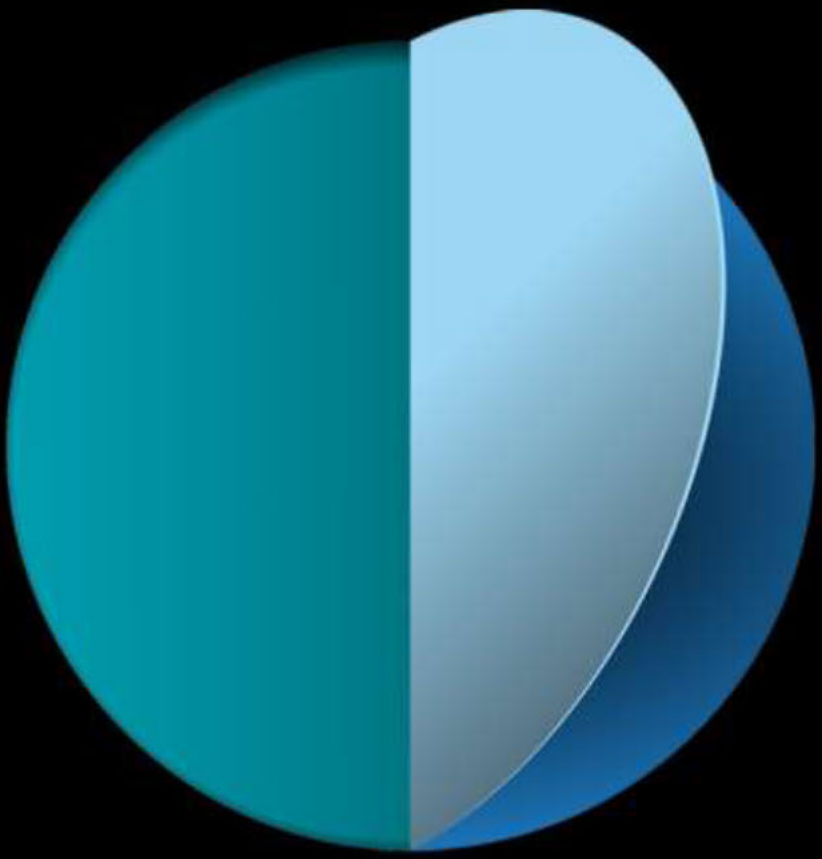
Deloitte.



Data Sharing and Release Legislative Reform Discussion Paper

Deloitte Submission

October 2019

Contents

Executive summary

Deloitte is pleased to provide observations on the Data Sharing and Release Legislative Reforms Discussion Paper, September 2019.

We strongly support the implementation of federal Data Sharing and Release (DS&R) legislation and the development of a consistent national data sharing and release framework so Australia can meet the original vision of the Australian Government to 'unlock the full potential of public sector data'.

We acknowledge the pragmatic approach taken to build out the rules in a rapidly evolving technology landscape, and the decision to establish both the Consumer Data Right and the Data Sharing & Release acts based on the recommendations of the Productivity Commission.

Deloitte supports the overarching principles and objectives set out in the discussion paper and our submission includes comments on each of the sections it contains.

There are some common themes that emerge in our submission.

Firstly, open data is not a binary choice between closed and open data. This is acknowledged in the discussion paper. However, the discussion paper proposes that the DS&R legislation will only focus on data sharing, noting that current mechanisms for open data release are sufficient.

Deloitte do not support this. Data openness is a continuum. Deloitte believe that the legislative framework for open data in Government, should recognise this continuum and include specific legislative reforms to enhance both open data release and data sharing in the public sector. This should also include the release of citizens' data to citizens, based on a similar framework to that set out in the Consumer Data Right legislation. If the DS&R legislation does not reflect this data openness continuum, it will not meet the aspiration to unlock the full potential of public sector data.

Secondly, effective implementation is necessary, and indeed critical, if government and society are to realise the benefits of open data sharing and release. The discussion paper highlights that while there are pockets of excellence, data practices need to be improved across all departments.

While guard rails and guidelines for data sharing are important, there is a risk that the prescriptive requirements for detailed descriptions that are proposed for Data Sharing Agreements will become another barrier to open data in the public sector. It is not clear that what is proposed will result in a clear, consistent and transparent approach to data sharing. In addition, Deloitte believes that the current mechanisms for open data release are not enough and could be improved by inclusion of open data release in the DS&R legislation.

We also recommend transparent policies, processes and systems along with enough funding and education be provided such that the DS&R can achieve the educational and behavioural transformation intended. Adequate funding is needed to ensure that data assets are identified, to enhance the skill sets and the capability in the public sector for sharing and using data, and to create a secure environment for data sharing and release.

Thirdly, accountability of all actors in data sharing is important – Data Custodians, Accredited Data Users and Accredited Data Service Providers, as well as the National Data Commissioner. The data sharing safeguards are important, as is accountability of organisations sharing and receiving data. Accountability enhances trust, and trust is a foundation for data sharing. However, the graduated approach to enforcement under the DS&R legislation is appropriate given it is seeking to achieve a paradigm shift in the culture of the Australian public service to data sharing and release to 'responsibility to share'.

Deloitte supports the inclusion of safeguards within the proposed legislation, however, clear guidance for participants should be developed to prevent the safeguards becoming barriers to achieving the legislation's purposes. Deloitte agrees that Data Sharing Agreements will be important for defining and publicising data

sharing arrangements but notes it will be important that the detail required, and purpose test thresholds do not present a new barrier to participating in data sharing.

Fourthly, we support the intention to appoint a National Data Commissioner. The independence given to the statutory authority for this office is significant and essential. However, the mandate of the Commissioner to simultaneously advocate, regulate and oversee risks compromising the effectiveness of this role.

Finally, allowing private sector entities to become Accredited Data Users is important if we are to unlock the full potential of public sector data. There is an important role for Government in educating the community about the potential benefits of data sharing and release with the private sector, and a danger in allowing policy to be determined by the sum of the community's fears.

1 Introduction

A decade ago, a key focus of government pertaining to data was how to make it more open and easily accessible to the public. Ten years later, with thousands of open government data sets worldwide, the discussion has evolved and become more nuanced. Governments are considering their role in overseeing the types and validity of the data they make available, seeking ways to create greater public value from data, and debating how best to protect privacy and govern data use.[1]

Australia has gone on a similar journey, starting with some steps towards open data, and now exploring how to 'unlock the full potential of public sector data' within a framework for data sharing and with clear privacy protections.

On 1 May 2018, the Australian Government released its final response to the Productivity Commission's Inquiry into Data Availability and Use. The Government committed to reforming data governance to better realise the economic and social benefits of increased data use while maintaining public trust and confidence in the system.[2] Underpinning this reform in the public sector will be the new Data Sharing and Release Act (DS&R Act) which has the following principles:

- Sharing data for appropriate and authorised purposes.
- Sharing data only with authorised users.
- Using data in a safe and secure environment.
- Applying appropriate protections to the data.
- Ensuring public outputs from data sharing projects do not identify the people or organisations in the data.[3]

In addition to these principles, the discussion paper outlines several objectives for the data sharing and release legislation. These include:

- Establishing enhanced safeguards, privacy and security protections.[4]
- Developing a clear, consistent and transparent approach to sharing public sector data.[5]
- Modernising how public sector data is used.[6]
- Unlocking the full potential of public sector data.[7]

Our response to the discussion paper includes comments on:

- The regulatory framework for DS&R, including the development of national legislation and the operation of sharing and release under the legislation.
- The omission from the scope of the DS&R legislation of the release of citizen data to citizens.
- The framework for sharing data, including comments on private sector usage of shared public sector data.
- The interaction of the DS&R legislation with other legislation.
- The proposed data sharing principles and associated privacy standards and their interaction with the Australian Privacy Principles.

