KPMG

Australian Data Strategy

KPMG Submission

July 2022

Contents

01

Executive Summary

Executive Summary

KPMG Australia (KPMG) welcomes the opportunity to provide a submission to the Department of Prime Minister and Cabinet's Australian Data Strategy (the strategy).

KATE MARSHALL
Head of KPMG Law
KPMG Australia

MARTIJN VERBREE
Partner, Technology Risk & Cyber
KPMG Australia

KPMG supports the Australian Government's ambition to position Australia as a leading digital economy and society by 2030 and commends the government on taking steps to achieve this through the Digital Economy Strategy, Digital Government Strategy, and now the Australian Data Strategy.

As outlined in the strategy, data is critical to achieving this ambition and a mature data ecosystem will deliver significant benefits for people, businesses and governments. It is critical that the right settings are in place to both unlock the value that data offers while ensuring appropriate safeguards are in place to prevent its misuse and potential harm.

In this response, KPMG has drawn on work from previous submissions to various forums including the Review of the Privacy Act, the Data Availability and Transparency Bill 2020, and most recently the Digital Technology Taskforce's consultation on Artificial Intelligence and Automated Decision Making Regulation.

KPMG notes the complexity of legislation that can apply to digital technologies and data, as well as various reforms that are currently underway. Entities must currently manage and comply with a range of data-related regulatory requirements that exist in overlapping and in some cases fragmented frameworks at both a state and federal level. In our view it is critical to carefully consider how legislation or regulation interacts with existing and proposed frameworks in order to minimise complexity, overlap and unnecessary regulatory burden.

If you would like to discuss the contents of this submission further, please do not hesitate to reach out. KPMG looks forward to continued engagement with the Department of Prime Minister and Cabinet as it seeks to finalise the strategy.

Background

About KPMG

KPMG is a global organisation of independent professional firms, providing a full range of services to organisations across a wide range of industries, governments and not-for-profit sectors. We operate in 146 countries and territories and have more than 227,000 people working in member firms around the world. In Australia, KPMG has a long tradition of professionalism and integrity combined with our dynamic approach to advising clients in a digital-driven world.

02

Findings

KPMG Findings

1

Recommendation 1

It is important to consider how the wide range of existing legislation and policies that regulate data align, interact and overlap with each other in order to create the right settings to facilitate a modern and mature data ecosystem.

2

Recommendation 2

KPMG is supportive of the Commonwealth public sector data sharing scheme given the significant benefits from the ability of government departments and agencies to share and access each other's data.

3

Recommendation 3

KPMG considers that in implementing the Data Availability and Transparency Act, there is an opportunity to develop a robust, consistent and clear national framework that addresses overlapping Commonwealth, State, and Territory privacy and data protection frameworks and learnings from other data schemes.

4

Recommendation 4

KPMG considers that there is a need to develop a multidimensional capability to anticipate and respond to systemic risks that widespread data availability may create.

5

Recommendation 5

Entities currently must manage and comply with a range of data-related regulatory requirements. The complexity of legislation in this area, both existing and proposed, should be addressed in order to help governments, consumers and organisations manage within a modern data economy.

6

Recommendation 6

KPMG considers that there are a significant number of existing data sets and it would be beneficial to create an inventory of public/government data assets in order to improve accessibility. Further to this, different data assets may require different treatment and safeguards depending on the sensitivity of the data.

7

Recommendation 7

In relation to overseas data flows, KPMG considers that APP8.2 exceptions and how they can effectively support cross-border transfers as part of the scheme should be given further consideration. In particular, an equivalency mechanism similar to the adequacy mechanism under GDPR would provide certainty and reduce burdens on business, without introducing any impact on individuals.

8

Recommendation 8

Effective data management is fundamental to the successful implementation of the strategy and plays a key role enabling the potential value of data and managing data risk.

9

Recommendation 9

KPMG considers that investment in data management is essential for creating a trustworthy data ecosystem. Such investment must be considered through the entire lifecycle of creation, collection, validation, verification, storage, curation, enrichment, processing and analysis, access and sharing, and deletion.

