Data Availability and Transparency Bill

KPMG Australia

November 2020

—

KPMG.com.au

Contents

Executive Summary

In this report, KPMG Australia (KPMG) responds to the Australian Government's Exposure Draft Data Availability and Transparency Bill 2020 (the Bill) and examines the key matters that will need to be considered in the final Bill and related legislative reform package.

As a leading professional services firm that undertakes a significant amount of data advisory and legal work for government and private clients, KPMG is very pleased to be able to draw upon our multi-disciplinary expertise to provide our feedback and submission on the Draft Exposure Data Availability and Transparency Bill. We strongly support a public sector data availability and transparency scheme given the significant benefits that can be drawn from greater levels of safe sharing of quality data across entities such federal and state government agencies, as well as the research community. Our submission is, therefore, designed to help inform and improve the ongoing development of the Bill and associated frameworks.

KPMG is supportive of a Commonwealth public sector data sharing scheme given the significant benefits from the ability of critical government departments and agencies such as Services Australia, the Australian Tax Office, the Department of Home Affairs , the Australian Bureau of Statistics and bodies such as the Australian Institute of Health and Welfare, to share and access each other's data to support the delivery of: day to day services, policy development and critical program provision during national disasters.

The Productivity Commission referenced several studies that have attempted to place quantitative estimates on the benefits that could arise from greater availability and use of public sector data in its report *Data Availability and Use*. Estimates for the value of Australian public sector data vary substantially from $625 million per year up to $64 billion for the potential change in economic output if all public data was made open[1]. While the Bill does not specifically focus on making public data open, there are still likely to be significant opportunities for broader economy wide benefit.

What many of these previous estimates of economic benefit did not predict is how fundamental data has been to the Australian Government's response to the COVID-19 pandemic and the recent bushfires. Government held data has been instrumental in developing responses that meet the needs of Australians in an unprecedented time of upheaval. The most significant was the ability for the Australia Government to meet the needs of millions of Australians online instead of queuing at a Centrelink office.

> *Government held data has been instrumental in developing responses that meet the needs of Australians in an unprecedented time of upheaval.*

[1] *https://www.pc.gov.au/inquiries/completed/data-access/report/data-access.pdf*

The Bill seeks to find the right balance between streamlining the sharing and use of data while addressing privacy and security risks by establishing oversight and good governance practices. It will also establish an independent National Data Commissioner (NDC) to uphold the safeguards embedded in this scheme and support scheme entities.

KPMG's submission looks at some of the topics that may warrant further investigation and consideration in drafting the provisions in the final Bill as well as the data codes and regulations that will underpin the framework. These include consideration of data ethics, how the scheme interacts with state and federal legislation, matters of consent, how data breaches are dealt with, risk management, the accreditation framework, data quality and the associated resources and training. The submission also makes several recommendations.

We expand on our eight key themes in Section A: **KPMG Australia's recommendations for data availability and transparency**.

Regards,

Sanjay Mazumdar

Dr Sanjay Mazumdar
Chief Data Officer/Partner
KPMG Australia

Government held data has been instrumental in developing responses that meet the needs of Australians in an unprecedented time of upheaval.

Our recommendations are centred on eight key themes:

1. Data Ethics

The ethical use of data is paramount to drive public trust in the sharing of public sector data. Our review of the Bill highlighted some areas for further considerations and potential improvement that are summarised below:

Recommendation 1.1

Refine the definition of public sector data to require additional details regarding the scope, nature (e.g. raw, processed) and origin (e.g. generated by algorithmic models) of the related data.

Recommendation 1.2

Provide further guidance on the use of data to protect children and vulnerable people.

Recommendation 1.3

Further define principles and boundaries for ethical data sharing practices.

2. Interaction with other Commonwealth and State & Territory privacy and data schemes

This is an opportunity to develop a robust, consistent and clear national framework that addresses overlapping Commonwealth, State & Territory privacy and data protection frameworks and learnings from other data schemes. Our review of the Bill has identified opportunities to further consider and reflects these. The Bill is being developed in the context of several data related reforms and review, including the *Privacy Act 1988* (Cth) (Privacy Act).

Recommendation 2.1

The legislative scheme should be interoperable with other privacy and data frameworks and clearly and consistently define terminology.

Recommendation 2.2

The operation of the Memorandum of Understanding (MOU) and other participation arrangements and how the data sharing scheme will operate alongside them should be clarified.

Recommendation 2.3

The adequacy of the provision in State and Territory privacy laws should be confirmed and the Rules should prescribe the requirements for how accredited users can demonstrate compliance with State and Territory privacy laws that meet Privacy Act standards.

3. Consent

Consent is a fundamental concept in modern data protection and privacy laws. KPMG makes the following recommendations to strengthen and clarify the role of consent in the Bill.

Recommendation 3.1

Define the requirements of consent in the Bill, aligned with Privacy Act requirements, to formalise the position set out in the Explanatory Memorandum.

Recommendation 3.2

Clarify the impact of aging or withdrawn consent to the ongoing sharing or use of personal information in public sector data.

Recommendation 3.3

Include requirements in the Bill for data custodians to provide information to individuals about the sharing of public sector data that is personal information (such as the purposes for which it will be shared, and which agencies it is likely to be shared with).

4. Dealing with data breaches

How data scheme entities deal with data breaches is critical to the success of the scheme and public trust in it. There is an opportunity to further develop and clarify the obligations in the Bill and how they will interact with data breach schemes in other Acts. We therefore make the following recommendations:

Recommendation 4.1

The risk of harm from non-personal data breaches and notification of affected entities should be further considered and closely align with the existing Notifiable Data Breach (NDB) Scheme.

Recommendation 4.2

Notification to affected entities should be required.

Recommendation 4.3

Further consideration be given to how data scheme entities comply with overlapping data breach reporting obligations that apply to datasets that may be released.

Recommendation 4.4

Clarification about the coverage of State and Territory privacy laws and the obligations of State and Territory bodies in responding to data breaches.

5. Risk Management and the Five Safes model

The Data Sharing Principles of the Bill are adapted from the Five Safes Framework, which has become a standard among Australian government departments in assessing the risks relating to data access and release. While KPMG agrees that the framework provides a good model for understanding and assessing data sharing holistically, the suitability of this model as a set of legislative principles will depend on the development of a very clear and robust framework through the provisions in the Bill and codes of practice.

With that in mind, we propose the following recommendations:

Recommendation 5.1

Create a list of principles that align with well-known privacy language, particularly due to the global nature of the Bill, and provide better clarity over what is expected from all parties, at all times.

Recommendation 5.2

Articulate a more stringent risk management framework such as the framework adopted by the ANAO, or the expectations around implementing such a framework, that better spells out the required controls to protect scheme data. This will help reduce the shared risk of onward access and release of data.

Recommendation 5.3

Ensure adequate guidance is released to cover how to release data, how to risk assess the release, and how to manage risk when holding and using scheme data.

Recommendation 5.4

Create a working group among select scheme entities, legislators and relevant parties, to foster collaboration, knowledge sharing, and alignment in terms of interpretation and implementation of the bill.

Recommendation 5.5

Clarify how existing participants of datasets and registers, particularly those granted access through MoUs, will be affected by the Bill and how participation in the bill will be encouraged where existing arrangements provide an easier mechanism to release data.

Recommendation 5.6

Provide stricter accountability measures on data custodians, such as the need to be accredited, and provide guidance on how data release assessments should take place, including, in particular, what is expected from the data custodian to go over and above the accreditation achieved by the requestor.

6. Accreditation framework

The accreditation framework is foundational to how the Bill will regulate and ensure that data scheme entities have demonstrated a level of rigor around their capabilities to handle government data and have considered the purposes for which they will use government data. We have made a few specific recommendations to help create a more streamlined accreditation process that benefits both data custodians and accredited entities:

Recommendation 6.1

Entities acting under an Accredited Data Service Provider (ADSP) or accredited user should not be required to accredit separately.

