacy/guidance-and-advice/australian-entities-and-the-eu-general-data-protection-regulation/>.

6.7 People principle

The people principle is that data is made available only to appropriate persons. To meet this principle, data custodians must consider the accreditation status and history of the entity collecting and using the shared data. Further, data is only to be shared with people who have attributes, qualifications, affiliations and expertise appropriate to the sharing.

This principle 'is intended to ensure data custodians take account of the recipient's past performance (including length of accreditation and any known data breaches) and any conditions on its accreditation that are relevant to suitability for the proposed project.'[53] IIS does not have concerns about the formulation of this principle, other than to note that having a sound accreditation process will ensure data custodians are supported in assessing the capability of any potential recipient of data (see Section 5.7 for further discussion of accreditation). As with other principles, the people principle would benefit from further explanation in the Guide or other supporting material to assist Data Scheme Entities in meeting their obligations.

6.8 Setting principle – security

The DATB's setting principle is that 'data is shared in an appropriately controlled environment'. This entails ensuring that 'the means by which the data is shared are appropriate, having regard to the type and sensitivity of the data, to control the risks of unauthorised use, sharing or release.'[54] It also involves applying reasonable security standards when sharing data.

The setting principle requires Data Scheme Entities to take account of the risks that expanded sharing of personal information, and de-identified information about individuals, could entail. The changing social and technological environment and the potential scale of the information flows means security risks are inherent and heightened. Sharing data multiplies and necessarily increases the risk profile of the entities that transmit and hold it. (The inverse of this is 'if you don't hold it, you can't be breached'). Data sharing may also enable the creation of 'data honeypots' that are attractive to hackers for the richness of the data they contain, or for the transfer process to be breached.

The DATB approaches security at a number of key points, including:

- The DATB accreditation framework requires security standards to be met.
- The DATB sits alongside but does not replace obligations in APP 11 (and other privacy law equivalents) requiring reasonable steps to protect personal information.
- The DATB includes data breach notification requirements for Data Scheme Entities and seeks to ensure the data breach notification provisions under the Privacy Act continue to apply to shared data.

[53] DATB, EM, December 2020, [125].

[54] DATB, cl 16(6)(a).

- The setting principle calls for specific consideration of whether data is shared in a sufficiently controlled environment.
- Regulatory and enforcement measures apply in the event that things go wrong.

Security will be an important area for guidance and should be included in the NDC's compliance and monitoring strategy. In addition to pointing to relevant standards, risk assessment and security management plans, IIS emphasises the need for proper security governance of data sharing activities. This would include a senior person responsible and provision for monitoring and assurance.

6.9 Data principle

The data principle is that appropriate protections are applied to the data. In contrast to the settings principle, the data principle focuses on the treatment of the data itself (for example, data minimisation, aggregation, removal of direct identifiers, cell suppression and so on). Such techniques help control for risks that are not otherwise addressed by the project, people and setting principles.

The data principle contains a data minimisation requirement: that only the data reasonably necessary to achieve the applicable data sharing purpose is shared. It further seeks to reduce privacy impacts by requiring that the sharing of personal information be minimised as far as possible without compromising the data sharing purpose.

6.9.1 Data minimisation

In line with the June 2019 PIA, and the Discussion Paper, the DATB includes a 'data minimisation element'. Data should only be shared if it is reasonably necessary to achieve the applicable data sharing purpose and the data custodian is satisfied that the data will not be used for any of the precluded purposes (for example, enforcement related purposes or national security). Further changes to the Bill now see the added requirement that 'sharing of personal information be minimised as far as possible without compromising the data sharing purpose.'

These data minimisation provisions are important and necessary for reducing privacy impacts of the Scheme. They provide a clear statement of intent. However, data minimisation provisions in the Privacy Act[55] have, in IIS's experience, provided only the broadest of limitations. Issues of this sort were in part the reason for the Australian Competition and Consumer Commission's (ACCC) Digital Platforms Inquiry, and the Government response calling for a review of the Privacy Act; the acknowledgement is that the current law is not sufficiently strong.[56]

It is reassuring to see the data minimisation provision expanded to specify that sharing of personal information, in particular, should be minimised.[57] Nevertheless, the risk remains that the concepts

[55] For example, Privacy Act, Schedule 1, APP Guidelines 3.1.

[56] Australian Competition and Consumer Commission, *Digital Platforms Inquiry – Final Report* (June 2019), Executive Summary, p 3, available at <https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report%20-executive%20summary.pdf>.

[57] See DATB, cl 16(8)(b).

'reasonably necessary' and 'as far as possible' are 'read down' over time – with consequent impact on privacy and public confidence – unless the requirement is reinforced with clear guidance and strong enforcement. IIS supports the ONDC's intention to address this matter in guidelines.

6.9.2 De-identification

The data minimisation requirement necessarily asks scheme entities to decide whether identified information is necessary for a given project. Providing de-identified data would be one way to comply with the Bill's data minimisation requirement, provided the proposed project is for a permitted purpose and can be achieved using de-identified data. IIS recommends that the NDC issue guidance on this matter and actively monitor it (see Appendix D).

Steps to de-identify data either before it is shared, or in the outputs phase, are important privacy protections. Current best practice advice here includes, for example, the De-identification Decision-Making Framework developed by the OAIC and CSIRO's Data61.[58]

However, as is now well understood and outlined in such guides, 'de-identification' or 'anonymisation' does nothing other than make data more difficult to identify. It does *not* guarantee there will never be 'identification' or 'personal information' in the data set. There are myriad examples showing that this is the case.[59] It is ever clearer that 'de-identification' or 'anonymisation' cannot be sold as a standalone panacea. It is a useful contributor to privacy when combined with the other principles, in particular the setting principle and the limitations on further sharing in the DATB (particularly in the provisions related to Data Sharing Agreements).

IIS considers de-identification, and the related risk of re-identification, are matters that should be addressed in NDC guidance. IIS is not suggesting guidance on de-identification as such; as noted this is well covered in the OAIC de-identification guide.

However, the guidance could set the expectation that where personal information is involved, it should be de-identified if possible. In addition, where de-identified data is used, the risks of re-identification must also be considered. IIS appreciates that there will be circumstances where the purpose cannot be served by de-identified information, and that indeed there could be a project in the public interest that did involve re-identification at some point in the process. What will be important is for the risks in handling even de-identified data to be recognised. There could be a case for additional requirements in Data Sharing Agreements, for example, making the Accredited Users responsible for prohibiting re-identification or attempts at re-identification, unless otherwise agreed.

---

[58] Available at <https://www.oaic.gov.au/privacy/guidance-and-advice/de-identification-decision-making-framework/>.

[59] Karl Bode, *Researchers Find 'Anonymized' Data Is Even Less Anonymous Than We Thought* (4 February 2020), available at <https://www.vice.com/en_us/article/dygy8k/researchers-find-anonymized-data-is-even-less-anonymous-than-we-thought>.

In addition, the NDC should monitor practices in this area and, if needed, provide additional guidance or seek additional protections. IIS considers this is also an area that would be valuable for the NDAC to have on its agenda.

6.10 Outputs principle

The outputs principle is that outputs arising from the sharing of scheme data are as agreed. IIS understands this formulation is intended to make the Data Sharing Agreement paramount. The principle does not allow activities that are not provided for in the Data Sharing Agreement but would otherwise be consistent with the Act. The principle specifies that the data custodian and accredited user must consider the nature and intended uses of the outputs of the sharing and the requirements and procedures for use of the outputs. Furthermore, the outputs may contain only the data reasonably necessary to achieve the applicable data sharing purpose.