03

KPMG Insights

KPMG Insights

1. Introduction

Data is a critical asset that can offer significant opportunities and value to people, businesses and governments. To realise these opportunities, Australia must ensure the effective, safe, ethical and secure use of data through the right legislative and regulatory settings.

Privacy and consumer rights are converging and new cyber, digital and data laws are being developed, both in Australia and overseas. We note the wide range of existing legislation, strategies, policies and reviews that regulate data that are outlined in the strategy, including: the Privacy Act 1988; the Freedom of Information Act 1982; the Data Availability and Transparency Act 2022; the 2015 Public Data Policy Statement; the Digital Economy Strategy; the Cyber Security Strategy; the Productivity Commission's 2017 Inquiry into Data Availability and Use; and the Consumer Data Right.

It is imperative to consider how these frameworks align, interact and overlap with each other in order to create the right settings to facilitate a modern and mature data ecosystem.

In this submission KPMG provides insights on the key themes identified in the strategy, including maximising the value of data; trust and protection; and enabling data use.

Finding 1
It is important to consider how the wide range of existing legislation and policies that regulate data align, interact and overlap with each other in order to create the right settings to facilitate a modern and mature data ecosystem.

2. Maximising the value of data

Making data available

KPMG strongly supports data sharing arrangements such as the *Data Availability and Transparency Act 2022* (Cth) and the *Data Sharing (Government Sector) Act 2015* (NSW) 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.[1]

KPMG is supportive of public sector data sharing schemes 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.

KPMG considers that in implementing the Data Availability and Transparency Scheme, there is an opportunity to develop a robust, consistent and clear national framework that addresses overlapping Commonwealth, State, and Territory privacy and data protection frameworks and learnings from other data schemes.

KPMG also acknowledges the evolution of data that may occur when more data becomes publicly available. It will be important for the Commonwealth Government to consider how data may evolve and what safeguards may be required. We note that the Privacy Act, Consumer Data Right (CDR) and Data Availability and Transparency Act provide a foundational level of protection for personal information. We also note the actions outlined in the government's Cyber Security Strategy 2020 to protect the confidentiality, availability and integrity of Australian data.[2]

[1] https://home.kpmg/au/en/home/insights/2020/11/data-availability-transparency-bill-2020-kpmg-submission.html

[2] https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/australia%E2%80%99s-cyber-security-strategy-2020

Systemic risk

Reducing silos and sharing data certainly offers significant benefits. However, it must be acknowledged that this also presents real risks of harm in two important ways.

First, widespread access to data has the potential to magnify existing systemic flaws by both accelerating the speed and capacity by which mismanagement or maladministration can cause harm, and by creating potentially dangerous feedback loops in decision making processes. For example, in the administrative law context, this has been demonstrated by the inappropriate deployment of Automated Decision Making in the administration of welfare. This has highlighted existing shortcomings of many of the legal safeguards that administrative law provides.

Secondly, malicious actors may be able to identify and exploit previously unknown systemic vulnerabilities latent in large amounts of data. An example of this can be seen in the recent proliferation of misinformation and disinformation in public discourse. This has been made possible by the manipulation of large, newly accessible data sets created by social media platforms. This has resulted in exacerbating existing social fault lines, aggravated political polarisation, and the erosion of trust in important democratic and rule of law institutions.

These risks should not be seen as a reason not to share data. Rather, the benefits of data sharing need to be embraced while remaining aware of the risks. Moreover, the risks described are social risks and so it is highly unlikely that there will be a technical solution to these problems. KPMG's view is that such risks are best anticipated and responded to in a multidimensional and interdisciplinary manner which could include, among other things, well-resourced public and private research capabilities that allow for sophisticated insight into potential and emerging threats.

Finding 2
KPMG is supportive of the Commonwealth public sector data sharing scheme given the significant benefits from the ability of government departments and agencies to share and access each other's data.

Finding 3
KPMG considers that in implementing the Data Availability and Transparency Act, there is an opportunity to develop a robust, consistent and clear national framework that addresses overlapping Commonwealth, State, and Territory privacy and data protection frameworks and learnings from other data schemes.