Recommendation 6.2

There should be a transition period for current government data service providers to enable them to continue to deliver their services while the Scheme comes into effect and applications for accreditation are being processed.

Recommendation 6.3

The scheme accreditation renewal period should be every 5+ years.

Recommendation 6.4

Ensure that there is consistency in the use of the data sharing agreement template through National Data Commissioner oversight and review.

Recommendation 6.5

Sub-contractors or suppliers to ADSPs or accredited users as part of delivering services to data custodians etc should be specifically considered as part of the data sharing agreement and should not be required to accredit separately.

Recommendation 6.6

The consent disclosure requirements in the data sharing agreement should be broadened to include ongoing monitoring and reporting on consent to ADSPs and accredited users.

Recommendation 6.7:

There are certain elements of data capability that we recommend should be captured in order to understand an accredited entity's ability to keep data safe, including labelling and tagging of data, as well as encryption or some form of protection.

7. Data Quality

Data quality is an essential factor in the integrity and reliability of the outcomes and an important driver of trusting its use. In the context of sharing, it will have even more importance given any issue can be scaled up when used more broadly or out of the original context. Some considerations under the Bill can help further managing such risks.

Recommendation 7.1
Embed data quality requirements in the accreditation framework.

Recommendation 7.2

Data custodians should be accountable for the data quality within the context and manage it through the data sharing agreement.

8. Resourcing and training

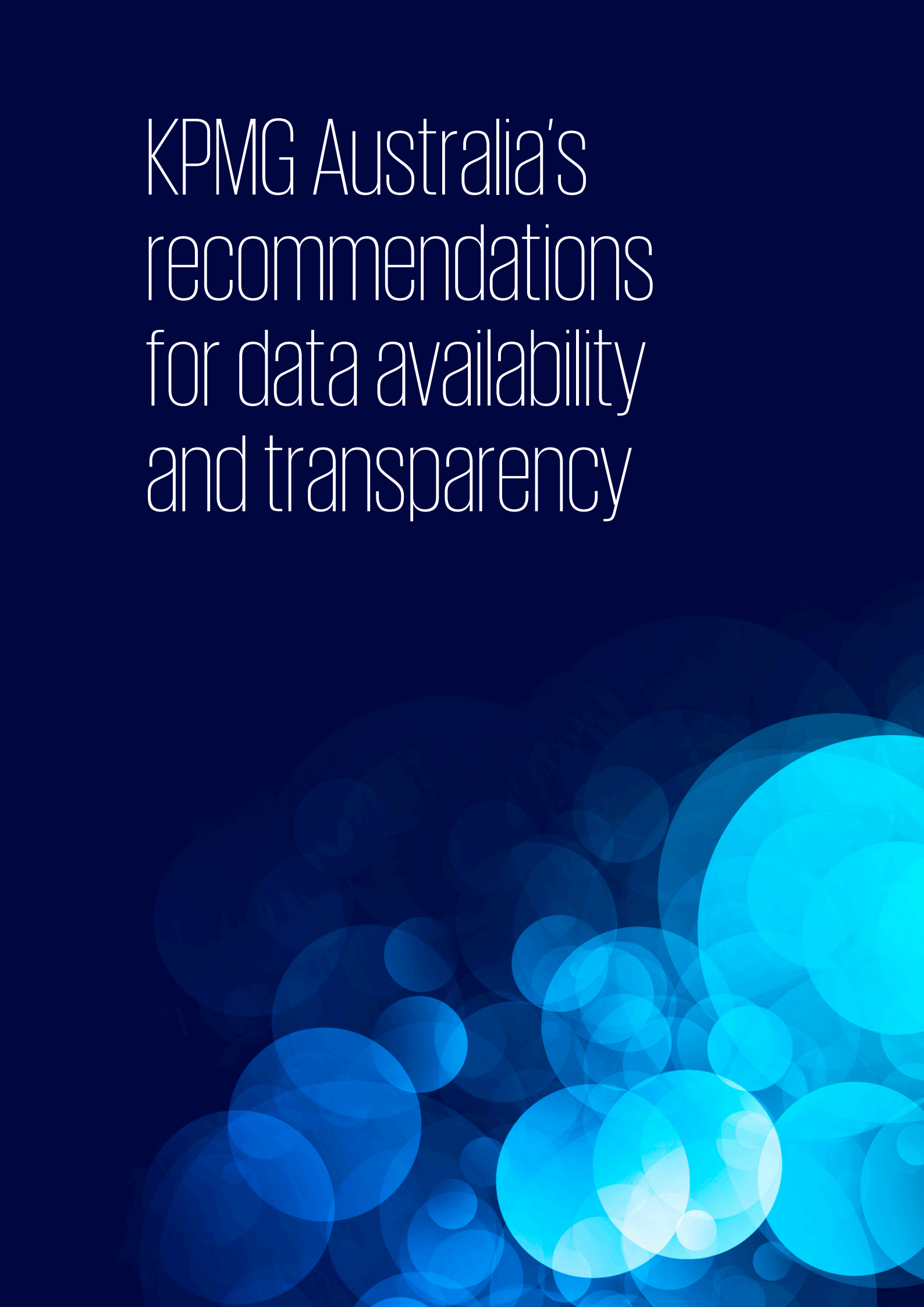
The Bill places additional workload on data custodians and accredited users to comply with its requirements, as well as on the ONDC to accredit users and data service providers and provide oversight of the scheme. It is KPMG's view that further consideration should be given to identifying the resources required (roles, skills) to adequately support the implementation the data sharing scheme and to track the performance of data scheme entities against this requirement.

Overall, we recommend:

Recommendation 8.1

KPIs should be established to track any shortfalls in resources (numbers, skills) of data scheme entities.

KPMG Australia's recommendations for data availability and transparency



1. Data Ethics

Our review of the Draft Exposure Data Availability and Transparency Bill 2020 (Bill), has highlighted the following considerations:

Increasing transparency on the scope and nature of data being shared:

A study conducted in 2018 by the Australian National University[2] shows that although the public is generally supportive of government using data, there is less consensus in the Australian Government's ability to use data in an appropriate and responsible way. The public ethical concerns on appropriate use, management and sharing of data become even more relevant when new technologies (e.g. Artificial Intelligence) are considered. Automated systems not only process the information provided by individuals but also create new types of data that individuals are not necessarily aware of (e.g. non-intuitive connections and patterns between people; predictions on people's behaviours). Greater transparency on the nature (and origin) of data subject to the sharing agreement is pivotal to build public trust. This is further emphasised in recent research conducted by the University of Queensland and KPMG Australia.

University of Queensland/KPMG Australia Trust in Artificial Intelligence report

KPMG's recently released the Trust in Artificial Intelligence (AI) report[3] in partnership with the University of Queensland. The report included the first national survey into AI, setting out the extent of Australians' trust in and support of AI, and aims to benchmark these attitudes over time. The report finds that more than half (61%) of Australians know little about AI and many are unaware that it is being used in everyday applications, like social media. While 42% generally accept it only 16% approve of AI.