IIS understands that the outputs principle is concerned with what data or information would be created as a result of a data sharing arrangement and what would happen to it. Some outputs will remain in the hands of the Accredited Users because the user and Data Custodians have agreed (per the Data Sharing Agreement) that it would not be appropriate for it to be distributed to a wider audience.[60] Other outputs could form part of a publication, report or other public release. Where the outputs move outside of the closed data sharing environment, in accordance with a Data Sharing Agreement, release of outputs should not contravene any law of the Commonwealth or a State or Territory and be consistent with the Australian Government's Public Data Policy Statement 2015, particularly around open data.

Other elements of the DATB – such as the layers of defence outlined in in Section 3.3 – support and reinforce the outputs principle. The Data Sharing Agreement layer, for instance, allows Data Custodians to proscribe sharing of outputs or specify circumstances and conditions under which an output may be shared or released. The output principle is also strengthened by a data minimisation requirement (carried across from the data principle). This requirement would result in removal of personal information from an output, even if such information was needed for data processing or linkage, where such identifiers were not necessary for the output achieving its intended purpose.

While the range of protections is strong, any potential for misuse or negative privacy impacts in downstream uses – for example the use of outputs to inform algorithms or to build automatic decision-making systems – should be explicitly addressed. IIS suggests that management of output data in accordance with DATB requirements be addressed in the updated Guide or other guidance material.

6.11 Data Sharing Agreements

Data Sharing Agreements are the third of the three main requirements the DATB introduces to manage data sharing processes; the other two requirements being the data sharing purpose limitation and the Data Sharing Principles. Agreements are intended to enhance the Scheme's transparency

[60] Though outputs may exit the Scheme in accordance with the '*Exit from data sharing scheme'* clause – see discussion that follows.

and accountability measures – key features of a strong privacy framework. IIS finds the use of Data Sharing Agreements to be an important and necessary measure to ensure sharing arrangements between the parties are clear, to clarify the purpose of the sharing and to prevent unintended additional uses or disclosures. In doing so, agreements help manage function creep risks. Further, IIS supports publication of the Agreements which strengthens transparency of data sharing under the Scheme and allows data sharing to be subject to scrutiny.

The DATB lists the matters that a Data Sharing Agreements must address. These are mandatory terms and Data Scheme Entities must comply with these provisions or risk penalties and, perhaps more importantly, lose the legal authority for the data sharing activity. Data Sharing Agreements will also be listed in a publicly available NDC register.

Data Sharing Agreements will be negotiated between Data Custodians and Accredited Users. In summary, they are expected to cover:

- The parties to the agreement, and who is the Data Custodian
- What data is to be shared, the data or outputs created and if an ADSP is to be involved
- Any applicable law that otherwise prevent the data sharing
- The purposes for which the data is to be shared
- The application of the Data Sharing Principles, including which party is responsible
- Prohibition on using the data for any purposes other than the specified purposes for which it is shared
- Prohibitions on sharing and releasing output that is scheme data, except for specified exit mechanisms
- Allocation of data breach responsibilities
- The duration of the agreement, review intervals and circumstances in which might be varied or terminated
- What happens to data at the end of the agreement.

The Discussion Paper stated that Data Sharing Agreements were expected to be 'simple, streamlined and consistent'.[61] The Paper noted that the NDC would be addressing cost and resource implications associated with sharing data under these Agreements and would respond to requests to provide templates and guidance.

Certainly, guidance for Data Scheme Entities to explain and expand on the terms in the Data Sharing Agreements will be important. IIS sees a possible conflict between the desire for efficiency and simplicity and the ability of the Agreements to support transparency and accountability. It would be a poor outcome if attempts to streamline and simplify Data Sharing Agreements meant they were rendered overly generic or non-specific. Specifying the matters that Agreements must cover in the DATB helps to counteract that risk. Involvement of the NDC will also help get the balance right when setting expectations for the form and content

[61] Discussion Paper, p 36.

of Data Sharing Agreements. The effectiveness of Data Sharing Agreements directly correlates with the effectiveness of privacy protections associated with the Scheme. IIS therefore encourages the NDC to monitor the form and content of Data Sharing Agreements and intervene to ensure they comply with the requirements and spirit of the DATB.

7. Findings and recommendations – Regulatory framework and approach

In undertaking this PIA, key issues for IIS were whether the DATB can protect all personal information shared, including the most sensitive, and whether one or more parties to the data sharing is always accountable for the data. There should be no room for 'buck-passing' when things go wrong or individuals wish to complain. IIS finds that the DATB framework provides a good range of mechanisms here; however, we believe the NDC will need to take a proactive approach to make these work effectively in practice.

The integrity of the Data Sharing Scheme will only be as strong as the assurance mechanisms in place to monitor compliance and address problems. IIS finds that the DATB establishes robust oversight via the legislated role and functions of the NDC. Again, the regulatory framework and the way the NDC approach the oversight role and the investment in the office will be critical to securing a strong and effective regulatory approach.

The discussion below outlines the approach in the DATB and where IIS sees a need for specific focus in implementation.

7.1 The DATB regulatory framework – range of functions and powers

The DATB establishes robust oversight via the legislated role and functions of the NDC and the NDAC. Under the Bill, the NDC's functions include:

- Providing advice to the Minister, on request or their own initiative, about the operation of the Act, actions being taken by Data Scheme Entities to comply with the Act, and the need for administrative or legislative change
- Providing guidance on any aspect of the Data Sharing Scheme, as well as matters incidental to the Scheme, such as data release, data management and curation, and emerging technologies
- Promoting understanding and acceptance of best practice in sharing, and releasing, public sector data and safe data handling practices.
- Regulating the Data Sharing Scheme, including by accrediting Data Scheme Entities and enforcing obligations.

The DATB gives the NDC monitoring and investigative powers, along with a range of enforcement powers that include the ability to seek injunctions and civil penalties from a court, issue infringement notices and enter into enforceable undertakings. The Bill also provides for complaint handling, where Data Scheme Entities have concerns about each other. Individuals could still pursue privacy complaints via the Privacy Act or other equivalent privacy legislation.

The DATB also establishes a range of civil penalties and some criminal offences, which give strength to the expectation that data will only be shared where safe and will only be used as intended under the DATB. The following actions could give rise to civil or criminal penalties:

- Engaging in conduct such as sharing that purports to be authorised by the DATB but is not authorised, or collecting or using scheme data in an unauthorised manner
- Failing to comply with the mandatory terms of a Data Sharing Agreement
- Providing false or misleading information to another Data Scheme Entity when developing Data Sharing Agreements or to the NDC in compliance with the DATB
- Failing to comply with ongoing accreditation requirements.

The Discussion Paper also reported on stakeholder concerns that the DATB overrides secrecy and non-disclosure offences in other legislation. These were considered to have offences that were appropriate for the data in question and therefore were fit for purpose. The DATB responds to these concerns with 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 DATB authority falls away and the original offences and penalties will apply. This is called the 'rebound approach.' Data Sharing Agreements will point to the relevant legislation and rebound penalties so Data Custodians, Accredited Users and ADSPs are aware of the consequences if something goes wrong.[62]

In addition to the offences and penalties that will be available under the rebound approach, the DATB includes a few scheme-specific civil penalties and criminal offences (such as the ones listed above). This is to provide gap coverage where penalties available via the rebound approach under existing non-disclosure laws do not provide coverage or protection against misconduct.

IIS considers this set of functions, powers and obligations is consistent with similar frameworks; we have not identified any gaps. In relation to the NDC's function of providing advice to Minister, IIS believes that, particularly in the early implementation stages, this function should be used actively to identify problems or gaps and to identify aspects of the Scheme that are operating differently to what was envisaged.

7.1.1 National Data Advisory Council

The NDC is supported by the NDAC. An earlier draft of the DATB stated that the NDAC's function is 'advising the Commissioner on matters relating to sharing and use of public sector data,'[63] without any further elaboration on what those matters could be.