Finding 4
KPMG considers that there is a need to develop a multidimensional capability to anticipate and respond to systemic risks that widespread data availability may create.

3. Trust and protection

Setting guardrails for a modern data economy

Entities currently must manage and comply with a range of data-related regulatory requirements that exist in overlapping and in some cases fragmented frameworks at both a State and Federal level. The complexity of legislation in this area, both existing and proposed, should be addressed in order to help governments, consumers and organisations manage within a modern data economy.

KPMG notes the work being undertaken by the Digital Technology Taskforce regarding the regulation of Artificial Intelligence (AI) and Automated Decision Making (ADM). While discrete topics, it is difficult to separate questions concerning regulatory settings for AI and ADM from a broader data strategy. Data is fundamental to complex algorithmic processes including both AI and ADM.

KPMG also acknowledges that a Review of the Privacy Act is underway, which will play an important role in providing protections for robust and modern cyber security and privacy settings. KPMG welcomed the opportunity to provide a submission to this Review, noting the importance of the Privacy Act as the central modern privacy law for Australia which plays a key role in protecting consumers and their data.[3]

As per KPMG's submission to the Review, KPMG supports the continued broad objects of the Privacy Act and believes that care should be taken to avoid narrowing, even unintentionally, the objects in an attempt to address perceived limitations. Clearly defined concepts and rules, that are interoperable and are supported by the regulatory tools of code-making, guidance and advice, together with a strong regulator, should be preferred as the most effective means for enabling compliance and be assessed as part of a comprehensive Regulatory Impact Statement process.

In light of the government's ongoing consultations and reviews in this area, there is an opportunity to carefully consider how legislative interventions can be harmonised with each other, as well as with other recent legislative initiatives such as the recent expansion of the Security of Critical Infrastructure Act regime.

KPMG makes two points in this respect. While adequate protection of privacy rights is undoubtedly necessary, it is not sufficient. The Australian Data Strategy must ensure adequate resourcing and the right regulatory settings to enable Australia to preserve the confidentiality, integrity and availability of its data. Furthermore, there are significant opportunities to learn from measures and strategies that have been proposed and adopted both in Australian states and internationally. In particular, the European Union (EU), United Kingdom (UK) and Canada have data and AI strategies that are well advanced.

Other existing legislation that can apply to data includes the Australian Consumer Law, anti-discrimination laws, and surveillance devices legislation. KPMG considers that when considering how to achieve robust and modern cyber security and privacy settings, the Commonwealth Government should endeavour to consider how existing regulatory frameworks and legislation in this area interacts and overlaps in order to both reduce complexity and achieve appropriate protections.

Finding 5

Entities currently must manage and comply with a range of data-related regulatory requirements. The complexity of legislation in this area, both existing and proposed, should be addressed in order to help governments, consumers and organisations manage within a modern data economy.

[3] https://home.kpmg/au/en/home/insights/2022/01/review-privacy-act-1988-kpmg-submission.html

4. Enabling data use

Creating the right infrastructure

Data assets

We note that the government is taking action to improve how data assets are managed and secured, including developing the right data sets the country needs. KPMG considers that there are a significant number of existing data sets and it would be beneficial to create an inventory of public/government data assets in order to improve accessibility. Further to this, different data assets may require different treatment and safeguards depending on the sensitivity of the data, and this exercise could also include classifying assets accordingly.

Overseas data flows

In relation to overseas data flows, and specifically APP8.2, we note the following from KPMG's submission to the Review of the Privacy Act.

The effectiveness of the APP8.2(a) and (b) exceptions do raise some challenges. In order to rely on these exceptions, an entity must undertake an assessment of the protections afforded by a jurisdiction in which the overseas recipient is located, and such an undertaking can be extremely burdensome on the entity (and potentially duplicates work done by similar entities). Australia does not provide any certainty through an equivalency mechanism or process that recognises the adequacy of overseas privacy laws that are similar to the European Commission's adequacy decision-making process for the General Data Protection Regulation (GDPR). This can result in an ad-hoc approach to reliance on the jurisdiction exception or it is otherwise considered as part of the APP8.1 assessment.