Some of the findings of the report that relate to data and AI ethics considerations include:

- Australians think data challenges are most likely to impact people in the near future - most respondents (67 – 70%) think data challenges such as fake online content, surveillance, data privacy and cyber-attacks are most likely to impact large numbers of Australians over the next 10 years
- The vast majority of Australians (71-80%) agree that assurance mechanisms that support the ethics of AI systems would make them more willing to use AI systems
- 45% are unwilling to share their data with an AI system

It is also important to recognise that many privacy laws around the world are centred around the protection of personal information, which relies on the idea of identifiability – that is, whether or not a person's identity can be reasonably ascertained from a piece of information[4]. This approach raises challenges from an ethical perspective as the emergence of Big Data and advanced data

[2] Public attitudes towards data governance in Australia, Australian National University, 2018: https://csrm.cass.anu.edu.au/research/publications/public-attitudes-towards-data-governance-australia-0

[3] https://home.kpmg/au/en/home/insights/2020/10/artificial-intelligence-trust-ai.html

[4] Submission in response to the Artificial Intelligence: governance and leadership White Paper – Office of the Victorian Information Commissioner, 2019 https://ovic.vic.gov.au/wp-content/uploads/2019/03/20190315-OVIC-submission-to-AHRC-AI-Governance-and-Leadership-White-Paper-v1.0-website-version.pdf

analytics techniques (e.g. Artificial Intelligence) challenge this binary understanding of personal information in a number of ways and result in the risk of managing new types of identifiable information[5] (e.g. inferences) that are not currently covered by the current legislative framework.

The importance of responsible sharing and use of children and vulnerable people's data:

As highlighted in the UNICEF Policy guidance on AI for children[6] "children's lives and well-being are directly and indirectly impacted by automated decision-making systems that determine issues as varied as welfare subsidies, quality of health care and education access, and their families' housing applications." Moreover, the need for pro-active protection of the most vulnerable segments of the population when making decisions or developing services and products informed, enabled or driven by data has been called out by numerous academics as well as Governments. In this context, consideration should be given to providing guidelines on how to use and share children and vulnerable people's data as well as to potentially limiting some of the exemptions (e.g. consent exemption – section 16) articulated in the Bill.

Setting consistent principles and guardrails for ethical data sharing practices:

The project principle articulated in the Bill requires that any applicable processes relating to ethics are observed. As soft and hard regulations governing and guiding the ethics of data are still evolving (in Australia as well as internationally) and mostly being adopted on a voluntary basis, it is important to further clarify the minimum data ethics practices that are expected to be met by the agencies participating in the data sharing agreement. This would ensure greater transparency as well as consistency in approach.

With these topics in mind, we recommend to:

Recommendation 1.1 *Refine the definition of public sector data to require additional details regarding the scope, nature (e.g. raw, processed) and origin (e.g. generated by algorithmic models) of the related data.*

Additionally, consideration should be given to providing additional guidelines on the types of data included in the "personal information" definition to ensure that new types of identifiable data that have not historically been covered by the current data privacy legislative framework are subject to adequate protection.

Recommendation 1.2

Provide further guidance on the use of data to protect children and vulnerable people

To provide guidelines on responsible practices for the use and sharing of children and vulnerable people's data, including, as a minimum, a definition of what constitutes a vulnerability, how to detect and understand those and ethical practices and guardrails to be consistently adopted and evidenced by the accredited entities.

[5] A right for reasonable inferences; re-thinking data protection law in the age of Big Data and AI, Sandra Wachter, Brent Mittelstadt, 2018:https://www.researchgate.net/publication/327872087_A_RIGHT_TO_REASONABLE_INFERENCES_RE-THINKING_DATA_PROTECTION_LAW_IN_THE_AGE_OF_BIG_DATA_AND_AI

[6] UNICEF, Policy Guidance on AI for Children, September 2020: https://www.unicef.org/globalinsight/reports/policy-guidance-ai-children

Consideration should also be given to revisiting some of the exemptions articulated in the Bill (e.g. consent exemption – section 16) to assess their adequacy and appropriateness in the context of sharing and use of children and vulnerable people's data.

Recommendation 1.3

Further define principles and boundaries for ethical data sharing practices

To further define minimum and consistent principles and practices to be met by accredited users to adopt (and evidence) ethical data sharing practices

2. Interaction with other Commonwealth, State & Territory legislation

The Bill is intended to support a cultural shift to data sharing and release by government agencies, which was identified as an objective by the Productivity Commission Report on its Inquiry into Data Availability and Use[7] (PD Report). This shift is towards institutionalising a robust risk-based authorisation approach to data sharing which focusses on mitigating the risks and enabling the safe sharing of data, to reduce barriers to sharing for certain public interest purposes. Since the PD report, the acceleration of the digital economy, including the delivery of government services and products through digital channels (partly as a result of the Covid-19 pandemic), has resulted in the datafication of both private and public sector.

To achieve its objectives, the Bill will establish another framework for Commonwealth public sector data sharing. Australia currently has a patchwork of fragmented and overlapping Federal, State & Territory and sector specific data protection laws that aim to facilitate and permit the safe sharing of or access to data, including personal information, whether in general or in relation to prescribed data sets, such as data collected in registers established by statute (e.g. the *National Cancer Screening Register Act 2016*– (the **NDCR Act**)). These include privacy, health records and surveillance devices laws, the Consumer Data Right (**CDR**) and *MyHealth Record Act*. Each creates a separate regulatory scheme for the sharing, transfer and protection of data which entities who are covered by or who wish to participate in the scheme must comply with.

These schemes most commonly relate to personal information but also cover other types of data and the risks that need to be addressed are commonly associated with the sharing of personal information or confidential data.

Privacy laws such as the Privacy Act are referenced in these legislative schemes as the applicable and founding framework for the protection of relevant data that is personal information. While it is not intended to specifically apply to personal information, the Bill contemplate that public sector data covered by the scheme will include information about individuals (see for example *Privacy Coverage* - section 27 and *Data breach responsibilities* - Part 3.3). (Reference to addressing the risks of release of personal information are also found in related documents such as the PD Report and the NDC's 2019 Data Sharing Principles Best

[7] https://www.pc.gov.au/inquiries/completed/data-access/report/data-access.pdf

Practice Guidelines[8] (**NDC Guidelines**)). The Bill will also establish a National Data Advisory Council which will have advisory functions relating to the sharing and use of public sector data including ethics and balancing data availability with privacy protection (section 60).

The CDR, which was also developed in response to the PD Report, covers the information of both individual and certain businesses who are defined as 'consumers' for the purposes of the CDR. The Victorian *Privacy and Data Protection Act 2016* applies to both personal information and public sector data and the same regulator has responsibility for both.

The introduction of this new public sector data sharing framework reinforces the need for a re-think of the current legal and regulatory data framework in Australia for an open data economy, which KPMG has previously called for in the context of its submission to the Federal Government's current *Inquiry into the Future Directions for the Consumer Data Right* [9].

This will help to achieve the objectives identified in the submission which include creating certainty, reducing the regulatory burden and maintaining community trust.

In the context of the Bill and the scheme it is establishing, it is also important that sufficiently clear and consistent direction is given in the legislation as well as the subordinate framework of codes, rules, regulations and guidelines to:

- prescribe the supporting mechanisms and features of the scheme with sufficient particularity;
- ensure the data terminology, safeguards, standards and principles to be developed are consistent and interoperable with other frameworks and commonly understood legal definitions. For example, the definitions of sharing and release, use and making available in the Bill as well as terms in the NDC's Guidelines[10] such as data provider and particularly sensitive information are not all consistent with the Privacy Act definitions including in the Notifiable Data Breach scheme;

Recommendation 2.1: *The legislative scheme should be interoperable with other privacy and data frameworks and clearly and consistently define terminology.*

The Bill will permit State and Territory bodies (departments or authorities) as well as, for example, universities who are subject to State or Territory laws, to become accredited users to be authorised to collect and use scheme data for the permitted data sharing purposes as long as the relevant government services, policy or programs include the Commonwealth government. Currently this type of data sharing is governed by numerous Memoranda of Understanding (MoU) or 'participation arrangements' that may be more or less prescriptive depending on the data, applicable legislative framework, the data custodian and the permitted data sharing arrangements. The introduction of data sharing agreements is a welcome development as it supports transparency, consistency and trust. It also provides a framework that can be leveraged by States & Territories in the future.

However, it is not clear how the new data sharing arrangement will operate alongside existing MoUs or arrangements under current data sharing schemes. These schemes already authorise or support the safe release and sharing of public sector data.