---

[1] Deloitte Centre for Government Insights, *The Chief Data Officer in Government: A CDO Playbook*, 2019. Refer https://www2.deloitte.com/us/en/insights/industry/public-sector/chief-data-officer-government-playbook.html
[2] Department of Prime Minister and Cabinet, *The Australian Government's response to the Productivity Commission Data Availability and Use Inquiry*, 2018. Refer https://dataavailability.pmc.gov.au/sites/default/files/govt-response-pc-dau-inquiry.pdf
[3] Discussion Paper, page 5, Figure 2
[4] Discussion Paper, page I
[5] Discussion Paper, page I
[6] Discussion Paper, page 1
[7] Discussion Paper, page 1

- The role of data sharing agreements.
- The role of the National Data Commissioner.
- Accountability.

In making these comments, we have considered how the proposals set out in the discussion paper contribute to the principles and objectives that the Government have set for the legislation.

References in our submission to the term 'government departments' includes the departments, agencies and authorities that exist within the federal, state and local government ecosystem.

It is important to acknowledge, as the discussion paper does, that the implementation of open data is not without risks. The increase in:

- the amount of data that is shared
- the number of counterparties with which this data is shared

where the data is:

- sourced from systems that were not necessarily built with data sharing in mind
- shared via a new regulatory environment which introduces new obligations on data holders and authorised data recipients

together create a risk of unintended, and potentially unanticipated, adverse consequences.

However, it is equally important, if not more so, to acknowledge that there is a risk that the detailed and specific requirements set out for Data Sharing Agreements reinforce and perpetuate existing cultural biases in the public sector against data sharing and contribute to a narrow interpretation of data which can be shared. The likely result being Australia failing to achieve its aspiration to 'unlock the full potential of public sector data'.

The scope of potential benefits for Australians and the Australian economy is likely to be further enhanced if the scope of DS&R legislation in Australia also includes release of data contributed by citizens to those citizens, and measures to enhance and expand the extent of open data release across the public sector.

Q1. Do you think the distinction between data sharing and data release is clear? How could this distinction be clearer?

The concept that open data can and should be treated separately from other formats of data sharing and release is arbitrary – they should be part of a continuum of data sharing and release rather than binary alternatives. This continuum includes release of citizen data to citizens and open data release.
While the distinction between data sharing and data release is generally clear, we see greater scope for data release than is proposed within the discussion paper. The DS&R legislation should specifically include release of citizen data to citizens and open data release.

2 Data Sharing and Release Framework

Deloitte supports the Data Sharing and Release Framework in principle; however, we have concerns with inconsistencies in the design and language used to describe data sharing and the intention of the legislation.

National Data Commissioner (Section 2.2)

Deloitte supports the establishment of the National Data Commissioner as an independent authority to drive change and support best practice. This will be an important role in achieving the Government's vision of open data, becoming 'one of the next great enablers of modern digital economies and better government'.[8]

The discussion paper highlights the importance of the Australian Public Service culture making the paradigm shift from 'need to know' to 'responsibility to share' where there is a clear public benefit.

We believe that this is an important objective for the legislation and for the Commissioner. As such it is an important benchmark against which the proposals in the discussion paper can be assessed.

However, existing mandates and directives have failed to realise this paradigm change despite it being an intent since the original adoption of data sharing and release in the public sector. This may be, in part, because this ambition is ambiguous and calls for participants to make judgement calls rather than defer to guidelines and rules.

We recommend that the Data Sharing and Release framework consider whether greater and more prescriptive direction and clarity is required to ensure the desired paradigm shift can occur.

The role of the National Data Commissioner is discussed further in section 6.

National Data Advisory Council (Section 2.3)

Deloitte supports the role of the National Data Advisory Council as an advisor to the Commissioner and notes the terms of reference of the Advisory Council.[9] Deloitte also supports the intention of the National Data Commissioner to engage with other experts to seek global best practice and to stay relevant with emerging challenges, technologies and methods to address them.

The role of the Advisory Council would be strengthened if the terms of reference provided greater clarity over the mechanism for member selection, recruitment processes and roles of the committee members. This is particularly the case as the terms of reference note that 'non-government members attend in their individual capacity, based on their skills and understanding of the data ecosystem'.

In addition, the terms of reference omit, and the framework does not comment on, the performance indicators and criteria for assessing the operating effectiveness of the Advisory Council. We recommend that the particulars of the Advisory Council are enhanced and recorded to strengthen the effectiveness of this element of the regulatory framework.

---

[8] Department of the Prime Minister and Cabinet, The Hon. Angus Taylor MP, Keynote Address to Data Transparency 2017 – Washington, 26 September 2017. Refer https://ministers.pmc.gov.au/taylor/2017/keynote-address-data-transparency-2017-washington

[9] Australian Government, Office of the National Data Commissioner, National Data Advisory Council, Terms of Reference, Role of the National Data Advisory Council, accessed 1 October 2019. Refer https://www.datacommissioner.gov.au/about/advisory-council

New legislation for data custodians to share public sector data (Section 2.4)

Research is vital to the economic and social evolution of Australia as a data-driven nation. The introduction of legislation should, if possible, leverage positive use-cases, such as the successful research advancements through data-sharing of the Australian Bureau of Statistics and the Australian Institute of Health and Welfare. Both were made possible through safe and effective practices. By duplicating these processes and practices we might expect to see an increase in both public support of the DS&R legislation and the data literacy of the public sector. The outcomes of research are not always visible at the time of inception, with benefits for some longitudinal research projects sometimes realised only after substantial periods of time and effort. The focus of this legislation should be to enact safe, controlled and transparent sharing of data by those organisations and individuals complying fully with the DS&R legislation.

Building towards a national system

The discussion paper highlights that 'the value of better data sharing between the Commonwealth and States and Territories was a consistent theme' during the consultation process.[10]

Deloitte strongly supports the extension of the legislation, or similar aligned legislation, to the States and Territories as part of the intention set out in the discussion paper for Australia to develop a national system for data sharing and release.

The discussion paper also notes the feedback received from earlier consultations on the importance of addressing the 'grey areas' between freedom of information, privacy and data sharing laws' and the need for 'consistent definitions to reduce possible confusion'.

The development of a consistent national framework would help reduce uncertainty and ambiguity reducing the risk of both incorrect release of data, and, arguably more importantly, the risk of unnecessary denials of data sharing requests.

The discussion paper notes that the Government is working with its State and Territory counterparts to achieve a 'consistent experience' of government and that 'future reforms will explore reciprocating State and Territory legislation to authorise sharing of data across borders to build a national system'.[11] However the discussion paper does not address timelines around this expansion, the resourcing needed and the process that this expansion will take.