The requirements for obtaining valid consent for the purposes of relying on APP8.2(b) means its application is potentially very limited save in some very specific cases, otherwise the validity of the consent is uncertain.

We suggest that these APP8.2 exceptions and how they can effectively support cross-border transfers as part of the scheme should be given further consideration. In particular, an equivalency mechanism similar to the adequacy mechanism under GDPR would provide certainty and reduce burdens on business, without introducing any impact on individuals.

Additionally, existing "follow-the-sun" support models mean technology platforms utilise global support teams to provide 24-hour service. As a result, personal information may well be accessed or transferred through a number of jurisdictions. There is certainly an opportunity to review and consider ways in which organisations can provide greater confidence to individuals that their information is being handled in a consistent manner.

KPMG also supports the adoption of a model similar to the European Union's Standard Contractual Clauses (SCC) model that's fit for purpose in Australia, which includes standard binding terms that entities can enter into with overseas recipients on the basis of which data transfers would be permitted. In adopting this model, it is important to give individuals appropriate rights and ensure that personal information is handled consistently with the Australian Privacy Principles (APPs) and applicable codes.

KPMG is conscious of the role of Australian business as data importers and data processors. Such businesses usually need to be able to comply with the local privacy and data protection laws of the data exporter. This is particularly the case under the EU's GDPR. The Court of Justice of the European Union's (CJEU) *Schrems II* judgment has had made legally compliant third country data transfers to Australia more onerous. The Australian Data Strategy should take steps to reduce undue burden in this regard by seeking to bring local privacy protections into alignment with international standards.

Moreover, KPMG notes that while the CJEU did not have call to assess Australian security legislation, the United States (US) Government powers that were of concern to the CJEU in *Schrems II* are similar to powers accorded to the Australian Intelligence Community under, for example, the *Telecommunications Interception Act* and Division 7 of Part 15 of the *Telecommunications Act 1997*. The Australian Government may wish to take this opportunity to implement oversight and safeguard mechanisms along the lines of those recommended by the Parliamentary Joint Committee on Intelligence and Security and the Independent National Security Legislation Monitor.

Cross border privacy rules

The APEC Cross-Border Privacy Rules (CBPR) has not yet been introduced. This system is a government-backed data privacy certification that companies can join to demonstrate compliance with internationally recognised data privacy protections. The CBPR System implements the PEC Privacy Framework endorsed by APEC Leaders in 2005 and updated in 2015. Any further take-up or endorsement of the CBPR should be carefully considered in the context of the overall objective and net benefits.

Finding 6

KPMG considers that there are a significant number of existing data sets and it would be beneficial to create an inventory of public/government data assets in order to improve accessibility. Further to this, different data assets may require different treatment and safeguards depending on the sensitivity of the data.

Finding 7

In relation to overseas data flows, KPMG considers that APP8.2 exceptions and how they can effectively support cross-border transfers as part of the scheme should be given further consideration. In particular, an equivalency mechanism similar to the adequacy mechanism under GDPR would provide certainty and reduce burdens on business, without introducing any impact on individuals.

Building a modern data system

Effective data management

The successful implementation of the Australian Data Strategy will rely on effective data management practices. KPMG's experience is that data management is fundamental across the four high level actions outlined in the strategy: making data available; setting guardrails for a modern data economy; creating the infrastructure we need; and building a modern data system.

The draft strategy states that the end goal of data management is to support decision-making to enable entities to meet their strategy, goals and objectives. KPMG's view is that the purpose of data management is broader; it is not simply about supporting decision-making, it is about enabling the potential value of data and managing data risk. This view is supported in the DAMA Data Management Body of Knowledge (DMBoK): "The primary driver for data management is to enable organisations to get value from their data assets". [4]

The strategy outlines data management's role in ensuring that public data is safely and securely collected and managed to ensure trust is maintained and data is of high quality. While these are important outcomes of good data management, there are additional reasons to emphasise the need for more mature data management capability, for example:

- The adoption of transparent and consistent metadata management would help streamline data sharing and improve data quality during times when data sharing, integration and reporting is time critical (e.g., national crises such as the COVID-19 pandemic).
- Developing standards to support data interoperability allows for data and information to be shared and exchanged more seamlessly. This is consistent with the National Digital Health Strategy, which highlights the importance of data interoperability to improve patient outcomes and facilitate data sharing across multiple systems and sources for healthcare providers.