The NDAC will play a critical role in guiding the NDC on strategic matters. Those matters should include ensuring a balanced approach to privacy that foregrounds respect for individuals and rigor in personal information protection. The NDAC is in a position to monitor and advise on the privacy

[62] See the DATB, EM, Draft, July 2020, [12] and its discussion of breaches and penalties, [54]-[59] and [86]-[100].

[63] Draft DATB, cl 60. Note, clause numbers may have changed.

impacts of the Scheme as a whole and the accumulating privacy impact of data sharing under the Scheme. Without an explicit requirement for the NDAC to advise on privacy, there is a risk that privacy considerations are sidelined in strategic discussions about advancing data availability.

IIS understands that omission of specific matters that the NDAC is to advise on from the Bill was partly to avoid limiting the matters the Council may consider. The ONDC also pointed out that the Information Commissioner will be a standing member of the NDAC and will therefore be in a position to represent privacy interests in the Council. The Bill also allows the NDC to appoint other members and, technically, those appointees could include privacy advocates or representatives from civil society.

IIS believes drafting can address concerns about limiting the NDAC's operations. Notwithstanding the membership of the Information Commissioner, IIS recommends specifying that ethics, privacy and transparency are matters the NDAC is to advise on. In the absence of explicit mention of respect for privacy in the Bill's objects clause, these provisions will signal that personal information protection is being considered at a strategic level.

Recommendation 7 – Specify 'privacy' in the NDAC's advisory function

Rationale

The NDAC will play a critical role in guiding the NDC on strategic matters. Those matters should include ensuring a balanced approach to privacy that foregrounds respect for individuals and rigor in personal information protection. The NDAC is in a position to monitor and advise on the privacy impacts of the Scheme as a whole and the accumulating privacy impact of data sharing under the Scheme. Without an explicit requirement for the NDAC to advise on privacy, there is a risk that privacy considerations are sidelined in strategic discussions about advancing data availability.

IIS recommendation

Specify the matters that the NDAC is to advise on in the Bill. These should include: ethics, balancing data availability with privacy protection; and trust and transparency.

Update: The DATB now specifies the matters on which the NDAC may advise the NDC.[64] They include 'ethics', 'balancing data availability with privacy protection' and 'trust and transparency'. Therefore, IIS considers Recommendation 7 to have been addressed.

7.1.2 Penalty provisions

As noted, the DATB specifies a range of civil penalties and some criminal offence and allows the NDC to apply to a court for enforcement.

[64] DATB, cl 61.

IIS supports the inclusion of such penalties. They highlight the intent that the DATB will provide for safe data sharing and that poor practices will be punished. However, IIS notes that offence provisions in similar laws, including the Privacy Act, are used minimally.

The penalties also apply to Data Scheme Entities; entities will be subject to a penalty, not a responsible person. IIS also understands that consistent with standard practice, the Crown is not liable to criminal prosecution, though it may be subject to civil penalty. However, the shield of the Crown does not extend to government business enterprises, or to Commonwealth employees acting outside their lawful authority.[65] There are also a number of well-established circumstances in which company directors will be held personally liable for the actions of the company.

The DATB civil penalties are generally 300 penalty units. The DATB also offers criminal penalties including imprisonment. In addition, if the rebound penalties described above come into play, the penalties in the original legislation would apply.

The proposed statutory reviews in the DATB would be a vehicle for testing whether the range of penalties and offences provides the right protection for shared data.

7.2 The DATB regulatory framework – possible privacy impacts

This section considers aspects to the DATB's regulatory framework that might have a particular impact on privacy. The section draws on IIS's experience of the operation of similar provisions and on matters raised in submissions to the Discussion Paper and in IIS's consultations with stakeholders.

7.2.1 Potential impact of legislative instrument making powers in the DATB

The DATB takes the form of principle-based law. It provides a high-level outline of the framework, and leaves other aspects to be filled in by other mechanisms. These include legislative instruments of the following kind:

- **Regulations** made by Governor General to limit a Data Scheme Entity's participation in the Scheme.
- **Rules** made by the Minister to set:
  - The requirements for the accreditation framework
  - The parameters of the Scheme (for example, rules may prescribe additional precluded purposes, requirements to be included in Data Sharing Agreements, other circumstances that allow data to exit the Scheme, or prescribe high-risk data integration services that may only be performed by an ADSP)

[65] The Bill states that conduct engaged in on behalf of an entity (that is a Commonwealth body) by an employee acting within the scope of their employment or authority is taken to have been engaged in by the entity, for the purpose of penalty and offence provisions. However, penalty and offence provisions will not apply to the entity if it can establish that it took reasonable precautions and exercised due diligence to avoid the conduct by the employee.

- Any other functions to be conferred on the NDC

- **Data codes** made by the NDC to prescribe how entities must apply the Scheme.

These are all disallowable legislative instruments, meaning they will be transparent and subject to Parliamentary oversight. The DATB, and its regulations and rules, would set additional limitations and requirements for the Data Sharing Scheme. Data codes, on the other hand, would set out how different parts of the Bill must be applied in practice.

IIS was asked to consider 'the potential privacy impacts of regulation-making powers in the DATB'. Regulations can undermine privacy in that, although disallowable instruments and subject to Parliamentary scrutiny, they can radically change and increase access to personal information.

The DATB appears to avoid this risk in that none of the legislative instrument making powers allow for expansions to the Scheme or to the amount of data shared under the Scheme. The ONDC told IIS that this was a deliberate drafting decision. In practice, this means that rules can restrict the Scheme (by prescribing additional precluded purposes, for example) but not expand it.

While it is difficult to say how the use of regulations will play out in practice, the DATB provisions do not raise immediate concerns. IIS also notes that the usual consultation processes will apply to the making of legislative instruments (such as regulations) under the Bill. This would include consulting the Australian Information Commissioner about matters affecting privacy. The ONDC also advises that it is releasing the draft Regulations and a Discussion Paper on the Accreditation Framework with the Exposure Draft of the Bill. It also intends to provide a draft of the Regulations and the Accreditation Rules to the Parliamentary Scrutiny committees when they consider the Bill so they can consider these at that time.

7.2.2 Protection of sensitive information

The Discussion Paper notes that questions about possible additional protections for sensitive information came up in several contexts in submissions and consultations. The Discussion Paper states that legislative safeguards will protect all sensitive information and require that it is handled appropriately and consistently. The ONDC also noted that the DATB would allow for data covered by specified legislative provisions to be excluded by regulations as appropriate. The approach will be to exclude data based on legislation it was collected under or other similar factors, rather than the nature of the data itself.

The draft Data Availability and Transparency Regulations 2020 set out secrecy and non-disclosure provisions that will complement the provisions of the Bill and ensure that specified agencies and certain types of very sensitive data are outside the scope of the Bill. The Explanatory Statement to the Regulations notes that:

> These Acts and provisions were identified by Australian Government stakeholders as strictly necessary to be exempt from the scheme to protect the national interest, maintain the integrity of the judicial system and protect public trust in the Government's handling of personal information.

In addition to the exclusion of national security and law enforcement activities, considered in Section 6.1.3 and Section 6.1.4 above, other data or activities initially excluded under the Regulations include:

- The Commonwealth Electoral Roll
- Child protection
- Agencies with an integrity or oversight function
- Royal Commissions
- The COVIDSafe App
- My Health Records.

The question of whether additional regulations are needed with regard to sensitive information is one that could be revisited when the Scheme is reviewed following implementation. The review may consider whether sensitive information has been handled appropriately and whether or not the community feels listened to in relation to information that is considered sensitive. IIS agrees with the ONDC that, while it will be reasonable and necessary for data to be excluded from sharing based on its nature, this is likely to occur via other mechanisms, such as when applying the public interest requirement or deciding the 'reasonableness' of seeking consent. The NDC should ensure guidance material reflects these considerations.