Given that State based data sharing legislation has in many cases only recently been passed (Victoria and Queensland in 2017), is currently being contemplated (Western Australia), or has yet to be developed (Tasmania and the Territories), we believe that the migration to a national system should be a clear objective rather than a 'future reform' to be 'explored'.

In addition, it is not clear how voluntary adherence by State and Territories to data sharing is consistent with the objectives of open by default or responsibility to share.

Consistency with other legislation

The discussion paper notes that 'government agencies are confused and uncertain about the existing mechanisms and lack the confidence to use them'. It further notes that the Government 'currently shares public sector data through various laws and mechanisms developed at various points in time, with little consistency or a single point of oversight'. [12]

The drafting of new DS&R legislation, while entirely necessary, is likely to result in further uncertainty around the rights and responsibility of both data producers and users, and ambiguity about the implications of obligations arising under other legislation on data sharing under the DS&R legislation. This uncertainty and ambiguity are likely to directly impede the intent of increasing data sharing and release.

We recommend that a review is undertaken of restrictions on data sharing which exist in the 'various laws and mechanisms' of the Federal Government and, wherever possible, seek alignment in obligations and responsibilities related to data sharing and release. Consideration should also be given to aligning

[10] Discussion Paper, page 8
[11] Discussion Paper, page 15
[12] Discussion Paper, pages 17 and 19

Commonwealth, State and Territory legislative requirements. This will be particularly important for data sharing use cases where the benefits are realised as a result of integration of Commonwealth, and State or Territory data sets.

The *Treasury Laws Amendment (Consumer Data Right) Bill, 2019* provides a relevant example.[13] The introduction of the Consumer Data Right legislation saw amendments of the *Competition and Consumer Act 2010*, and *Privacy Act 1988* on several accounts. These amendments were deemed necessary to maximise the outcome of the proposed Consumer Data Right and to remove ambiguity and overlap for Consumer Data Right participants. This exercise must be performed on both a national, state and jurisdictional basis to ensure clarity around the new DS&R framework.

The comments in the discussion paper that the legislation is principles-based to allow flexibility in its interpretation[14] is somewhat paradoxical and at odds with the intention to provide a clear, consistent approach to the sharing of public data.[15] By necessity the DS&R framework must be responsive to change: the discussion paper outlines the use of binding and non-binding Data Codes in conjunction with principle-based legislation to achieve this.[16] However, there are existing cultural barriers to data sharing within the public sector. Without sufficient codification of data sharing requirements, and a measure of prescription in relation to their application, there is considerable scope for variation in how the requirements are interpreted and applied across the public sector, either due to uncertainty around rights and responsibilities or variation of interpretation because of organisational capability, culture and norms. As a result, we encourage the use of Data Codes to provide clarity as opposed to a reliance just on best practice guidelines and an individual Data Custodian's interpretation of the principles. For example, a Data Code could bring greater clarity in relation to the requirements for the appointment, accountabilities and necessary expertise of Data Custodians.

The introduction of dedicated data sharing and release provisions affords the opportunity to simplify the navigation of a complex landscape of legislative mechanisms. Four examples of this overlap that would require a participant to review and decide if their intentions may conflict with any or all of the laws are:

- The Patents Act 1990 refers to the ability for government agencies to determine whether the data is suitable for open data release.
- The Privacy Act, 1988, which relates to the rules around de-identification of data.
- The Freedom of Information Act, 1982, which encourages a pro-disclosure culture across government.
- The Archives Act, 1983, which provides a right of access to Commonwealth records in the open access period.

It would be beneficial for the legislation to provide unambiguous language and guidance in relation to legislative overlap to realise the objectives of a 'clear, consistent and transparent approach' to data sharing.

We also recommend the examples of cross-border data-sharing occurring in Canada, Europe and the United Kingdom be researched and assessed when developing DS&R legislation in Australia.

Role of community expectations

Public trust associated with the implementation of a data-sharing landscape will be critical to the long-term success of the legislation; however, public trust can be influenced and grown through increased and systemic education and awareness of the benefits of the leading safeguards, penalties for misuse and the expectation of the Government to enable collaboration, increase efficiency and to support research.

While we acknowledge a desire to meet community expectations around data sharing, the role of the legislation must be prescriptive and based on evidence and research.

---

[13] The Parliament of the Commonwealth of Australia - House of Representatives, *Treasury Laws Amendment (Consumer Data Right) Bill*, 2019
[14] Discussion Paper, pages 14 and 40
[15] Discussion Paper, page 1
[16] Discussion Paper, page 14

The discussion paper intends to create a framework which builds trust in the use of public sector data. The discussion paper specifically notes that the DS&R legislation will preclude the sharing of public data considered too sensitive, for the purposes of compliance and assurance activities, and for national security and/or law enforcement. However, it also notes that the DS&R legislation will not allow public sector data to be shared if 'the Australian community does not support it'.[17]

Deloitte support the exclusion of data sharing for the purposes of national security and/or law enforcement. However, Deloitte believe that additional ambiguous classifications of data sets excluded from data sharing may be harmful to the intention of the legislation. In particular, the exclusion of data sharing on the basis that 'the Australian community does not support it' is entirely inappropriate. Such a requirement is difficult to define and measure and is open to wilful or accidental misuse by bureaucrats and politicians. The Law Councils' "Rule of Law Principles" include that a law 'must be both readily known and available, and certain and clear.[18] The inclusion in the DS&R legislation of an exclusion of data sharing on the grounds that 'the Australian community does not support it' would appear to fail that test.

Operation of sharing under the legislation (Section 2.5)

The challenge in Australia has not been in the design of principles: it has been in their implementation. While overarching principles have been well specified in legislation, they must also be translated into practice at the detailed operational level.

Data sharing process map

The discussion paper includes a process map for sharing public sector data under the Data Sharing and Release framework.[19] This process map refers to several processes, tests and principles that need to be applied when deciding whether to share data under the DS&R legislation.

If the staff asked to navigate this process map aren't qualified to classify, analyse or reproduce the data they are asked to assess, the roadmap will lead to additional barriers and uncertainty to data sharing and release. This will be compounded if effective Departmental processes designed to both facilitate and govern sharing and release are not in place. In extreme cases, a misunderstanding may lead to sensitive data being mistakenly released due to a lack of data proficiency or appropriate governance.

In practice, the process map will be more effective where it provides fail-safes, points of authority, and contacts for remediation/clarification of specific nuances and individual use-cases for the data.

One role of the National Data Commission is that of an educator and for the process map to be effectively adopted and the sensitivity of the data or the recipient's right to access correctly classified, it would be beneficial if ALL public sector staff and eventual data sharing participants received appropriate training on decision making under this process map. This will need to be embedded in the same way that staff training on privacy and security obligations is embedded in most employee on-boarding and ongoing training.

The first test is whether the data can be shared easily under an existing authority. As noted above, while the intent of the DS&R framework is that it provides an **alternative** pathway for Government agencies to share data and that existing processes will continue, the discussion paper also acknowledges that there is 'little consistency' in these existing processes. As a result, there is a risk that government departments will continue to need to assess their ability to share data under other legislative frameworks in parallel with the DS&R framework. The effect of this could be to impede the willingness of government departments to share more data.