[8] https://www.datacommissioner.gov.au/sites/default/files/2019-08/data-sharing-principles-best-practice-guide-15-mar-2019.pdf

[9] KPMG's submission to the Federal Government's current Inquiry into the Future Directions for the Consumer Data Right : https://treasury.gov.au/sites/default/files/2020-07/KPMG-2020.pdf

[10] https://www.datacommissioner.gov.au/sites/default/files/2019-08/data-sharing-principles-best-practice-guide-15-mar-2019.pdf

Recommendation 2.2: *The operation of the MOU and other participation arrangements and how the data sharing scheme will operate alongside them should be clarified.*

Further, the privacy protection and data breach notification provisions in the Bill also demonstrate how the laws are fragmented, overlap and are not consistent which provides added complexity and could be a potential barrier to data sharing as well as cause confusion for data scheme entities.

First, the Bill will provide that any data scheme entity that is not an organisation that is subject to the Privacy Act, must not handle personal information for the purposes of the Bill, unless in relation to the act or practice either:

a. the Privacy Act applies as if it were an organisation as that term is defined in the Privacy Act; or
b. a State or Territory law applies which has provisions for: the protection of the personal information in a *comparable* way to the APPs, monitoring and compliance with the law and individuals to seek redress if there is a breach of the law.

This would appear to require the relevant State or Territory body, if it is intending to collect data that includes personal information, to assess whether the State or Territory law to which it is subject contains the above provisions. The prescribed requirements for the data sharing agreement do not include any terms relating to the application of privacy law regimes or for their assessment. However, we note that the Accreditation Framework Discussion Paper indicates that the accreditation criteria will be established in Ministerial Rules based on three categories, including arrangements for security and privacy of data. The paper also appears to confirm that a State or Territory body has equivalent 'coverage' under the relevant State or Territory privacy laws. We submit that this should be clarified. We are not aware of a detailed comparative assessment being undertaken between the relevant principles in the State & Territory privacy laws and the APPs. We note that the coverage provision in (b) above does not require the relevant law to make provision for data breach notification. The Rules should prescribe the requirements for demonstrating coverage that meets all these coverage provisions.

Recommendation 2.3: *The adequacy of the provision in State and Territory privacy laws should be confirmed and the Rules should prescribe the requirements for how accredited users can demonstrate compliance with State and Territory privacy laws that meet Privacy Act standards.*

3. Consent

Consent is a fundamental concept for authorising the collection, use and sharing of personal information in modern data protection and privacy laws, including the Privacy Act and international laws (such as the EU's General Data Protection Regulation). The Bill recognises the role of consent in the Project Principle (s 16(1)(b)):

> *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.*

Genuine consent puts individuals in control, builds trust and engagement, and enhances entities' reputations. The key elements of consent (that the consent is informed, current and specific, voluntary and given by an individual with capacity to do so) are recognised in guidance from the Office of the Australian Information Commissioner (OAIC),[11] and their importance has been reinforced in the ACCC's 2019 Digital Platforms Inquiry report.[12] However, obtaining genuine consent for the purposes of meeting data protection and privacy requirements is often challenging: information and power imbalances often mean that individuals are not fully informed, that consent is not voluntarily given, or that individuals may be asked to give consent when they do not have capacity to do so, and common practices for organisations requesting consent (such as 'bundled consent') often mean that consent is not current or specific.

Relying on inappropriate or invalid consent can damage trust and harm the organisation's reputation. Conversely, strong processes for obtaining valid consent can help to build trust and confidence in data sharing practices and in the services provided by the government, industry, research, and other private sectors, encouraging individuals to trust these entities with more useful data.

Against this background, KPMG recommends that the Bill be amended to clarify the expectations on data custodians seeking to rely on consent as a basis for determining that data sharing is consistent with the project principle. While we note that the Explanatory Memorandum to the Bill aligns (at para 123) the consent requirements to those under the Privacy Act and guidance from the Information Commissioner, we recommend that these requirements are prescribed in the Bill for the following reasons:

1. the Privacy Act, in its current form, does not explicitly set out the requirements of consent- while the Information Commissioner's guidance notes the importance of consent being current, specific, etc., this guidance is, strictly speaking, non-binding;
2. enshrining the requirements of consent in the Bill would be consistent with the ACCC's recommendations to formally define those requirements in the Privacy Act (notwithstanding the previous point, the Privacy Act has not yet been amended following the ACCC's recommendations);
3. formally setting out consent requirements in the Bill would enable the Government to clarify important aspects of consent, such as whether consent must be express (or whether implied consent is sufficient) and whether consent can be withdrawn or revoked; and

[11] Office of the Australian Information Commissioner, APP Guidelines, Chapter B, available at <https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-b-key-concepts/#consent>.

[12] 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

4. specific consent requirements in the Bill (possibly supported by guidance or rules made under the Bill) could be tailored to the specific context of data sharing and the extent to which it includes or could include personal information which may include higher expectations from individuals, and could recognise both the important role of government and the power imbalances that may exist between individuals and government agencies.

Recommendation 3.1: *Define the requirements of consent in the Bill, aligned with Privacy Act requirements, to formalise the position set out in the Explanatory Memorandum.*

Additionally, it is not clear from the Bill whether data sharing (or use of shared data) may continue when consent can no longer be considered valid (e.g. when sufficient time has passed that the consent should no longer be considered current, or where the individual withdraws their consent). This presents risks both to individuals (who may find themselves unable to limit the ongoing use of their information as their circumstances change) and to entities involved in data sharing (who may continue to share or use data even when the consent requirement of the project principle no longer holds).

We recommend that the Bill be amended to clarify the impact that aging or withdrawn consent has on the validity of data sharing, and in particular on the consistency of the data sharing with the project principle. The consent withdrawal provisions in the Consumer Data Right (CDR) scheme may provide a suitable model.

Recommendation 3.2: *Clarify the impact of aging or withdrawn consent on ongoing sharing or use of data.*

Finally, we recommend that the Bill clarify the kinds of information that must be given to individuals, and the way in which this information should be provided, to ensure that consent is fully informed and specific. APPs 1.4 and 5.2 under the Privacy Act set out matters that must be disclosed to individuals in a privacy notice and a collection notice, respectively. These requirements help to ensure that any consent provided by the individual is made on the basis of clear information about how their personal information will be collected, used and disclosed.

A similar requirement in the Bill would assist custodians in obtaining consent that meets the requirements of the Bill and individuals' expectations.

Recommendation 3.3: *Include requirements in the Bill for custodians to provide information to individuals about the sharing of data under the data sharing scheme that is personal information (such as the purposes for which it will be shared, the basis on which it will be shared and which agencies it is likely to be shared with – they could refer to the Register of accredited entities).*

4. Data Breach

The data breach responsibilities that will be established in Part 3.3 provide that a data custodian will be deemed to hold any personal information that forms part of the public data it shares for the purposes of the Notifiable Data Breach (**NDB**) Scheme in Part IIIC of the Privacy Act (section 36(1)). This is a potential barrier to data custodians being willing to share public sector data given the potential risks to individuals if the accredited user suffers a data breach. Section 36(2) aims to address this by enabling the data custodian and any accredited entity that holds the personal information and that is also an APP entity subject to the NDB Scheme, to agree that section 36(1) will not apply. This means the data custodian will not have responsibilities for the personal information the accredited entity holds.

There are no notifiable data breach schemes in the State & Territory privacy and health records laws that currently would apply to State and Territory bodies. Only the Privacy Act and the *MyHealth Records Act* as well as some prescribed schemes (such as the NDCR Act), which are all Commonwealth legislation, establish mandatory data breach notification schemes. Therefore, no accredited entity that is a State or Territory body who may hold personal information for the purposes of section 36(1) will be subject to the NDB Scheme or equivalent. However, the Bill would require a State or Territory body that is an accredited entity to takes steps to mitigate any harm to an individual from a data breach involving their personal information (section 35). This leaves the data custodian responsible for taking all of the other steps required by the NDB Scheme in response to a data breach which the State or Territory body has had that affects personal information the body holds as part of the public sector data shared with it as an accredited user, including notifying the OAIC and affected individuals and providing a copy of the notice to the NDC.