7.2.3 Outputs exiting the scheme

The DATB provides for a limited and controlled 'exit' arrangement so that data outputs may be shared by the Accredited User in a way that removes the output from the Scheme (and therefore means it is no longer subject to the DATB). The aim is to allow for uses that are consistent with the objects of the DATB, and that, unless involving aggregated data, would be for the benefit of the entity or individual concerned, but which would otherwise be prevented by the DATB's construction.

Two main situations where exit from the Scheme is contemplated:

- *Validated output exit*
  The output is shared with an entity or individual to which the output relates, for the purpose of validating or correcting the output. The intent is to support government service delivery that depends on accurate and up-to-date information (such as pre-filling forms and providing a single point-of-contact for individuals to engage with multiple government agencies). Under this clause personal information may only exit the scheme with a positive act of validation or correction by the individual concerned.
- *Released output exit*
  The output is released in a way that is specified in the Data Sharing Agreement and does not contravene any Commonwealth, State or Territory law. The intent is to facilitate the release of outputs such as highly aggregated research outputs.

The OAIC has raised concerns about the DATB's exit provisions, which it notes is a 'significant change to the framework that has previously been consulted.'[66] While acknowledging the need for outputs to exit the scheme in certain circumstances, the OAIC recommended additional protections, including:[67]

- The output permitted to exit the scheme for validation or correction should be limited for the purpose of delivery of government services
- The output that is released under a Data Sharing Agreement (likely for sharing research or policy outcomes) should not be permitted to include personal information.

The OAIC raises important points in relation to privacy risks and suggests workable solutions that IIS would support. It is vital that the DATB's exit provisions not operate permissively contrary to the narrower intentions of the Bill. In IIS's view, personal information should rarely if ever exit the Scheme via the avenue of 'released output exit'.

Existing measures in the Bill offset many of the privacy risks before this point of exit. This includes purpose limitation and data minimisation, including at the output stage, along with the restrictions imposed by the Data Sharing Agreement. In practice, this should preclude both the inclusion of personal information in a released output and its exit in most circumstances, while leaving open the possibility of its exit in appropriate circumstances (e.g., where individuals have consented).

While IIS will not make a formal recommendation here, we agree with the OAIC that there should be guidance to Data Scheme Entities to explain what is permitted under the exit provisions, where the authorisations under the Scheme end and what protections apply once the outputs have exited the system. This matter could also be considered in the first statutory review.

7.2.4 Data sharing involving overseas bodies

The DATB allows for the involvement of foreign entities. The accreditation framework may prescribe 'the kinds of entities that may be accredited under the Scheme (including foreign entities)'. The DATB also provides for extraterritorial application where an activity occurs wholly or partially outside Australia and the conduct has an Australian link (e.g. conduct was undertaken by a Commonwealth body, an Australian citizen, a trust created in Australia, a partnership formed in Australia, etc.).

The issue from a privacy perspective is whether individuals would find it easy to seek redress where data sharing involved a foreign entity.

The DATB deals with this potential risk with a number of layers of protection, which include that:

- Foreign entities must be accredited before they can participate

[66] See the submission of the OAIC to the DATB exposure draft, [28], available at <https://www.datacommissioner.gov.au/exposure-draft/submissions>.

[67] Id, [31].

- All other aspects of the Data Sharing Scheme – including its obligations and penalties – would apply, including the requirement to maintain privacy coverage. This includes the obligations in APP 8. Entities are required to take reasonable steps to make sure the overseas recipient will not breach the APPs and, unless other protections apply, are accountable if the overseas entity breaches the APPs.
- The Data Custodian is 'deemed' to hold the data for the purposes of the Privacy Act's Part IIIC (notification of eligible data breaches).

IIS considers this approach should minimise the risk that individuals would find it more difficult to seek redress for a breach of privacy. However, IIS also notes that many Australians are uncomfortable having personal information shared overseas.[68]

The extent of data sharing involving personal information and overseas entities will be an issue to monitor as the Data Sharing Scheme is implemented. Additional steps might be needed to maintain community confidence in data sharing.

7.3 Interoperability of the DATB with other existing legislation

As emphasised at other points in this PIA, the design approach for the DATB is to aim for strong protections that work alongside but do not overlap with other relevant law, including the Privacy Act.

The DATB aims to reflect the fact that the Privacy Act covers the field for privacy law and to avoid overlaps. It does seek to reinforce privacy law obligations; Data Scheme Entities must maintain privacy law coverage.

The DATB also recognises the potential for the NDC to receive complaints, including privacy complaints from individuals, or to become aware of other matters that would be better handled by another regulator. The NDC can receive or provide information to specified regulators, including privacy regulators, and can transfer or receive matters. IIS understands that these powers should also allow the NDC to, for example, participate in joint investigations.

This suite of powers should support the ability of privacy regulators to work together and to prevent privacy issues, or individuals' privacy concerns, from falling through gaps.

The powers would need to be supported, particularly in the early stages of implementation of the Data Sharing Scheme, by close cooperation. This is especially so between the NDC and the OAIC but also between privacy regulators in all jurisdictions. The Discussion Paper flags this as an important strategy and IIS understands from the ONDC that this is already a feature of the implementation approach.

The NDC should monitor the regulatory landscape associated with the Data Sharing Scheme for gaps or overlaps in regulatory oversight. For example, the ONDC has indicated that aspects of Data Sharing Agreements would be regulated by the OAIC. This will necessarily require close cooperation

[68] OAIC, *Australian Community Attitudes to Privacy Survey 2017*, available at <https://www.oaic.gov.au/updates/videos/australian-community-attitudes-to-privacy-survey-2017/>.

between the NDC and the OAIC. Communication about issues, and discussion about risks and priority areas for attention, will be needed to ensure the Data Sharing Scheme works well alongside the Privacy Act. This matter could also be considered in the first statutory review.

IIS acknowledges the close working relationship the OAIC and the ONDC have had to date and encourages ongoing cooperation.

7.4 Approach to implementation

7.4.1 Regulatory approach/posture of the NDC

A theme in IIS's risk assessment as outlined so far in this report is that implementation will be critical to ensuring privacy impacts of the Data Sharing Scheme are minimised. In IIS's experience the effectiveness in any regulation implementation comes down to regulatory stance. This will be affected by factors such as:

- **The legislative framework** – which is discussed in detail in this report, and which is potentially strong but equally open to interpretation and therefore in need of clear guidance and strong oversight
- **The expectations on the regulator** – from the community, government, and other stakeholders, in this case Data Custodians and Accredited Users. The expectations for the NDC will become clearer over time. At least the community is likely to expect a proactive regulator from the start
- **The resources available to the regulator** – these are still to be established. As discussed at Section 7.4.2, the Data Sharing Scheme is likely to need considerable resources particularly in the early implementation phases when it will be developing guidance and accrediting Data Scheme Entities.

The DATB is meant to be enabling and encouraging safe data sharing to promote innovation and efficiency. The open, principles-based nature of the DATB is designed with these objectives in mind. The regulatory stance will need to be consistent with these objectives. It will need to find the balance between giving clear and consistent riding instructions, including to ensure privacy is considered and protected, and avoiding over-prescription.

In IIS's view this calls for a strong focus on developing guidance and importantly keeping a very close eye on things and if there are problems emerging, fixing them. The evolutionary nature of the Data Sharing Scheme adds to the importance of ongoing thinking and risk assessment and management.

The Discussion Paper indicates the NDC's regulatory approach will be to use the 'Regulatory Pyramid'.[69] In general IIS supports this approach. It is consistent with its view that the NDC's early focus should be particularly on education and guidance. However, the approach also needs to take account of the fact that the Data Sharing Scheme could evolve rapidly, could involve extensive amounts of data being shared, and new players and multiple jurisdictions. The NDC will need an

[69] Discussion Paper, p 50.

oversight, compliance and enforcement strategy that takes account of these factors as well as the potential for Data Scheme Entities to include new players that may be under-equipped on privacy and security considerations.