The act of creating an alternative pathway from existing laws and mechanisms will not achieve a smooth transition or successful adoption of practices or volume. As the Productivity Commission depicted in its Inquiry Report in the table 'Comparing privacy principles across Australian jurisdictions' just one application

[17] Discussion Paper, pages 14 and 25
[18] Law Council of Australia, Rule of Law, https://www.lawcouncil.asn.au/policy-agenda/international-law/rule-of-law
[19] Discussion Paper, page 16, Figure 4

of existing legislation and principles across the nine domains can produce substantial variation and contradiction.[20]

Regarding privacy principles surrounding data, while both the Commonwealth and majority of States and Territories have regulatory frameworks around this topic, the nature of these vary significantly, from guidelines and regulation through to legislation. Also, there is a risk that these frameworks are interpreted inconsistently in different jurisdictions.

We strongly recommend that a review of restrictions on data sharing across federal government is undertaken to align existing Acts with the DS&R legislation. We acknowledge that this will likely be a lengthy and potentially costly exercise for each organisation involved. However, failure to review and align these requirements risks reinforcing the current cautious culture and mindset and could potentially lead to a low adoption of the framework, compromising the ability to realise the objectives of a 'clear, consistent and transparent approach' which 'unlocks the full potential' of public sector data'.

Funding

One of the biggest challenges for the implementation of effective data sharing and release in Australia is funding. In our discussions with Federal, State and Local governments we are consistently told that without specific funding, the organisations will not be able to invest in the skills, capabilities and physical/cyber infrastructure needed to codify data assets, store these data assets securely, manage the quality of the data assets and use shared data to enhance outcomes nor maintain the contract/legal expertise necessary to establish appropriate sharing arrangements.

As part of the impact assessment for the implementation of data sharing and release we recommend that the Government undertake an assessment of the current skills, capabilities and technology available to support data sharing and release.

In addition, based on the current state assessment, we recommend that the Government ensure that departments are provided with specific funding to enable them to enhance the departmental infrastructure necessary for an effective data sharing and release regime. This includes the creation of data asset registers, ensuring that the appropriate technology and cyber infrastructure is in place to store and share data assets securely, and building the skills and capabilities to ensure that data is secure, effectively managed, and appropriately shared and used.

Reporting on data sharing

The current approach to reporting data sharing has focused on reporting the number of data sets published. This has driven the wrong behaviours – a focus on box-ticking compliance, where data sets are disaggregated and published to meet target numbers rather than the sharing and release of high value, granular data sets.

Deloitte recommends that the process for sharing and releasing public sector data include a specific requirement to provide more granular reporting on data sharing and release. This may include, for example, reporting on the number of data sharing agreements executed, and the uses to which data sharing was applied. It could also include reporting on best practices and success stories.

Such practices would result in data sharing and release being seen as more than a compliance exercise and contribute to the desired cultural change by highlighting the benefits that were realised from data sharing and release.

Data Sharing Agreements

The requirement for all Data Sharing & Release participants to publish a Data Sharing Agreement is intended to promote greater transparency. However, there are challenges with the proposed approach.

These are explored in more detail in Data Sharing Agreements (Section 5.3).

[20] Productivity Commission, *Data Availability and Use, Report No 82*, Canberra, March 2017, Table D.1 Comparing privacy principles across Australian jurisdictions, page 456

Open data release (Section 2.6)

The discussion paper notes that the DS&R legislation is intended to 'empower the government to share public sector data for specified purposes'. It also notes that the legislation will ***not*** provide a new legislative authorisation for open data release.

The concept that open data can and should be treated separately from other formats of data sharing and release is arbitrary – they should be part of a continuum of data sharing and release rather than binary alternatives.

In his keynote address to the Data Transparency Conference in Washington, 2017, the then Assistant Minister for Cities and Digital Transformation, Angus Taylor, highlighted that since 2013 open data has been at the forefront of Australia's innovation. He explained that 'Open data, alongside well targeted Government standards and platforms, will be one of the next great enablers of modern digital economies and better government'.[21]

There is a risk that the exclusion of open data release from the DS&R legislation will result in increased uncertainty and confusion around the purpose and restrictions of numerous datasets across both Commonwealth and other data custodians.

The discussion paper notes two reasons that open data release is excluded. Firstly, it notes that the conclusion from the consultation process was that 'current mechanisms are sufficient'. Secondly it implies that extending the DS&R legislative framework to open data release would 'duplicate existing legislative authorisations to release open data'.

However, despite noting that current mechanisms for open data release are 'sufficient', the discussion paper then contradicts this by noting that 'Government agencies are confused and uncertain about the existing mechanisms [for open data release] and lack the confidence to use them'.[22]

The discussion paper also notes the intention that the Commissioner will, in conjunction with other government agencies and regulators including the Australian Information and Privacy Commissioner, 'improve guidance on using existing mechanisms to release open data'.[23] Deloitte recommends that **all** data practices, including open data release, are reviewed, clarified, and improved. This review should be undertaken, across the entire government including other government participants in data sharing and release under the DS&R legislation.

The assurance that the DS&R legislation will not duplicate existing legislative authorisations to release open data is paradoxical. While Deloitte acknowledges that not all data will be fit for public release and publication, the practices, review and treatment of open data release should be no different to the treatment of the most sensitive of national data.

The Commonwealth mandate of releasing all non-sensitive data by default has not worked. The discussion paper acknowledges the cultural factors, risk aversion, inconsistent standards and lack of understanding that have contributed to this.[24] While the availability of open data has increased, the quality of that data and the reluctance of some departments to participate for fear of breaching existing legislation or concerns about the risk of re-identification has limited the extent of open data release. In addition to improving the practices and policies in relation to open data release, the sharing of best-practice and use-cases will also contribute to the desired cultural change by highlighting the benefits that were realised from open data release.

---

[21] Department of the Prime Minister and Cabinet, 2017
[22] Discussion Paper, page 19
[23] Discussion Paper, page 19
[24] Discussion Paper, pages 1 and 19

OPEN DATA in the US: the DATA Act and OPEN Government Data Act

In the US one of the key drivers for data transparency is the federal government's effort to implement wide-scale data interoperability through the Data Accountability and Transparency Act of 2014 (DATA Act), which seeks to create an open data set for all federal spending. The DATA Act has the potential to transform various federal management practices. If successful, the DATA Act could dramatically increase internal efficiency and external transparency. If the act is successfully implemented, by 2022, spending data will flow automatically from agency originators to interested government officials and private citizens through publicly available websites.[25]

In January 2019, the US enacted the Open, Public, Electronic, and Necessary Government Data (OPEN) Act. A recent report by Deloitte on the US OPEN Government Data Act for the Data Foundation has points that are relevant in Australia.[26] "Policymakers [in the US] are now demanding that agencies become better positioned to increasingly and meaningfully use high-quality evidence to inform key decisions. … OPEN builds on previous federal open data laws by adding an expectation that the federal government's data will be open and accessible, by default, unless there are restrictions or limits such as for protecting confidentiality and national security."