Non-personal data breach criteria

The Bill also makes overlapping provisions for responding to and notifying serious data breaches that do not involve personal information but would be likely to result in serious harm to an entity (section 37). The definition of entity includes individuals and the section does not exclude individuals from notification obligation.

It is expected that any breach which involves personal information must be handled and assessed under the NBD Scheme and any serious breach involving any other data must be assessed according to the criteria in section 37(2) and notified to the NDC. We understand that this contemplates that a breach involving data that is not considered personal information, may in any event cause a risk of serious harm to individuals and require notification. De-identification continues to remain a challenge for government and industry alike. In our view, the criteria in the Bill for assessing whether a breach is serious should be further developed and align with the NDB.

Recommendation 4.1: *The risk of harm from non-personal data breaches and notification of affected entities should be further considered and closely align with the existing NDB Scheme.*

There is also currently no requirement in the Bill for a data scheme entity to notify any affected entities (including individuals), in the same way the NDB Scheme would require the data custodian or an APP entity, in order to enable the affected entities to take steps to mitigate harm to them directly or to anyone they are in a position to determine may be affected by the breach. KPMG submits that this is a potential gap in the data breach scheme which the Bill should include, particularly given the potential for individuals to be affected by what data scheme entities may consider to be non-personal data breaches.

Recommendation 4.2: *Notification to affected entities should be required.*

Overlapping data breach requirements

As noted above, there are particular datasets or registers that are subject to pre-existing data scheme frameworks, such as the NCSR (which also makes provision for criminal offences and data breach notification obligations to the OAIC for unauthorised access and disclosure of NCSR data). Like the Bill, they have privacy terms and data breach definitions and obligations that are in addition to or overlap with the Privacy Act. This means that departments and agencies who hold public sector data that is likely to be of interest to accredited users will need to address multiple overlapping data breach regimes and may need to notify more than once.

KPMG submits that careful consideration should be given to the effect of these overlapping data breach requirements and clarification for how breaches in relation to data sets that are the subject of another scheme are notified and which regime would apply. This could also be further addressed in the Rules for the Accreditation Framework, accreditation conditions, and data codes.

Recommendation 4.3: *Further consideration be given to how data scheme entities comply with overlapping data breach reporting obligations that apply to datasets that may be released.*

Recommendation 4.4: *Clarification about the coverage of State and Territory privacy laws and the obligations of State and Territory bodies in responding to data breaches.*

5. Risk Management and the Five Safes model

The Data Sharing Principles of the Bill are adapted from the Five Safes Framework, which has become a standard among Australian government departments in assessing the risks around data access and release. While KPMG supports that the framework provides a good model for understanding a data release holistically, the suitability of this model as a set of legislative principles needs to be considered carefully. Given our experience of how we have seen the model implemented we wish to highlight the following for consideration:

- The principles emphasise safety at the point of assessment and do not clearly explain the broader data protection and privacy expectations.
- The assessment of data releases adopting the Five Safes Framework is currently unlikely to be consistent in and across all data custodians.
- Further clarification is required about how MoUs, between Commonwealth and State & Territories and 'participation' arrangements under current legislative data schemes, will apply, which may deter entities from taking part in the scheme.
- The principles need to be reconciled against the need for accreditation.
- There may be a lack of accountability for data custodians.

These matters are expanded on below.

The principles over-imply a focus on safety at the point of assessment and do not clearly spell out broader data protection and privacy expectations

In their current form, the principles may be interpreted in a misleading manner that places too much emphasis on security at the point of release while foregoing other important principles of data protection & privacy or the ongoing protection of the information post-release. For example, it is KPMG's experience that organisations interpret the 'safe settings' principle with an over-emphasis on the security of the transfer of the data when assessing a release but may not adequately assess the security of the recipient's environment once the transfer has taken place. In addition, Data Custodians can lack the expertise or resources to assess whether data can be or has been properly deidentified, or whether data can be reasonably re-identified by the recipient based on other information available to them. There have been recent examples where a data release mirrored many of the elements already addressed in the Bill. That is, the data was released in good faith, in the public interest, for appropriate purposes. However, as the dataset was not adequately de-identified it was determined to be a breach of APPs 1, 6 and 11. In their current form, the Data Sharing principles also may not clearly address other important privacy & data protection data handling concepts, such as data accuracy, integrity, or storage limitations, and while we appreciate that not all data released will include personal information, the current iteration of the Data Sharing Principles in the Bill may not adequately address ongoing data protection and handling expectations once the data has been released (that is, the principles in their current form imply a greater focus on the data at the point of assessment, but do not clearly articulate the ongoing expectations of how data should be handled once released).

Therefore, a better approach may be to mimic that of the EU GDPR and other relevant privacy and data laws that better spell out the specific principles and expectations of how data should be handled. For example, the principles of the GDPR suggest that, at all times (meaning in the context of a data release they would apply at both the point of assessment and continue to apply thereafter) data should be: used only for limited purposes (purpose limitation), minimised to only that data which is adequate, relevant and necessary for the purpose (data minimisation); processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures (integrity and confidentiality); stored for a

limited period and only as long as they serve the purpose of release (storage limitation); and the data should be accurate and kept up-to-date (accuracy). The more precise mention of such elements as 'technical and organisational measures' makes it clearer what is required under elements such as 'safe settings' while also still providing the scalability and flexibility that the bill is aiming to achieve through adopting a principles-based approach. Further, the GDPR principles better articulate ongoing expectations around privacy and data protection once data are released/disclosed and, unlike the five Data Sharing principles adopted from the Five Safes Framework, the GDPR principles adopt more globally recognisable language. Considering the extra-territorial applicability of the Bill, it would be prudent for it to also adopt globally recognisable privacy language.

While KPMG also understands that measures in the Bill such as the data sharing agreement and accreditation mechanisms of the recipient provide additional controls in this regard, the Data Custodian is not expected to achieve such accreditation and is responsible for making the ultimate decision on whether to release the data. By ensuring the principles provide greater clarity on the expectations of the Data Custodian, as well as ongoing accountability regarding how the data are handled, there is an increased likelihood that an agreement drafted by the Data Custodian will better reflect these expectations and a greater consideration of the relevant risks and controls will take place.

Inconsistency among government departments in the assessment of data releases adopting the five safes framework

In KPMG's experience there is broad inconsistency among organisations in the assessment of data releases and the application of the five safes framework. In many cases organisations may not have mature assessment processes, meaning data requests are light on information, are not auditable and do not involve a thorough assessment that considers all relevant matters, such as risks, controls and compliance with applicable laws. In these instances, assessments may fall to a sole individual approver, rather than operating within defined governance protocols with committees. In other cases, organisations have a more mature overarching governance system in place such as a committee and escalation pathways, but a lack of controls such as secure transfer mechanisms or de-identification protocols, or lack of expertise in privacy, security or law and ethics hinder the capability to adequately assess or release the data. Given the nature of the bill is to allow for the sharing and release of data that was previously barred by secrecy provisions it may also be the case that Data Custodians who have no prior experience with the five safes assessment or data release procedures may wish to begin releasing data. In addition, there may be scenarios where there are multiple Data Custodians involved in assessing and approving a data release, or there may be multiple parties involved through the chain such as service providers to ADSPs or data requestors. Such a chain of involvement can expose data releases to shared risks.