IIS understands the NDC will be developing a detailed strategy on how the regulatory powers will be used. IIS considers there would be value in this, and in making the strategy available publicly.

7.4.2 A properly resourced and independent regulator

The discussion above highlights the importance of adequate resourcing for the NDC and the risks to community confidence if the resourcing is not adequate. There will be unknown factors in assessing resourcing needs, such as the actual size of the data sharing ecosystem and how much data sharing actually occurs.

Data will be shared in a controlled way, not released into the wild, and IIS understands the ecosystem would be finite, perhaps in the order of 1000-2000 participants. However, as noted the Data Sharing Scheme does give the NDC roles and responsibilities that are resource-intensive, in particular the accreditation of Data Scheme Entities. IIS has also flagged throughout this PIA both the range of guidance material that will be needed, and the role that NDC oversight will have on confidence in the Scheme.

Equally critical to regulator resourcing levels to community confidence, is the need for the regulator to be, and be perceived to be, able to act independently. Former Privacy Commissioner, Malcolm Crompton, noted that 'A regulator will have a wider scope to act independently and without fear where its governing law has provisions that restrict the conditions under which the regulator can be removed and limit the extent to which external parties can direct its activities'.[70]

Under the Bill, the NDC will be an independent statutory officer appointed by the Governor General and not subject to the direction of the Minister. IIS understands that the NDC will be supported by staff allocated by the Secretary of the Department responsible for the Bill. This is currently PM&C.

In recognition of the NDC's important role and some of the possible downsides of the staff and governance model, the Bill contains provisions which are intended to ensure the NDC is able to operate independently, avoid actual or perceived conflicts of interests, and has adequate resources.

The relevant provisions in the Bill deal with:

- Staffing – The Secretary must make adequate staff available to meet the NDC's needs, both in terms of numbers and abilities. It will be up to the NDC to determine the necessary skills, experience and/or qualifications that staff must have.

[70] *'Light Touch' or 'Soft Touch' – Reflections of a Regulator Implementing a New Privacy Regime*, delivered at National Institute of Governance – Canberra and Committee for Economic Development of Australia – Melbourne (March 2004), available at <https://webarchive.nla.gov.au/awa/20101011223836/http://pandora.nla.gov.au/pan/64350/20101012-0000/www.privacy.gov.au/materials/types/speeches/view/6354.html>

- The delegation framework – This reserves some decisions for the NDC only. For example, the NDC must make codes, guidelines and directions. Staff and contractors may assist in the preparation of instruments and documents. In addition, the NDC cannot delegate their functions and powers with respect to regulating the Department or its portfolio agencies. This aims to avoid conflicts of interest that would arise, for example, if Departmental staff were to make accreditation decisions that affect the Department. The NDC can engage contractors (instead of Departmental staff) to assist with regulating the Department and its portfolio agencies.
- Exclusion of the NDC or their staff from participating in the Data Sharing Scheme.
- Transparency – The NDC's annual report must contain information about the number of APS employees made available, and a report on financial matters, including discussion and analysis of the financial resources made available in the financial year and how they were used.

The NDC's role is a strong element of the privacy protections in the Data Sharing Scheme and IIS welcomes the measures that go to ensuring the independence of the role.

IIS has some reservations about the fact that the Data Sharing Scheme will be implemented by the NDC as an office within the PM&C, rather than a separate entity, and that the NDC's staff will be allocated by the Secretary of the PM&C. While there is no intrinsic reason why such a model will not work well, experience has shown it does not always work in practice. Where an office holder does not have full control of their budget or staff, there is potential for conflicts or situations to arise that can impede their ability to do the job. Additionally, there is at least potential for the NDC to have, or be perceived to have, less standing or autonomy because of its location. IIS considers adequacy of resourcing to be an important consideration in the first statutory review of the DATB (see **Recommendation 8**).

7.4.3 Dual role of the NDC as advocate and regulator

The NDC will be the regulator of the Data Sharing Scheme but, under clause 42(1)(d), it will also have the function of advocating for data sharing – specifically by promoting understanding and acceptance of the benefits of sharing and releasing public sector data. The NDC additionally has the function of promoting understanding and acceptance of safe data handling practices.

Stakeholders have raised concerns about whether this advocacy role may affect the independence and impartiality of the NDC in relation to its regulatory and enforcement functions.[71] This is relevant to this PIA as some of those regulatory functions will necessarily involve enforcing safeguards in the Bill that protect privacy or curtail data sharing. It is conceivable that a conflict could arise between the NDC's regulatory functions and its function of advocating for data sharing and release.

[71] See the submissions of the Information Privacy Commission NSW, ElevenM, Office of the Victorian Information Commissioner, Electronic Frontiers Australia, Australian Privacy Foundation, Dr. Lynda Crowley and Ms. Carole Caple (Supplementary submission), and Australian Medical Association to the DATB exposure draft, available at <https://www.datacommissioner.gov.au/exposure-draft/submissions>.

It was pointed out to IIS that other regulators operate under a similar model – including the OAIC which has functions under privacy and FOI law. While it is true that the Information Commissioner has the function of promoting awareness, understanding and acceptance of privacy and FOI law, the OAIC's enabling legislation stops short of including advocacy functions. IIS recommends that this issue be considered in the first statutory review of the DATB to check that the NDC's advocacy functions are not unduly influencing its regulatory functions.

Recommendation 8 – Review effectiveness of the NDC support, staffing and operating model in first statutory review of the Act

Rationale

The NDC's ability to carry out its role in the Data Sharing Scheme will depend in part on the level and nature of resources available to them. In particular, the NDC plays an important role in monitoring compliance with the Scheme and complaint handling – privacy protections embedded in the DATB will only be as strong as the enforcement, oversight and assurance measures in place. There is also an open question as to how the NDC will perform the dual role of being an advocate for data sharing and a regulator enforcing compliance. The effectiveness of the NDC's independence, level of resourcing and performance of its dual advocate/regulator role should be subject to early review.

IIS recommendation

Review effectiveness of the NDC support and staffing model and the performance of its functions 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 its statutory functions, including monitoring compliance with the Scheme and investigating complaints.

7.4.4 Regulatory action plan including monitoring and compliance strategy

IIS sees the NDC's oversight and monitoring role as the bedrock for effective implementation of the Data Sharing Scheme as it relates to privacy. We have made suggestions in this report both for areas which we consider should be given particular attention in guidance (see Appendix D) and monitoring, as well as factors that should be taken into account in developing a regulatory action plan (including a monitoring and compliance strategy).

The NDC will be facing a complex regulatory environment. The legislation will be new and there is likely to be strong interest in how it will work and what is expected. There will also be an unknown number of players, who might or might not have strong privacy and security expertise. In addition, because of the close connection with the privacy jurisdictions and at the same time the wish to avoid overlaps, the strategy will need to consider how the schemes and the regulators should interact.

In addition, IIS strongly urges the NDC to make sure they can quickly become aware of any system issues or failures and can deal with them quickly and transparently. It is beyond doubt that there will be failures and also that the better failures are handled, the better will be the community reaction.

Recommendation 9 – Develop and publish a regulatory action plan

Rationale

The NDC's oversight and monitoring role will be crucial to the effective implementation of the Data Sharing Scheme as it relates to privacy. It will be operating in a fast-moving regulatory and technological environment. Having a well thought-out and publicly-available regulatory action plan helps to facilitate, and signal the importance of, the NDC's oversight and monitoring role.

IIS recommendation

Develop and publish a regulatory action plan that specifies the NDC's approach to oversight and the use of their enforcement powers. The plan should cover matters such as:

- 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.

8. Findings and recommendations – Safety net for individuals

IIS's view is that the DATB framework is strong and provides layers of defence, which should work together to identify and manage privacy risks associated with any data sharing project.