Deloitte's report recommends governments:

1. Properly empower agencies to effectively implement new directives about data quality and management in government.
2. Share leading practices and success stories.
3. Establish cross-agency data governance processes to work across silos.
4. Ensure agencies have the necessary resources to fulfil their open data obligations.

The inclusion of open data release in the scope of the DS&R legislation would provide an opportunity for the government to implement similar requirements in Australia and could help to 'unlock the full potential' of public sector data.

Q2. What are the challenges for open release of public sector data?

The open release of public sector data has been limited by a 'need to know' rather than a responsibility to share' culture in the public sector. This has been amplified by conflicting legislative requirements, inconsistent skills, difficulties in measuring benefits from data sharing and release, and inadequate funding to support the data sharing and release agenda.

As noted, data sharing and release are both part of an open data continuum. There is a risk that the exclusion of open data release from the DS&R legislation will result in increased uncertainty and confusion around the purpose and restrictions of numerous datasets across both Commonwealth and other data custodians.

[25] Deloitte Centre for Government Insights, *Implementing the DATA Act for greater transparency and accessibility*, The Chief Data Officer in Government: A CDO Playbook, 2019

[26] Deloitte and the Data Foundation, *Future of Open Data: Maximizing the Impact of the OPEN Government Data Act*, 9 October 2019. Refer https://www.datafoundation.org/future-of-open-data-cover-page and https://www.biia.com/us-public-sector-information-the-future-of-open-data-maximizing-the-impact-of-the-open-government-data-act

Release of citizen data to citizens

The discussion paper correctly highlights that discussion in Australia has been focused on open data –data that anyone can access, use modify or share for any purpose, usually for free – and closed data which is only accessible by the government agency which is the data custodian for that data. This reflects the genesis of open data in the government sector. The discussion paper expands on this in Figure 1 where it outlines three types of data:[27]

- Closed data – internal agency access only.
- Shared data – controlled access to the right people for the right reasons.
- Open data release – public access to open data.

What this excludes however is the release of information that a citizen has provided to a government organisation to that citizen or to a recipient that the citizen chooses to share it with.

The Farrell Report on open banking noted that:

> "Personal details and information on their financial situation that a customer has provided to a bank clearly 'belong' to the customer. It can be provided to anyone they chose [sic], without any argument being raised that it did not belong to them to do so or did not belong to them exclusively. In principle, customers should have the right to instruct that it be given to them, or shared with data recipients they choose, in a form that facilitates its transfer and use."[28]

Deloitte believe that this same principle should be applied to information that a citizen (including businesses) has provided to a government organisation. Farrell's comment on open banking could be paraphrased for the public sector:

> Personal details and information that a *citizen* has provided to *a government organisation* clearly 'belong' to the *citizen*. It should be able to be provided to anyone they choose, without any argument being raised that it did not belong to them to do so or did not belong to them exclusively. In principle, *citizens* should have the right to instruct that it be given to them, or shared with data recipients they choose, in a form that facilitates its transfer and use.[29]

The exclusion of citizens' right to access and share information that they have provided to a government is also inconsistent with global data policies such as the European Union's General Data Protection Regulations (GDPR). The same data rights that apply to individuals under GDPR extend to data that a government agency collects about a citizen (as well as other individuals and data subjects that are not citizens).

There are several potential benefits from extending the DS&R legislation to data contributed by citizens to the government.

- Providing citizens with access to their data could assist with identify verification or income verification.
- Providing citizens with the ability to share education data could assist with the delivery of a qualification and skills inventory which could enhance employment opportunities and reduce inefficiencies resulting from bureaucratic qualification validation.
- Providing citizens with the ability to share data with family members that they nominate could improve the delivery of health services or aged care.

---

[27] Discussion Paper, page 3, Figure 1: Data Sharing and Release legislation focuses on shared data

[28] The Australian Government, *Open banking: customers, choice, convenience, confidence*, December 2017, page 34. Refer https://treasury.gov.au/consultation/c2018-t247313

[29] The statement from the Farrell Review has been amended to substitute 'citizen' for 'customer' and 'a government organisation' for 'a bank' to highlight the application of this principle to data governments hold about citizens as a result of citizens providing that data to the government.

These are just a few potential examples.

Paraphrasing Farrell again: "Many *citizen* benefits should come from new products and services that are currently unable to be foreseen."[30]

The GDPR allows for exceptions which permit a government organisation to refuse to share certain data sets or to refuse to share data with certain individuals for national security and law enforcements reasons. Similar restrictions could be included in citizen access provisions which we are proposing should be included in the DS&R legislation.

The inclusion in the DS&R legislation of a right for citizens to access their data, and the associated express informed consent for the use of that data, could be seen to be antithetical to the sharing of identified citizen data with accredited third parties. We do not think that this is correct. The citizen access provisions which we are proposing should be included in the DS&R legislation could also note that the requirement for express informed consent before a citizen's data is shared with a third party do not apply to data which is shared with an accredited recipient under the data sharing provisions of the DS&R legislation.

Q3. Do you think the Data Sharing and Release legislative framework will achieve more streamlined and safer data sharing?

The DS&R legislative framework has the potential to contribute to more streamlined and safe data sharing. However, as noted in our comments, the exclusion of data release, the prescriptive detailed requirements for Data Sharing Agreements, and the relegation of alignment of Federal and State legislation on data sharing and release to a 'future reform' to be 'explored', may lead to the DS&R Act's overall outcomes being diluted, and may result in the overarching intention of removing barriers and reducing uncertainty surrounding the sharing of data within the Australian Public Sector remaining largely unimproved or unachieved. As a result, the DS&R legislation may fail to 'unlock the full potential of public sector data'.

Q4. What do you think about the name, Data Sharing and Release Act?

As noted in our responses to this section, we believe it is important that the Data Sharing and Release Act should encompass the breadth of scope reflected in this name and in the original ambition set out in the Productivity Commission's report on Data Availability and Use in Australia. This would require the legislation to include matters relating to open data release, and to sharing and release of data with citizens.

We have also recommended that this Act become the primary legislation for data sharing and release and other acts are amended to reflect this. If this is not done explanatory text will be important considering the interdependency with other legislation and excluded elements.

[30] The Australian Government, *Open banking: customers, choice, convenience, confidence*, December 2017, page 9.

3 Sharing Data for Public Benefit

There is a public expectation that the Government collects, processes and appropriately treats data to provide the essential services citizens need, when they need them. The discussion paper highlights that while there are pockets of excellence, data practices need to be improved across all departments. To improve the outcome, transparent policies, processes and systems must be implemented to facilitate the educational and behavioural transformation referred to in the legislation.

When can data be shared for the public benefit (Section 3.2)

The process map for sharing discussion paper highlights that data should only be shared where it meets the 'purpose test'. Acceptable purposes for data sharing are then limited to just three:

- Government policy and programs.
- Research and development.
- Government service delivery.

However, there are several other benefits from data sharing and release, and as a result, a number of other potential purposes for data sharing:

- Improved risk management with data sharing contributing to better identification and understanding of risks, coordination of activities to mitigate risks, and improved resilience.[31]
- Improved governance and enhanced transparency, resulting in more engaged and empowered citizens.[32]
- Reduced cost of government service delivery - data can offer new ways to curb waste as well as to operate more efficiently and get more done with less.[33]
- Exposure of government waste or corruption - with mounting public pressure for transparency and accountability, data can offer new ways to curb fraud, and abuse.[34,35]
- Improved transparency as citizens, governments, industries and researchers use and share data, contributing to greater competition and innovation.[36]
- Greater alignment with organisational purpose.