The scheme should encourage specific risk management frameworks that more clearly articulate what is required from the internal environments of all parties (including Data Custodians, ADSPs and so on). One such framework is that which the Australian risk management model adopted by the Australian National Audit Office (ANAO). ANAOs framework clearly maps out all risks, controls, shared risks, consequences, roles, and so on. When taken alongside the above-mentioned concern about the five safes acting as a set of legislative principles, the ANAO framework should instead be used as an appropriate data-management framework and be supplemented with global appeal and clear expectations around the implementation model and risk management protocols that should be in place. It would also be recommended that the Commissioner develop guidance that is specifically tailored to the Bill to articulate such expectations as well as establish a small working group for knowledge sharing among Data Custodians and other relevant parties to foster collaboration and alignment of implementation across government and other Data Scheme Entities. Such a working group would also serve to uplift those Data Custodians who may lack prior experience releasing data due to secrecy provisions.

Clarification required over MoU and 'participation' arrangements, which may deter entities from taking part in the Scheme

There are many datasets whereby entities other than the main Data Custodian, such as States & Territories, are able to collect, hold, record, access, use or disclose the data from the dataset so long as they agree to 'participate'. For example, many health data registers have such clauses applicable to 'participating states & territories'. There are also MoUs in place between the Data Custodians and such entities which outlines expectations and responsibilities. Under such arrangements it is common for the Data Custodian to expect the participant to have their own policies, governance and measures in place to assess and manage data releases, and otherwise comply with legislation and keep data safe. Many such participants may not have such arrangements despite the MoUs, and that there can be a lack of cooperation between those participants and the Data Custodian. Data Custodians also do not always intervene once the MoU is drafted or ensure ongoing assurance. It is therefore recommended that clarification is provided over whether such participants may also take advantage of data releases via the scheme, as the current arrangements already offer such participants a means to release data without the need for accreditation. In this way, the ease of existing arrangements may make the scheme a less enticing option, despite the scheme offering an overall higher level of trust than current data release operations.

The principles may be at odds with the need for accreditation

The general intention of the five safes Framework is to provide a scalable model that allows for controls to be tuned up or down depending on the level of risk, however the need for the recipient of the data (aside from government transfers for service delivery) to achieve accreditation (and therefore evidence stringent technical and organisational controls and governance arrangements) clashes with the idea of scalability. In this way, data requestors may be expected to evidence a level of assurance that is far beyond what is necessary in the context of the data release where such a release would pose a low risk. This may be particularly problematic in the case of small agencies, not-for-profits, or some researchers, where the accreditation scheme may act as a barrier to entry. It should be considered whether accreditation may be scalable using a levelled/tiered system, so that scheme participants may be able to gain access to certain risk thresholds or categories of data based on the level of accreditation they are able to achieve. On the flip side, this may also create a scenario already highlighted in this section whereby a Data Custodian may fail to adequately assess a data release on the grounds that the requestor is already accredited (i.e. Data Custodians may see accreditation as a quick way of assessing whether data can be released and forego a rigorous assessment pre-release). Guidance should address what is expected from Data Custodians above and beyond the accreditation when conducting an assessment to release data, and such accountability should be more explicitly placed on Data Custodians through the drafting of the legislation to ensure stringent assessments are always carried out.

Potential for a lack of accountability for Data Custodians

In its current draft the Bill may not adequately balance the accountability of Data Custodians. While there is an expectation that other entities must become accredited to receive data, there is no expectation on Data Custodians to achieve accreditation. Further, Data Custodians are able to transfer responsibility of breach reporting to other scheme entities. There is also no overall principle addressing the concept of accountability for Custodians. While KPMG appreciates that a Data Custodian is in many ways responsible for data, particularly through other legislative mechanisms, we feel there is a need to create more harmony between those requirements and the Bill to reduce risk of inappropriate use of or sharing of data via the scheme. This is particularly risky regarding data sets that were previously prevented from sharing due to secrecy provisions and Custodians are unfamiliar with data access & release processes. This can be achieved by introducing an accountability principle, as well as by implementing some of the recommendations already outlined above.

Recommendation 5.1: *Create a list of principles that align with well-known privacy language, particularly due to the global nature of the Bill, and provide better clarity over what is expected from all parties, at all times.*

Such principles should consider other well – known privacy and data legislation, such as the GDPR principles, for inspiration, to include such concepts as data limitation, purpose limitation, and organisational and technical measures.

Recommendation 5.2: *Articulate a more stringent risk management framework such as the framework adopted by the ANAO, or the expectations around implementing such a framework, that better spells out the required controls to protect scheme data. This will help reduce the shared risk of onward access and release of data.*

Recommendation 5.3: *Ensure adequate guidance is released to cover how to release data, how to risk assess the release, and how to manage risk when holding and using scheme data.*

Recommendation 5.4: *Create a working group among select scheme entities, legislators and relevant parties, to foster collaboration, knowledge sharing, and alignment in terms of interpretation and implementation of the bill.*

Recommendation 5.5: *Clarify how existing participants of datasets and registers, particularly those granted access through MoUs, will be affected by the bill and how participation in the bill will be encouraged where existing arrangements provide an easier mechanism to release data.*

Recommendation 5.6: *Provide stricter accountability measures on Data Custodians, such as the need to be accredited, and provide guidance on how data release assessments should take place, including, in particular, what is expected from the Data Custodian to go over and above the accreditation achieved by the requestor.*

6. Accreditation framework

The Accreditation Framework Discussion Paper[13] (**The Paper)** makes clear that this will involve a risk management framework to safely share the data and that arrangements included in the Data Sharing Agreements between participants will guide safe data sharing in a specific manner for each project being undertaken. In consideration of the Paper, we make the following comments:

- **Accreditation granted based on one application but multiple data sharing agreements:** Requiring Accredited Data Scheme Providers or Accredited Users to make multiple applications for accreditation would decrease the speed-to-market in relation to the services that could be provided and create an unnecessary compliance burden on organisational participants. Agreements at a project level to set scope and contractual controls, on top of the requirement to continually advise the NDC of certain changes to circumstances relating to accreditation is a preferred mechanism for ensuring optimal control and efficiency in the use of government data and we support this method of accreditation going forward.
- **Whether individuals acting on behalf of an Accredited Data Service Provider should be accredited individually (including being required to have specialist data skills and be subject to stringent hiring, vetting and training practices):** Considering the obligations on organisations to monitor their organisational competence and resources when accredited as part of the Framework, requiring individuals to self-accredit or separately accredit would pose a significant hurdle to utilisation of those individuals and their own skillsets. In addition, imposing those obligations on individuals directly whilst part of an accredited organisation may require a continuous level of oversight that may prove difficult when those individuals are in junior roles or roles that are removed from the organisational structure, particularly during the COVID-19 environment. Our view is that guidance should be created on certain required skillsets and benchmarks for vetting and training for organisations when tendering for government work which can then be filtered into organisational hiring, vetting and training practices. When compared as well with the regulation of the Privacy Act 1988, there are limited obligations on individuals (including no current criminal liability) and to create a scheme that would require working at external organisations to be personally liable for their handling of this data over and above the Privacy Act when governmental officials working under Data Custodians are not seems to be an incongruous policy position.
- **Status of current government data service providers whilst application to National Data Commissioner is pending:** Considering the legislation may apply to a large proportion of the Australian economy providing these types of government services and that it is currently unclear what a 'reasonable period of time' would be to assess applications and provide accreditation, there should be relief provided for a period of time to current government service providers whilst they work through the accreditation process and wait on that outcome. This will allow the continuation of services provided to government whilst the scheme comes into effect.

[13] Available at *https://www.datacommissioner.gov.au/sites/default/files/2020-09/Accreditation%20Framework%20Discussion%20Paper.pdf*

- **Renewal requirements:** As the Scheme contains numerous continuous disclosure requirements and requires entities applying to be accredited to provide a holistic view of how their data, security and privacy controls work within the organisation, there is a level of certainty with which Data Custodians can continue to provide data on an ongoing basis. Our view is that Accredited Data Service Providers and Accredited Users should only be required to renew every 5 years. This will allow the harmonisation and streamlining of application processes as part of that renewal (e.g., organisations that are accredited for both types can apply at the same time to renew both).