IIS also recognises that the DATB will not supplant privacy laws. The ONDC has designed the Bill to preserve the OAIC's regulatory remit to the extent possible. The ONDC advises it would not be appropriate for the NDC to address complaints and issues involving the handling of personal information.

Where issues do arise for individuals, whether affecting them alone, or because there is a data breach involving potentially many people, they would generally need to go through the usual channels. That is, the first step is to approach the agency involved and then, if the matter is not resolved, the OAIC.

That said, individuals who become aware of something going wrong with shared data, for example, mishandling by an Accredited User, might well approach the NDC. The ONDC has indicated that there would be 'no wrong door'. It would assist the individuals, including by referring matters to the relevant regulator.

While often these processes will resolve issues, data sharing will take place in a complex system and individuals should not need to understand the system to have any issue resolved. In addition, the diffuse accountability in the Data Sharing Scheme should not result in harm to individuals not being remediated because each party points at the other parties. Part of the ecosystem governance that the NDC is established to provide (along with the OAIC) must be to ensure remediation happens.

IIS emphasises here that it is not saying that the NDC has to provide the mechanisms (although it could). Rather it should make sure they are in place and working.

IIS also considers that the NDC should monitor, and report on, the way in which individuals are interacting with the Scheme. This could include gathering information about complaints and enquiries to it and to the OAIC.

Recommendation 10 – Individuals to have access to simple arrangements for addressing privacy complaints and issues

Rationale

Data sharing will be taking place in a complex system, involving parties that may not be previously known to individuals. As the entity responsible for ecosystem governance, the NDC should work with the OAIC should ensure that individuals have easy access to a mechanism for dealing with privacy complaints, queries and issues without being passed around or getting lost in the system.

IIS recommendation

Work with the OAIC and other privacy regulators to ensure:

- 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).

Recommendation 11 – Measure and report on individuals' interaction with the scheme

Rationale

As the Data Sharing Scheme exists to benefit the community, the NDC, in consultation with the OAIC, should monitor how individuals are being affected from a privacy standpoint. Measuring individuals' interactions with the scheme – for example, number and nature of privacy complaints – will allow the NDC to address the scheme's shortcomings and make continuous improvements.

IIS recommendation

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:

- 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).

9. Findings and recommendations – Transparency

Transparency measures are included in the APPs to help ensure individuals have as much control as possible over information about themselves.[72]

The Productivity Commission and the ONDC (and the PM&C) processes have also recognised the value of transparency in building and supporting community acceptance of data sharing of public sector data. The name change from the Data Sharing and Release Bill to the 'Data Availability and Transparency Bill' is significant in this regard. It not only emphasises that the Data Sharing Scheme will occur within a controlled environment, with release being a separate, and separately regulated matter; it also emphasises the DATB's intention, included in its objects, to enhance integrity and transparency in sharing public sector data.

IIS understands that the transparency objective is partly about helping potential Accredited Users understand the nature of data available. However, it is also about and should assist individuals and the community understand how data is being used and handled in the system.

There are a range of measures included in the DATB to promote transparency. These include:

- The NDC to maintain publicly available registers of Accredited Entities and the mandatory terms in Data Sharing Agreements[73]
- The NDC's function to report to the Minister, on own their initiative or at the Minister's request, on operation of the Act scheme or the need for legislative or administrative action
- The NDC to report annually on the Act, addressing matter specified including the number of requests for public sector data, the number of Data Sharing Agreements made, regulatory actions taken, including assisting Data Scheme Entities with compliance, and the staffing and resources available to it and how they are used
- Empowering the Minister, rather than the NDC, to make rules relating to the accreditation process.

IIS supports these measures. We have also made other recommendations that go to transparency. These include suggesting that the NDC should develop and publish information about their proposed enforcement approach and their compliance and monitoring strategy. IIS also considers that there are issues to which the NDC needs to give particular attention to ensure the community is aware of the ways in which public sector data is being shared and used. These include the nature of commercial activities and the involvement of foreign entities.

[72] In particular, APP 1 (open and transparent management of personal information) requires APP entities to prepare and make available a privacy policy, and APP 5 (notification of collection of personal information) require APP entities to take reasonable steps to tell individuals at the point of collection, about matters including why the information is needed and to whom it might be disclosed.

[73] The mandatory terms are outlined in the draft DATB.

In the sections below, IIS identifies two areas which we consider would also support the transparency objectives.

9.1 Review of the Act

The DATB provides for periodic reviews of the Act, the first no later than three years after commencement and subsequent reviews no later than every ten years after commencement.

The ONDC notes that this is likely to mean there would be two reviews within the first 10 years (the second review is counted from commencement of the Act, not from the date of the last review).

For a piece of law with such potential to impact on the amount of information about individuals that is shared for new purposes, the number of parties that could be involved in data sharing and given the rapidly changing nature of the technological and social environment in which data sharing will occurs, IIS considers the review periods (seven years after the initial review, and every ten years thereafter) to potentially be too infrequent. While the risk of obsolescence is reduced due to the DATB's principles-based approach and the NDC's ability to make codes and issue guidelines, there is nevertheless the possibility that the Act's privacy protections will no longer be fit-for-purpose and require updating within the span of 10 years.

Given the dynamic environment that the Data Sharing Scheme will operate in, IIS considers that there should be scope for allowing the DATB to be reviewed within a shorter period. IIS also considers that the first statutory review should start early, to ensure that relevant data to inform the review will be available.

Recommendation 12 – Allow for shortening the period for review of the Act and make reviews public

Rationale

The draft DATB proposes that the Act is to be reviewed no later than every ten years after commencement, with an initial review three years after commencement. The regular ten-year review interval is very long considering the dynamic technological and social environment in which data sharing will occur.

IIS recommendation

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.

Subsequent reviews should formally consider whether the next review should occur sooner than ten years, taking into account:

- How the Scheme is operating in practice, including any privacy impacts of concern
- The changing technology landscape

Recommendation 12 – Allow for shortening the period for review of the Act and make reviews public

- Amendments to the Act, especially those that significantly expand the Scheme or otherwise have the potential to impact privacy.

The reviews of the Act and the government responses should be made public.

9.2 Public awareness raising

As noted, transparency is a central element of individual choice and control over their personal information and the Privacy Act has specific measures in this regard (in particular in APP 1 and APP 5). In the lead up to the DATB introduction, the ONDC is working with the OAIC to ensure privacy notices cover data sharing matters. While this is an important measure, privacy notices, as discussed in Section 6.5.1, have limitations as far as transparency measures go. In any event, even where effective, privacy notices will only reach individuals whose information is collected, rather than the community at large.

IIS considers that the NDC should continue to raise awareness about the Data Sharing Scheme with individuals and the community, including via a public awareness raising campaign and plain English explanatory material. The campaign should be operational in time for the launch of the Data Sharing Scheme.

Recommendation 13 – Conduct public awareness campaign about the Data Sharing Scheme

Rationale

The Data Sharing Scheme is a very significant change to the way data sharing will occur in Australia. With any initiative that touches on the (potential) sharing of personal information, it is important to build social licence and trust among the community. Public awareness to promote the scheme and allay concerns should occur well before it enters into operation.

IIS recommendation

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:

- 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.

10. Appendix A – ONDC response to the PIA Recommendations

The Department of the Prime Minister and Cabinet (PM&C, or 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 Data Availability and Transparency Bill (the Bill), as introduced to Parliament on 9 December 2020. The PIA and these responses are draft, to allow for update if the Bill is changed following further consultation and review. Recommendations that have already been addressed are highlighted green.