While arguably, some of these could be included in the three purposes set out in the discussion paper, the identification of just three 'acceptable' purposes seems inconsistent with the intent to promote a cultural change in the public sector. It also seems to be inconsistent with the stated intent to 'unlock the full potential' of public sector data, to shift thinking about data sharing from '*can I share*?' to '*how can I safely share*?' and the desire to achieve a paradigm shift from 'need to know' to 'responsibility to share'.[37]

There are two objectives that the 'purpose test' should meet.

On the one hand it is important that purposes are well-defined to ensure that data is not improperly shared. This aligns with the *Privacy Act 1988* requirements to define primary and secondary purposes to collect

[31] Productivity Commission, 2017, page 110
[32] Productivity Commission, 2017, page 111
[33] Deloitte Centre for Government Insights, *The Chief Data Officer in Government: A CDO Playbook*, 2019, page 1
[34] Productivity Commission, 2017, page 114
[35] Deloitte Centre for Government Insights, The Chief Data Officer in Government: A CDO Playbook, 2019, page 1
[36] Department of Prime Minister and Cabinet, Media Release, *Greater competition will come from more access to data*, 8 May 2017. Refer https://ministers.pmc.gov.au/taylor/2017/greater-competition-will-come-more-access-data
[37] These statements of intent are set out in the Discussion Paper on pages 1, 5 and 13

and handle personal information, including Australian Privacy Principle (APP) 5.2(d) (notification of the purpose of collection) and APP 6.1 (use or disclosure of personal information permitted for the primary purpose, and for a secondary purpose in limited circumstances).

However, it is also important that the requirement to describe the purpose 'in detail' in a Data Sharing Agreement does not drive data sharing and release practices which fail to 'unlock the full potential' of public sector data.

It is common practice to share and correlate unrelated data sets to assess the combined data for common trends and behaviours. For example, combining data on education and health may yield significant developmental benefits to society and considered regions, however, the specific insights obtained may differ from those set out in the original detailed description of the purpose for which the data was being shared. In order to achieve true innovation it is also common to refrain from making predictions so as not to stifle creativity and limit the potential outcomes. Further, the rapid rate of change, e.g. in technology, can afford opportunities not envisaged at commencement.

The purpose test as currently described requires consideration of both currently intended and potential future purposes and uses for shared data. Given the challenge with predicting future use, this may limit the uses of shared data or lead to unnecessarily cautious decisions on sharing data. Decision-makers may have a legitimate fear of data recipients using the analytical output for a purpose which is not consistent with a narrow interpretation of the purpose described in detail in the Data Sharing Agreement. This outcome would be incongruous with the intent of the DS&R and contrary to the Government's clear innovation agenda[38] and desire to use data to achieve maximum economic benefit to Australia.[39]

Deloitte recommend that the National Data Commissioner develop guidance to assist Data Custodians and other data sharing participants in understanding the permitted purposes and the level of detail that is required to be documented in the Data Sharing Agreement. (Refer also to our comments in Data Sharing Agreements (Section 5.3)).

Q5. Do the purposes for sharing data meet your expectations? What about precluded purposes?

This question has been addressed in our comments above.

Private sector use of data sharing for commercial applications (Section 3.4)

The discussion paper notes that consideration is being given to:

- How to enable data sharing for research and development for commercial uses that benefit society, but do not harm individuals or businesses.
- How to design the purpose test to maximise public benefits while meeting community expectations.

The discussion paper also notes that the purpose test and the Data Sharing Principles are the avenues to prevent commercial uses not supported by the community. The discussion paper invites further comments about this area to 'fully understand Australians' concerns'.

Deloitte is pleased to note that the discussion paper does not propose preventing users participation in data sharing based on their sector.

However, we do not believe that community support is an appropriate standard for assessing or preventing commercial uses of shared public sector data. Differing levels of awareness, knowledge and interest make this a problematic measure.

[38] https://www.industry.gov.au/strategies-for-the-future/boosting-innovation-and-science
[39] Productivity Commission, 2017

The acts of collecting data, processing, sharing and releasing data require resources and technology. Where the government performs these acts, there is a public assumption of funding through taxation. Where these acts occur in a non-government or private organisation, a commercial reality exists.

When considering feedback that 'Australians are concerned about public sector data being used by the private sector' it is useful to consider the broader global socio-political context in which this feedback is being received.

Recent findings by Deloitte Canada are that 80% of consumers believe organisations have an ethical responsibility with respect to the data they collect from the public. Furthermore, 90% of global consumers would cut ties with organisations that used their data unethically.[40] In addition many people find the sheer velocity of change in society overwhelming. As a result, they feel increasingly vulnerable, as citizens, employees, and consumers. It is this general sense of vulnerability—a belief that the system is no longer working for them—that plays a significant part in creating and sustaining a climate of public distrust towards institutions.

As noted in the 2017-18 APS State of the Service Report, 'Public trust in governments in many countries, including Australia, is in decline'.[41] The Independent review of the APS: Priorities for Change report expands saying, 'we have seen declining trust in traditional institutions, accompanied by dissatisfaction with public services and a push to solutions that are more local and personalised in design and delivery. The last five years have seen the emergence and rapid growth of new political parties in some of the world's largest economies. Trust scores are the lowest on record, particularly for government. The pressures of 24/7 news coverage have been amplified by social media networks'.[42]

This generalised distrust is likely to lead to scepticism about how government data on citizens may be used, particularly by the private sector. This is likely to particularly be the case for people from disadvantaged or vulnerable groups. A study undertaken for Data61 as part of the standards development for the CDR found that people from disadvantaged or vulnerable groups were more inclined to be concerned about harm arising from data sharing and had more explicit concerns about how their data might be used to classify or exploit them.[43]

However, people's intentions as a result of their expressed distrust do not always correlate with their actions.

A key concept in behavioural economics is the 'intention-action' gap also referred to as the 'say-do gap': the difference between what people say they want to do and what they do.