Further, the NDC has provided a draft Data Sharing Agreement template which will be used to ensure consistency of contracting across different Data Custodians[14]. In consideration of the draft template, we make the following comments:

- **Clarification on whether sub-contractors or suppliers of Accredited Data Service Providers or Accredited Users are covered under the Data Sharing Agreement:** The draft template makes reference at Clauses 4.4, 4.6 and 4.7 to 'intermediaries' in relation to the provision of government data and the circumstances where a user may share data. Considering many government services use third parties (e.g., software vendors to deliver technology solutions, sub-contractors who work for the service provider) it may be impracticable to request that these entities accredit themselves (particularly if they are small entities that offer niche or tailored solutions or services to an Accredited Data Service Provider or Accredited User). Currently, many services provided to government rely on the quick onboarding and utilisation of sub-contractors or technology suppliers. Requiring each sub-contractor or supplier to go through the accreditation process and/or be party to a Data Sharing Agreement may lead to an unnecessary administrative burden and decrease the speed and efficiency with which technology and capability can be utilised when providing these services to government as an Accredited Data Service Provider or Accredited User. There should be consideration given to how these kinds of arrangements are considered as part of the scheme and whether this is specifically called out under the draft template.
- **Confirmation on boundary of consent in Data Sharing Agreement:** We note that Clause 4.2 of the draft template references a consideration to consent, however during a project, individuals may revoke consent or the basis for the consent may change as additional data is collected and disseminated by the Data Custodian. There should be a mechanism in the contract for allowing and requiring continuous disclosure to the Accredited Data Service Providers and Accredited Users to ensure the data quality and basis for consent is still valid.

Recommendation 6.1: *Entities acting under an Accredited Data Service Provider or Accredited User should not be required to accredit separately*

To create a frictionless compliance framework at an organisation, it should be the organisation's obligation to ensure that they have employed or contracted individuals or entities with the required data skills and capabilities and continue to have oversight of the data activities that those individuals/entities undertake whilst providing the services to government. In addition, this allows for a holistic view of where capability exists within an organisation without relying on individuals/subcontracted entities to demonstrate a broad skillset in relation to data for accreditation purposes or prove governance and administrative arrangements where part of a larger entity structure. Attestation processes could be created to ensure that the organisation has required capabilities working on data projects to submit to the NDC's training requirements and that across a team there are sufficient data capabilities.

[14] Available at *https://www.datacommissioner.gov.au/resources/draft-data-sharing-agreement-template*

Recommendation 6.2: *There should be a Transition Period for Current Government Data Service Providers to enable them to continue to deliver their services while the Scheme comes into effect and applications for accreditation are being processed*

While the Scheme comes into effect and applications for accreditation are being processed, relief should be provided to current government data service providers to allow the continuation of the provision of these vital services to government. The relief period should be made clear and should have a particular end date to provide certainty to entities applying under the scheme that their application will be finalised by that date.

Recommendation 6.3*: The Renewal period should be every 5+ years for Accreditation with the Scheme*

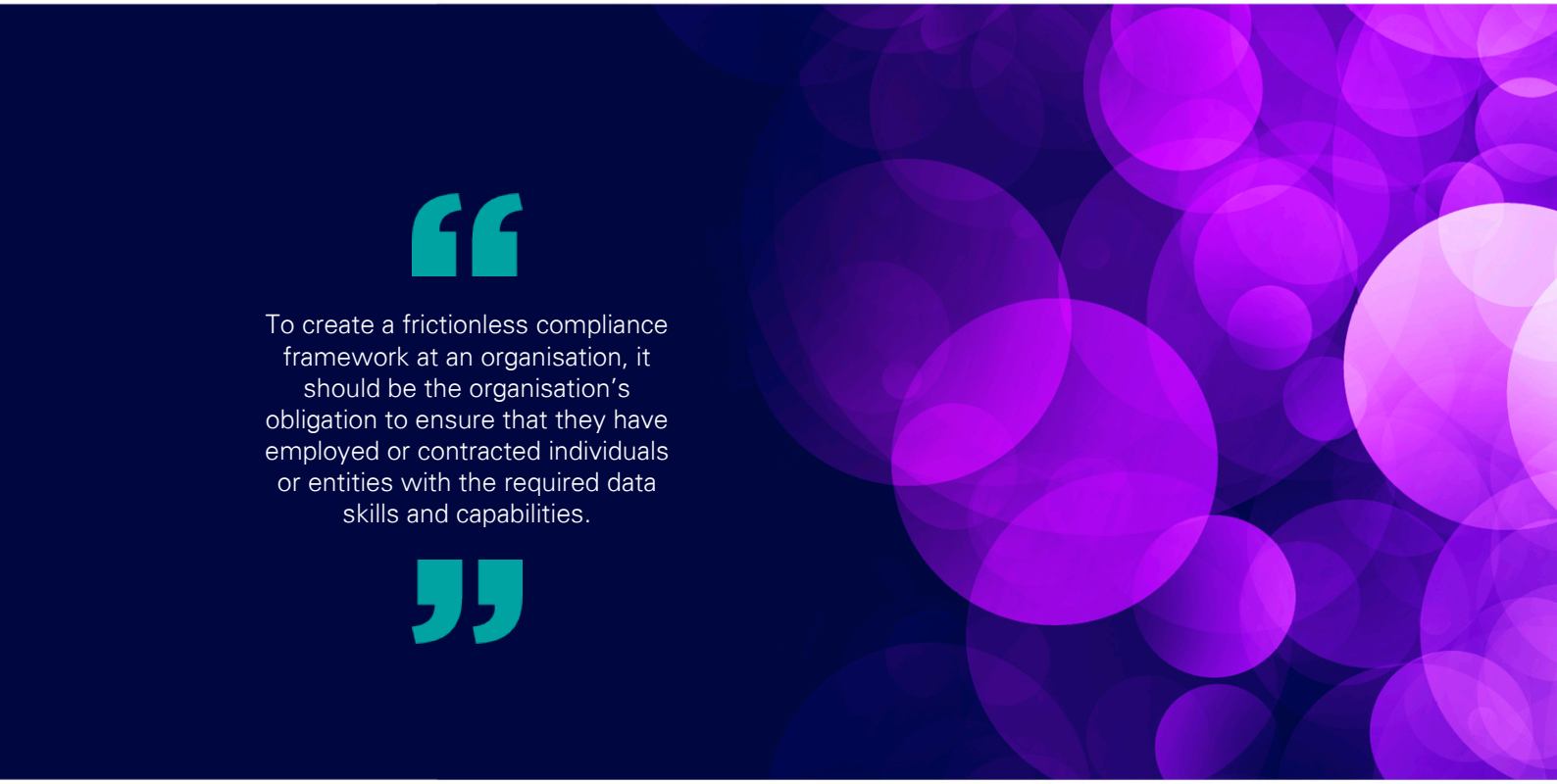
To decrease the compliance burden on Accredited Data Service Providers and Accredited Users that comply with their continuing disclosure obligations, renewals for both types of accreditations should be harmonised to a standard of every five years or more.

Recommendation 6.4: *Ensure that there is consistency in the use of the Data Sharing Agreement Template through National Data Commissioner oversight and review*

To ensure a standardised and streamlined process for each project that requires government data, there should be oversight from the NDC on the use and detail contained in each Data Sharing Agreement Template. For example, if a Data Custodian consistently pushes obligations to manage data breach response to Accredited Data Service Providers / Accredited Users or consistently skips over the confirmation of consent to share and use the data, there should be a mechanism to ensure that this is challenged and rectified.