IIS Recommendation	PM&C Response
Recommendation A: NDC to be given more scope for action in the accreditation process for non-corporate Commonwealth bodies. Amend the Bill to: • Enable the NDC to seek evidence from a non-corporate Commonwealth body to support their application for accreditation • Enable the NDC to refuse to accredit a non-corporate Commonwealth body when there are sufficient grounds for doing so	
PM&C Comment:	
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. 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.	**Agree**
PM&C Comment: The Department agrees and notes that the proposed accreditation framework is being developed in consultation with the OAIC.	
Recommendation 2: Ensure that accreditation involves regular assurance that standards are being met. 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.	**Agree**
PM&C Comment: 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.	
Recommendation 3: Draft DAT Bill to effectively exclude sharing for 'compliance and assurance' purposes 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.	**Agree**

PM&C Comment: 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.	
Recommendation 4: Articulate meaning of permitted purposes in Explanatory Memorandum (EM). 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.	**Agree**
PM&C Comment: The Department agrees and confirms it has included description of the permitted and precluded purposes in the draft EM.	
Recommendation 5: Provide guidance on the ethics process in appropriate circumstances. 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: • 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**
PM&C Comment: The Department agrees and will develop guidance to provide advice on ethics.	
Recommendation 6: Provide guidance on how consent operates in the data sharing scheme. Specify, in the EM, guidelines and other guidance material, matters such as: • 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**
PM&C Comment: The Department agrees and will develop guidance on how consent operates in the data sharing scheme.	
Recommendation 7: Specify 'privacy' in the National Data Advisory Council's (NDAC's) advisory functions. Specify the matters that NDAC is to advise on in the Bill, including: ethics; balancing data availability with privacy protection; and trust and transparency.	**Agree**
PM&C Comment: 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.	
Recommendation 8: Review effectiveness of the National Data Commissioner (NDC) support, staffing and operating model in first statutory review of the Act Review effectiveness of the NDC support and staffing model and the performance of its functions 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.	**Agree in principle**
PM&C Comment: 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.	
Recommendation 9: Develop and publish a regulatory action plan.	**Agree**

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: • 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.	
PM&C Comment: 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.	
Recommendation 10: Individuals to have access to simple arrangements for addressing privacy complaints and issues Work with the OAIC and other privacy regulators to ensure: • 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).	**Agree**
PM&C Comment: 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.	
Recommendation 11: Measure and report on individuals' interaction with the scheme. 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: • 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).	**Agree in principle**
PM&C Comment: 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.	
Recommendation 12: Allow for shortening the period for review of the Act and make reviews public. 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. Subsequent reviews should formally consider whether the next review should occur sooner than 10 years, taking into account: • 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.	**Agree in principle**

The reviews of the Act and the government responses should be made public.	
PM&C Comment: 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.	
Recommendation 13: Conduct public awareness campaign about the data sharing scheme. 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: • 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.	**Agree**
PM&C Comment: 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.	

11. Appendix B – Scope and methodology

11.1 PIA scope and assumptions

11.1.1 Scope

IIS was engaged to provide a systematic assessment of the DATB, which would identify the impact that the DATB might have on the privacy of individuals, and to make recommendations for managing, minimising or eliminating that impact. IIS was asked to consider:

- Whether the DAT legislative framework is compliant with privacy laws, and reflects community values around privacy and personal information in the project design
- Whether the DATB's adoption of the purpose test, the Data Sharing Principles and an implicit public interest consideration is reasonable, necessary and proportionate in the current policy context
- Likely community opinion
- Changes to the proposed DATB, including its scope, since the June 2019 PIA and public consultations
- The potential privacy impacts of regulation-making powers in the DATB
- The privacy-by-design approach the ONDC has used in developing the DATB, and the effectiveness of using this as a process to build public trust in the DAT framework
- The DATB's privacy coverage model, particularly in relation to breaches
- The human rights aspects of the DATB
- The DATB's approach to consent
- Whether sharing of government-held personal information under the purpose test and safeguards which may lead to commercial applications raises additional privacy impacts
- The interoperability of the primary DATB with the proposed delegated legislation, and the appropriateness of this division of matters as it relates to privacy
- The interoperability of the DATB with other existing legislation, such as the Privacy Act, and any other areas of regulatory overlap and interaction.

It was out of scope for the PIA to consider any review of the Privacy Act, the Consumer Data Right, the ACCC's Digital platforms inquiry, or reviewing Commonwealth legislative secrecy provisions, or other elements of any existing Commonwealth legislation.

11.1.2 Agreed assumptions and qualifications

- The PIA has focused on areas of the proposed DATB subject to privacy impacts; IIS has not undertaken an exhaustive review of all provisions of the DATB.
- The PIA does not provide legal advice; rather it provides strategic privacy and security advice.

11.2 Methodology

IIS took a consultative, practical and strategic approach to the consultancy and worked closely with the relevant staff of the ONDC at all stages. In planning and undertaking the PIA, IIS drew on the OAIC Guide to undertaking privacy impact assessments and its own depth of experience in conducting PIAs, as well as, its extensive experience of privacy regulation and what makes an effective regulatory framework to identify privacy issues and possible solutions.

The PIA involved the following stages.

11.2.1 Planning

IIS finalised the methodology and work plan in consultation with the ONDC during the kick-off meeting. Key inputs from this phase were the legislation and documentation that IIS had to take into account as well as the consultation preferred process and key targeted stakeholders.

In addition, the key outputs were the confirmation of the key project phases, milestones, and dates

11.2.2 Information gathering and internal meetings with the ONDC

The main objective of this stage of the PIA was to ensure that IIS had a sufficient understanding of the proposed DATB and the related context to inform the PIA drafting and any consultation processes.

As such, IIS reviewed the documents reflected on table below in order to proceed with consultations and meetings with the ONDC and in its analysis for the PIA.

List of documentation reviewed

ONDC
1. ONDC summary of consultation feedback (September – October 2019)
2. Data Availability and Transparency Bill, January 2020
3. Data Availability and Transparency Bill, August 2020
4. Data Availability and Transparency Bill, December 2020
5. Explanatory Memorandum, December 2020
6. Explanatory Memorandum, Draft, July 2020
7. Data Availability and Transparency Regulations 2020
8. DAT Regulation 2020 Explanatory Statement, APS referral draft v11
9. The Department of the Prime Minister and Cabinet, Australian Government Data Sharing and Release Legislative Reforms Discussion Paper, September 2019
10. Presentation: Data Sharing and Release Legislative Reforms, Office of the National Data Commissioner, Department of the Prime Minister and Cabinet, Public Consultation, October 2019

Other
11. The Department of the Prime Minister and Cabinet *New Australian Government Data Sharing and Release Legislation Issues Paper for Consultation* July 2018
12. Productivity Commission's Data Availability and Use Inquiry Report (in particular, section related to community attitudes)
13. Galexia Privacy Impact Assessment on the Proposed Data Sharing and Release (DS&R) Bill and Related Regulatory Framework (June 2019 PIA)
14. Office of the Australian Information Commissioner's (OAIC) Guide to Undertaking Privacy Impact Assessments (May 2014)
15. The Department of the Prime Minister and Cabinet *Best Practice Guide to Applying Data Sharing Principles* (March 2019)
16. Office of the Australian Information Commissioner *Australian Privacy Principle Guidelines* Combined 2019

Submissions to the ONDC Discussion Paper
The submissions to the Data Sharing and Release Legislative Reforms Discussion Paper are available from the ONDC website here submissions. IIS undertook a high-level review of all submissions to assist it to identify issues for this PIA. It reviewed the following submissions in detail to help focus its consultations with these groups. ● Australian Bureau of Statistics ● Australian Privacy Foundation ● Office of the Australian Information Commissioner ● Office of the Victorian Information Commissioner ● Office of the Information Commissioner, Queensland

11.2.3 Meetings and Key project Milestones

IIS held a series of meetings with ONDC staff to clarify its understanding or to gain input to support the different version of report drafts.