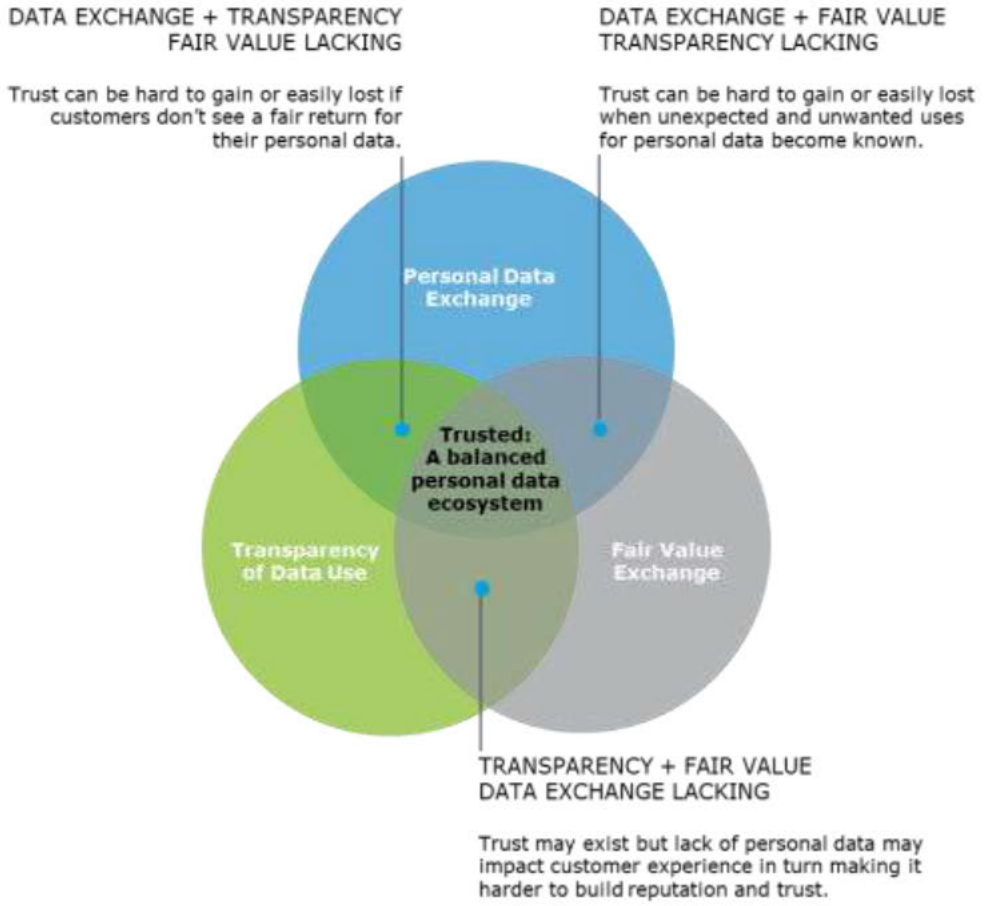
In a recent consumer survey Deloitte has undertaken we noted how people's willingness to share data was influenced by the value and benefits they could receive from sharing data, and the levels of information trust they had in the organisation with which they were sharing their data.[44]

Organisations need to create a balanced data ecosystem for their customers, where the exchange of customer data is balanced with security and transparency, and the fair exchange of value.[45]

---

[40] Deloitte, *Privacy for sale – To the highest bidder*, 2017. Refer www2.Deloitte.com/ca/en/pages/Deloitte-analytics/articles/dataethics2017.html
[41] Australian Public Service Commission, *State of the Service report 2017-18*, page 14. Refer https://www.apsc.gov.au/state-service-report-2017-18
[42] Australian Government, Independent review of the APS: *Priorities for Change*, 19 March 2019, page 11. Refer https://www.apsreview.gov.au/resources/priorities-change
[43] GippsTech, *Consumer Data Standards: Consent Flow, Phase 2 CX Stream 1 Report*, June 2019, pages 52 and 53. Refer https://consumerdatastandards.org.au/wp-content/uploads/2019/07/Phase-2-CX-_-Stream-1-_-Consent-Flow.pdf
[44] Deloitte, *Open Banking: Switch or Stick? Insights into customer switching behaviour and trust*, October 2019. Refer https://www2.deloitte.com/au/en/pages/financial-services/articles/open-banking.html
[45] Deloitte, *Deloitte Australian Privacy Index: The Symbiotic Relationship: getting the balance right*, 2018. Refer https://content.deloitte.com.au/20180821-ris-inbound-risk-privacy-index-2018-registration

Figure 1



The same principles are likely to apply to the commercial uses of public sector data.

Where citizens and consumers receive value that they perceive is fair in exchange for public sector data which is shared, where there is transparency on which data is shared, and where they have confidence that the data is being stored securely then they are more likely to support sharing of public sector data with the private sector.

Allowing private sector entities to become Accredited Data Users is important if we are to unlock the full potential of public sector data. There is an important role for Government in educating the community about the potential benefits of data sharing and release with the private sector, and a danger in allowing policy to be determined by the sum of the community's fears.

Q6. What are your expectations for commercial uses? Do we need to preclude a purpose, or do the Data Sharing Principles and existing legislative protections work?

This question has been addressed in our comments above.

4 Strengthening Safeguards

Deloitte supports the inclusion of safeguards within the proposed legislation, however, suggests clear guidance for participants be developed in order to overcome the risks of these safeguards becoming barriers to achieving the legislation's purposes.

Broadly, we support the proposed safeguards for the DS&R legislation, which are intended to assist in ensuring that data is shared safely and for the public good. Acknowledging the broad definition of public sector data, we note the importance of approaching the application of safeguards with consideration of the vast range of data that may be subject to the legislation, and the need for different classifications of data to be protected in different ways.

Data Sharing Principles (Sections 4.2 and 4.3)

Deloitte supports the introduction of the five Data Sharing Principles: project, people, settings, data and outputs.[46]

These Principles are based on the UK Office for National Statistic's 'VML Security Model', or Five Safe's framework and set out the 'requirements for safeguarding any sharing activity authorised under the legislation'.[47]

The adoption of a readily identifiable international framework will enhance the potential for cross-border data sharing of Public Sector data with foreign allies, assist in the development of institutional research collaboration on a global scale, and support the adoption of a data-sharing culture throughout the multi-national private sector.

It is noted within the Privacy Impact Assessment (PIA) that the detailed requirements of the Principles will not be set out in the proposed Bill, but will be set out in the Best Practice Guidelines.[48] A Best Practice Guide to Applying Data Sharing Principles, to be updated periodically, has already been published.

We support the development of tailored guidance for Data Custodians to assist in the application of the Data Sharing Principles. It is important that this guidance is detailed, practical, and easy-to-understand in order to assist decision-making, enable the purposes of the DS&R legislation to be achieved, and ensure the Principles are a substantive consideration, rather than an impractical obstacle to data sharing. It is also important that, as noted, the guidance emphasises the different considerations that may be required depending on the classification of the data that is subject to sharing.

The discussion paper notes the intent that the new principle-based framework (the five Data Sharing Principles) will streamline data sharing through the introduction of the right protections as an alternative to the ad-hoc safeguards currently used in practice. However, the discussion paper also notes that the DS&R legislation will operate 'alongside existing requirements for the collection, storage, integration and management of data'.[49]

Given that these 'existing requirements' are also likely to be ones which are contributing to the 'ad-hoc safeguards currently used in practice' Deloitte believe it would be beneficial to undertake a review of existing requirements with the objective of removing 'ad-hoc' or inconsistent requirements. Greater alignment and consistency would support the government's intention to have 'a clear, consistent and

[46] UK Office of National Statistics, Five Safes: designing data access for research, 2016
[47] Discussion Paper, page 30
[48] Department of Prime Minister and Cabinet, *Privacy Impact Assessment on Proposed Data Sharing & Release Bill and Related Regulatory Framework*, June 2019, page 22
[49] Discussion Paper, page 29

transparent approach' to data sharing and help address the uncertainty and ambiguity which are contributing to the current public sector culture towards data sharing.

Q7. Do you think the Data Sharing Principles acknowledge and treat risks appropriately? When could they fall short?