[4] https://www.dama.org/cpages/body-of-knowledge

In a *Recommendation of the Council on Enhancing Access to and Sharing of Data*, adopted by the OECD in 2021, the OECD recognised the wide range of benefits that can come from greater data access and sharing, such as collaboration, data-driven scientific discovery and innovations.[5] However it also recognised that the data management required to support this will require substantial investments over time.

KPMG's experience supports this view, recommending the need to establish public data standards to facilitate data consistency and interoperability. KPMG considers that investment in data management is essential for creating a trustworthy data ecosystem. Such investment must be considered through the entire lifecycle of creation, collection, validation, verification, storage, curation, enrichment, processing and analysis, access and sharing, and deletion.

The adoption of digital technologies accelerated during the COVID-19 pandemic. This has changed the way society uses services, and is fuelled by data consumption and production. KPMG believes there is significant opportunity for government to extract greater insights and deliver more effective outcomes by using data, collected both from within government and from non-government organisations. The concept of "frictionless and integrated" service delivery, outlined as an objective in the Australian Digital Economy Strategy, can only be realised when data is integrated, interoperable and collectively leveraged.

The COVID-19 pandemic drove greater global sharing and collaboration of research data, accelerating the pace of research to combat the disease. One example includes the tremendous achievement of sharing the full genome of the novel coronavirus in open access, less than a month after the first COVID-19 patient was admitted to a Wuhan hospital.[6] Such achievements would not have been possible without open data policies, which, as a result, are being increasingly adopted internationally to remove obstacles to the flow of research data and ideas.

Open science and its ability to rapidly address health and other issues is just one use-case that demonstrates how open data collaboration can benefit society. Continuing to reduce barriers to data collaboration, both within government and across other sectors will be essential to facilitate ongoing data-driven innovation.

Finding 8
Effective data management is fundamental to the successful implementation of the strategy and plays a key role enabling the potential value of data and managing data risk.

Finding 9
KPMG considers that investment in data management is essential for creating a trustworthy data ecosystem. Such investment must be considered through the entire lifecycle of creation, collection, validation, verification, storage, curation, enrichment, processing and analysis, access and sharing, and deletion.

[5] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0463

[6] OECD (2021). Source: https://express.adobe.com/page/wt6Xz7XVVX91k/

04 Key Authors

Key Authors

KATE MARSHALL
Head of KPMG Law
KPMG Australia

PAOLA REDECILLA
Associate Director, Compliance & Conduct
Privacy & Data Protection
KPMG Australia

MARTIJN VERBREE
Partner
Technology Risk & Cyber Security
KPMG Australia

DIANE TSUJI
Associate Director
Audit Assurance & Risk Consulting
KPMG Australia

KELLY HENNEY
Compliance & Conduct Leader
Privacy & Data Protection
KPMG Australia

NATHAN JAMISON
Associate Director
Audit Assurance & Risk Consulting
KPMG Australia

MARK GEELS
Partner
Audit Assurance & Risk Consulting
KPMG Australia

SAM HARTRIDGE
Senior Manager
KPMG Law
KPMG Australia

VERONICA SCOTT
Cyber, Privacy & Data Lead
KPMG Law
KPMG Australia

NAVEEN MALHOTRA
Manager, Compliance & Conduct
Privacy & Data Protection
KPMG Australia

SHUBHAM SINGHAL
Director, Compliance & Conduct
Privacy & Data Protection
KPMG Australia

STEPHEN CHEN
Senior Consultant
Audit Assurance & Risk Consulting
KPMG Australia

DOMINIKA ZERBE
Director, Cyber Growth National
Execution Lead
KPMG Australia

OLIVIA SPURIO
Senior Consultant
Corporate Affairs
KPMG Australia

KPMG.com.au

July 2022. 927437848CORPS