Meeting	Date - FY 2020
1. Kick-off Meeting	9 January
2. Information gathering	17 January
3. First draft report issued – meeting	6 February
4. Second draft report issued – meeting	17 February
5. Third draft report issued – meeting	20 February

Meeting	Date - FY 2020
6. Kick-off meeting – revising PIA to take account of Bill changes	12 August
7. Information gathering	18 August

11.2.4 Stakeholder consultation for IIS PIA

IIS conducted a targeted consultation with stakeholders to identify areas where impacts on privacy can be addressed, minimised, and/or mitigated. It was aimed at surfacing solutions and testing preliminary recommendations. The consultation took place in February in parallel with preparation of the second, third drafts of the PIA report.

The following organisations participated in consultation meetings, and/or provided written comments.

Consultation date	Participants
11 February	NSW Information and Privacy Commission
	Office of Australian information Commissioner
	Office of the Victorian Information Commissioner
	State Records of South Australia
	The Office of the Information Commissioner (WA)
12 February	Consumers Health Forum of Australia
17 February	Consumer Research Policy Centre
	Electronic Frontiers Australia (EFA)

A summary of the matters raised by stakeholders is at Section 4.

11.2.5 Analysis

The objective of this phase was to hone in as quickly as possible on issues where there was still a need to clarify approaches, to make any modifications to the draft DATB or to take other steps to mitigate privacy impacts.

The steps taken during the analysis phase included:

- Developing a good working understanding of the draft DATB, and the other relevant material including the Discussion Paper, submissions to the Discussion Paper and the June 2019 PIA.

- Identifying positive privacy impacts as well as privacy risks, taking account of the responses in the draft DATB to issues raised in submissions.
- Considering relevant provisions of the draft DATB, and the Privacy Act and broader issues including possible risks to individuals not yet considered and possible community trust or social licence issues.

11.2.6 Preparation of draft and final PIA report

Following its analysis, IIS developed its draft report and provided this to the ONDC. IIS then finalised the report taking account of the ONDC's feedback.

12. Appendix C – Background to the DATB and Data Sharing Scheme participants

12.1 Background to the Bill

The ONDC has consulted widely during the development of the Bill and will continue to consult stakeholders during 2020. Key dates in the evolution of the DATB include:

- March 2017 – Productivity Commission report recommends reforms to public sector data system
- 1 May 2018 – Government responded to the recommendations made by the PC Inquiry into Data Availability and Use
- July 2018 – Issues paper released on the proposed legislation; 108 submissions,
- August 2018 – Interim National Data Commissioner appointed
- July 2018 – April 2019 – Over 50 roundtables hosted to discuss policy intent and seek views on how to address them.
- July 2019 – Galexia PIA completed on policy settings for the proposed legislation; the PIA process included consultation
- September 2019 – Discussion Paper and PIA released to elicit stakeholder feedback; the ONDC received 79 submissions
- September 2019 roundtables – 26 additional roundtables organised to discuss the policy positions outlined in the Discussion paper and PIA
- February 2020 – This PIA conducted on draft DATB taking into account feedback and changes since September 2019 consultation
- February 2020 – Targeted consultation on this PIA with key stakeholders (see section 11.2.4)
- September 2020 – Release of DATB exposure draft and call for public submissions
- December 2020 – DATB introduced to Parliament.
- January 2021 – DATB considered by the Senate Standing Committee for the Scrutiny of Bill: Scrutiny Digest 1 of 2021
- February 2021 – DATB referred to the Senate Finance and Public Administration Legislation Committee.

12.2 Significance of the change to data handling

The type of data sharing that might occur under the Data Sharing Scheme would not necessarily be new or different to current data sharing activities. The problem, identified in the Productivity

Commission inquiry, is that, for many reasons including impediments in law and culture, the amount of data being shared is relatively small, meaning that opportunities are being missed.[74]

Currently data sharing occurs on an agency-by-agency basis, each one guided by enabling legislation, its interpretation of secrecy and disclosure provisions, its risk matrix for data release and so on. The DATB aims to streamline this and in the process encourage greater data sharing.

What is significant are changes to process and scale. Also significant is the social and technological environment in which the DATB's Data Sharing Scheme would operate. The advent of new technologies like data analytics, artificial intelligence, face recognition – and indeed the combination of these technologies – as well as increased inherent security risks when sharing data must also be considered.

Outside of the Australian public sector, the scale of data flows and sharing is also still exploding, including indiscriminate sharing globally for state and business activities. And much sharing is unregulated at either the national or international level and even if it is, enforcement is a challenge.

Because this is the environment into which all this shared data could enter into, extremely tight control is needed on the shared data so that the result is not simply additional and authoritative information going into those lakes.

Where data sharing has been impeded by law and culture in the past, this has had the unintended but sometimes beneficial effect of rendering government-held personal information 'practically obscure.' Privacy is protected through obscurity and data siloes. The potential scale and processing capabilities of data sharing raises the stakes for the policy advisers and legislative drafters. Small changes to the DATB, for example, carry potentially large implications for the privacy of individuals.

12.3 Key participants in the DATB Data Sharing Scheme

The DATB defines and/or specifies the roles of participants in the Data Sharing Scheme it would establish. This includes:

- **National Data Commissioner**
  Promotes the use and reuse of public sector data and data sharing best practice; regulates and enforces the Data Sharing Scheme; administers the accreditation framework and accredits entities; guides Data Scheme Entities via data codes and guidelines; advises the Minister on data sharing matters; cannot compel data sharing.
- **National Data Advisory Council**
  Advises the National Data Commissioner on ethical data use, community engagement, technical best practice, as well as industry and international developments.[75]

[74] Productivity Commission, Data Availability and Use Inquiry *Final Report* (8 May 2017), available at <https://www.pc.gov.au/inquiries/completed/data-access#report>.

[75] Discussion Paper, p 13.

- **Data Scheme Entity**
  A term used by the DATB to refer to Data Custodians and Accredited Entities.
- **Data Custodian**
  A Commonwealth body that holds public sector data and has a right to deal with it.
- **Accredited User**
  An organisation or individual who may access public sector data under the Data Sharing Scheme.
- **ADSP** (short for 'Accredited Data Service Provider').
  May be recruited by data custodians to help the custodian make decisions about data sharing and to undertake sharing on the custodian's behalf (including related services such as cleaning data, providing secure access and safely storing datasets). In high risk data integration cases ADSPs must be used.
- **Accredited Entity**
  A user or service provider that has been accredited under the accreditation framework administered by the National Data Commissioner.

13. Appendix D – Areas for guidance to support the DATB

IIS identified the following broad areas on which it considers the ONDC would need to prepare guidance to assist Data Scheme Entities apply the DATB consistently and as expected. IIS understands that the ONDC already has many of these areas on its radar and has, or is in the process of, undertaken development work.

- Privacy governance standards for accreditation
- Privacy and security guidance for Data Scheme Entities
- The meaning and scope of Data Sharing Purposes
- Data minimisation
- The scope of 'enforcement related matters'
- Undertaking a holistic risk assessment of the Data Sharing Principles
- Development of Data Sharing Agreements, including the level and nature of detail to ensure the Agreements are transparent and accountable
- Governance of data sharing activities, including of security for data sharing processes
- Applicable ethics processes
- Consent for sharing for delivery of government services
- Application of the Data Sharing Principles
- Application of the consent provision, including the meaning of 'unreasonable or impracticable', considering use of de-identified data, and the meaning of consent
- Describing and weighing the public interest
- Managing re-identification risks
- Operation of the exit mechanisms for shared or released outputs.

INFORMATION
INTEGRITY
SOLUTIONS

Information Integrity Solutions Pty Ltd
PO Box 978, Strawberry Hills NSW 2012, Australia
P: +61 2 8303 2438
F: +61 2 9319 5754
E: inquiries@iispartners.com
www.iispartners.com

ABN 78 107 611 898
ACN107 611 898