Recommendation 6.5: *Sub-contractors or suppliers to Accredited Data Service Providers or Accredited Users as part of delivering services to Data Custodians etc should be specifically considered as part of the Data Sharing Agreement and should not be required to accredit separately*

Unless sub-contractors or suppliers are providing services directly to Data Custodians or directly collecting the data on behalf of an Accredited Data Service Provider or Accredited User, they should not be required to separately accredit themselves. When they provide services to an Accredited Data Service Provider or Accredited User, this should be considered in the Data Sharing Agreement with obligations resting on the parties to ensure that the Data Sharing Agreement obligations are adhered to in the use of government data as part of the services provided. This would give more weight to the Data Sharing Agreement as the prime source of obligation and create impetus for all sub-contractors or suppliers being considered by an Accredited Data Service Provider or Accredited User to be disclosed before the data is shared (rather than through separate agreements and accreditation processes).



***Recommendation 6.6**: The Consent Disclosure Requirements in the Data Sharing Agreement should be broadened to include ongoing monitoring and reporting on consent to ADSPs and accredited users*

The draft template should be updated to include ongoing disclosure requirements on Data Custodians where consent of an individual is revoked, modified or otherwise ineffective to ensure that the data quality and basis for data handling is preserved. This should be considered as part of the Data Sharing Agreement as the responsibility of the Data Custodian.

Recommendation 6.7: *There are certain elements of data capability that we recommend should be captured in order to understand an accredited entity's ability to keep data safe, including labelling and tagging of data, as well as encryption or some form of protection.*

Data is quite obviously at the heart of this Scheme, as it is in all information systems. Processes, processors, actions, transformations all act on data. The protection of data, rather than the protection of data processes or access controls, is the ultimate focus of cyber security. All data elements that governments hold must be protected at all costs and only disclosed under the appropriate circumstances and with appropriate authorisation.

To ensure that the accreditation framework addresses this appropriately, there are certain elements of data capability that we recommend should be captured in order to understand an accredited entity's ability to keep data safe. These include whether the entity utilises labelling and tagging of data, as well having the ability to receive encrypted data, store encrypted data, and handle data encryption or provide some form of data protection (such as air-gapping networks and not allowing USB or data exfiltration). The mantra in industry for some time has been encrypt by default. Consideration should further be given to an encrypted data handling scheme, such as tagging and labelling the encrypted data, so that systems can understand what is within the encrypted packet, and then whether further controls are then required to protect the encrypted data. Fundamental controls such as Data Loss Prevention (DLP) – preventing the propagation of data, Rights Management – preventing and controlling access to data, coupled with the above encryption methods must be considered within the accreditation framework.

7. Data Quality

Given the importance and critical role of data quality in the success of its applications we suggest following considerations in the context of the Bill.

Data quality as an anchor of trustworthy and ethical management, sharing and use of data: our research in data trust[15] shows how limitations in the quality and integrity of data still represent an area of concern and continuous investment for C-suites, Chief Information Officers and Chief Data Officers in public and private organisations. The quality of data has a direct and significant impact in the integrity and reliability of outcomes and decisions made based on that. Data driven solutions can easily scale up many existing processes and bring benefits of accuracy and speed. However, they may also replicate and expand any existing quality issues like discrimination or unfair representation, especially when shared and used in a new context. In the context of the Bill, the opportunities presented by the modernisation of government data sharing and use can be significantly undermined by immature and/or inconsistent data quality practices that may result in poor, incorrect or unfair outcomes affecting the public.

Importance of accountability and context for the data quality: In addition to its criticality in generating trustworthy results, the data quality is a technical and in situations complex topic. To ensure any relevant risks are minimised, in a data sharing framework the accountability for the data quality should be very clear. Additionally, in a realistic environment the quality of any data set is contextual and closely relates to where and how the data is going to be used. The entities who collect the data in the first place are usually best positioned and should be responsible to provide thorough quality checks of the raw data and the context in which it has been collected and assessed. Keeping such metadata together with the datasets while being shared and through their lifecycle will help in managing the quality risks and keeping it transparent.

Overall, we recommend to:

Recommendation 7.1: *Embed data quality requirements in the accreditation framework to make sure users of the data have the right capability to understand the quality implications and use it in the right context based on the provided metadata*

To broaden the scope of section 74 of the Data Availability and Transparency Bill to include data quality accreditation criteria, covering - as a minimum - standards on data coverage and representativeness, provenance and traceability, metadata, and how the data has been generated. This approach is aligned with the data ethics and trust frameworks developed in other jurisdictions – e.g. the United Kingdom [16]- designed to guide the adoption of appropriate and trustworthy data use in the public sector.

Recommendation 7.2: *Data Custodians should be accountable for the data quality within the context and manage it through the data sharing agreement*

It is the responsibility of the data custodians who collect the data to clearly define the context and assess the quality within that context. This information should be accompanied with the data when being shared and clarified in the data sharing agreement specially regarding the context

[15] Guardians of Trust, KPMG, 2018: https://assets.kpmg/content/dam/kpmg/xx/pdf/2018/02/guardians-of-trust.pdf

[16] United Kingdom – Data ethics workbook: https://www.gov.uk/government/publications/data-ethics-framework

that the data may be used. The responsibility of the subsequent processed data quality generated by the accredited users will be with those respected users.

8. Resourcing and training

The Bill places additional workload on data custodians and accredited users to comply with its requirements, as well as on the Office of the National Data Commissioner (ONDC) to accredit users and data service providers and provide oversight of the scheme. Moreover, ONDC has a significant role in education and promotion of good data practices.

KPMG welcomes the announcement in the 2020-21 Budget that the Government will provide $39.2 million over four years to the Department of the Prime Minister and Cabinet to support the Government's policy priorities, including its COVID-19 response and establishing ICT systems for the Office of the National Data Commissioner to regulate public sector data sharing and release[17]. Moreover, the Government's commitment to uplift the Data Professional Stream to further source, grow and mobilise data expertise across the APS is highly commendable. This initiative will further contribute to the responsible use of data for better policy advice, regulation and services.

While the supporting consultation paper and documentation, e.g. best practice guide[18][19] and accreditation framework[20], are silent about the resources required to implement these requirements, the funding in the Budget is welcome.

This funding commitment is important given that experience with other schemes requiring similar government oversight and/or accreditation is that a lack of resources or inadequately trained resources is a significant contributor to inefficiencies in such schemes. Consideration should be given to identifying the resources required (roles, skills) to implement the data sharing scheme and to track the performance of relevant organisations against this requirement.

Overall, we recommend:

Recommendation 8.1: *KPIs should be established to track any shortfalls in resources (numbers, skills) of organisations involved in the data sharing scheme.*

[17] https://budget.gov.au/2020-21/content/bp2/download/bp2_complete.pdf

[18] https://budget.gov.au/2020-21/content/bp4/download/bp4_02_preface.doc

[19] https://www.datacommissioner.gov.au/sites/default/files/2019-08/data-sharing-principles-best-practice-guide-15-mar-2019.pdf

[20] https://www.datacommissioner.gov.au/sites/default/files/2020-09/Accreditation%20Framework%20Discussion%20Paper.pdf

Key contact

Dr. Sanjay Mazumdar
Chief Data Officer & Partner
KPMG Australia
+61 478 403 462
skmazumdar@kpmg.com.au

Co-authors

Rossana Bianchi
Associate Director,
Data and AI Ethics Lead

Veronica Scott
Director, Privacy, Technology
& Data Protection, KPMG Law

Sophie Finemore
Associate Director, Regulatory Affairs

Dr. Ali Akbari
Director, AI Capability Lead

Robert Griffiths
Manager, KPMG Law

John Jordan
Senior Compliance Analyst

Paolo Redecilla
Associate Director, Data Privacy

Dr. Steven Robertson
Associate Director, Data Privacy

Ian Gray
Partner, Cyber Security Services

Matthew Quick
Director, Technology Risk

KPMG.com.au