This question has been addressed in our comments above.

8. Is the Best Practice Guide to Applying Data Sharing Principles helpful? Are there areas where the guidance could be improved?

The Best Practice Guide provides useful guidance on applying the Data Sharing Principles.

It is important that this guidance is detailed, practical, and easy-to-understand in order to assist decision-making, enable the purposes of the DS&R legislation to be achieved, and ensure the Principles are a substantive consideration, rather than an impractical obstacle to data sharing. It is also important that, as noted, the guidance emphasises the different considerations that may be required depending on the classification of the data that is subject to sharing. Possible improvements include leveraging the data de-identification process output under the Consumer Data Right framework.

Privacy by design (Section 4.4)

The Data Sharing Principles enable a privacy by design approach to data sharing. We support the commitment to privacy by design practices. Privacy by design allows for more proactive and efficient management of privacy risks, assists in minimising security risks, and allows the right protections to be in place by default. Privacy by design also assists by placing the individual at the centre of the project and promotes transparency and social licence.

However, it is important to note that privacy is one of many factors that need to be considered for the intent of the data sharing and release legislation to be realised. While privacy is important, it should not be given priority over other factors such as the identity of the data recipients and the purpose for which data is being shared.

The discussion paper highlights the significant change that the DS&R legislation represents in the way the government handles public sector data: from 'need to know' to 'responsibility to share' where there is a clear public benefit. It will be important that the 'privacy positive' measures incorporated into the DS&R legislation do not perpetuate existing cultural barriers, or create a new cultural barrier, to data sharing.

Privacy standards (Section 4.5)

The discussion paper notes that the government intends to build privacy positive measures into the legislation. These privacy positive measures include:

- Requiring all entities handling personal information to be subject to equivalent legal privacy obligations.
- Listing permitted and precluded purposes for sharing.
- Only authorising data sharing that is reasonably necessary for a permitted purpose.
- Designing the Data Sharing Principles to provide holistic risk management.
- Restricting on-sharing of information.

Requiring all entities handling personal information to be subject to equivalent legal privacy obligations

The discussion paper notes that all entities handling personal information will be required to be subject to equivalent legal privacy obligations, including individuals and small businesses who may be exempt from the Privacy Act. For State and Territory users, they will be required to be covered by the Commonwealth Privacy Act, or a State or Territory law that provides equivalent protection to the Privacy Act.

We note the Department's agreement with Recommendation 4 from the PIA on additional Data Breach Notification requirements, and support this requirement as a measure to promote consistency and privacy safeguards.

In accordance with this measure, it is recommended that consideration be given to extending the application of the Australian Government Agencies Privacy Code 2017 to entities participating in data sharing who are otherwise not required to comply with this Code. The application of the Code to all authorised users will ensure that mutually stringent privacy requirements are in place to safeguard personal information that is shared or released.

Permitted and precluded purposes

As noted in section 3.2, the discussion paper notes that the legislation will authorise data sharing to inform government policy and programs, research and development, and delivery of government services. The legislation will preclude the sharing of public sector data for the purposes of compliance and assurance activities, and national security and/or law enforcement.

We have highlighted that there are two objectives that the 'purpose test' should meet. The purpose should be defined in sufficient detail so that data is not improperly shared by Data Custodians. However, it is also important that the requirement to describe the purpose 'in detail' in a Data Sharing Agreement does not preclude unanticipated uses that emerge from the analysis of the shared data.

Deloitte recommend that the National Data Commissioner develop guidance to assist Data Custodians and other data sharing participants in understanding the permitted purposes and the level of detail that is required to be documented in the Data Sharing Agreement. (Refer also to our comments in Data Sharing Agreements (Section 5.3)).

Only authorising data sharing that is reasonably necessary for a permitted purpose

The PIA recommended that the DS&R Bill should include the word 'only' in the data minimisation requirement, in order to strengthen the requirement and avoid the risk that data minimisation is lost or downplayed (Recommendation 7). The discussion paper notes that the purpose test incorporates the 'data minimisation' concept by authorising sharing of only data that is reasonably necessary to achieve an approved purpose.[50]

If Data Custodians interpret 'data that is reasonably necessary' too broadly, there is a risk that privacy will be compromised. However if 'data minimisation' is applied too strictly, together potentially with a restrictive interpretation of the purpose, then data may not be made available to data recipients which could result in data sharing and release practices which fail to 'unlock the full potential' of public sector data.

In addition to the permitted and precluded purposes, and the data minimisation requirement, the discussion paper also outlines a number of other parameters that Data Custodians are required to consider before sharing data: what project the data will be used for, how detailed the data is, how the data will be protected, who will use the data, and whether outputs can be published without identifying individuals or businesses.[51]

There is a risk that these requirements place an unfair burden on members of the public sector who are not equipped for this responsibility. The ability to assess the safe and secure environment for the data analysis and use may not align with the professional skills and expertise of the Data Custodian.

---

[50] Discussion Paper page 61; and DPMC, June 2019, page 22
[51] Discussion Paper, page 29

The requirement for all Data Sharing Principles to be satisfied prior to data being exchanged has contributed to the current low levels of data sharing in the public sector. The DS&R legislation intends to remove the uncertainty and concerns around breaching privacy and sharing principles that currently impede data sharing.

Deloitte recommend that the National Data Commissioner develop guidance to assist participants in understanding the purpose test, the 'data minimisation' concept and their impact on the level of detailed description required in a Data Sharing Agreement, together with the other requirements of a Data Sharing Agreement.

This provision of this guidance would support the objectives of the DS&R legislation of having 'a clear, consistent and transparent approach' to data sharing which 'unlocks the full potential' of public sector data. (Refer also to our comments in Data Sharing Agreements (Section 5.3)).

Holistic risk management

In order to provide holistic privacy risk management, it is important that safeguards are in place throughout the information's lifecycle. This includes consideration of privacy requirements prior to sharing, and once the information is no longer required or necessary as identifiable or reasonably identifiable information.

We support the Data Sharing Principles Best Practice Guide's current recommendation of removing direct identifiers in most cases of data sharing and retaining identifiers only if they are critical for the purpose of the project.

We also support the inclusion of general de-identification and destruction considerations within the Guide. To enhance consistency of data practices across Australia, the DS&R regulatory framework should consider leveraging the data de-identification process output under the Consumer Data Right framework.

Holistic privacy risk management is hampered by the existence of several privacy acts and other legislative requirements which restrict or regulate data sharing and privacy. Unless these are aligned, data sharing and release participants will still face the complexity of reconciling different regulatory requirements, and understanding how each apply to a specific data sharing request. This is likely to perpetuate the uncertainty and barriers to the adoption of the data sharing and release that have impeded the use of public sector data to date and contributed to the risk averse data sharing culture in the public sector.

In Section 2.5 we recommended that a review be undertaken of restrictions on data sharing across federal government to align existing acts with the DS&R legislation. This will also contribute to achieving the government's objective of providing holistic risk management.

Restricting on-sharing of information

The discussion paper proposes to support positive privacy measures by restricting on-sharing of information. The PIA suggests that on-sharing of data will be authorised where the proposed sharing meets the purpose test, is consistent with the Data Sharing Principles, and is subject to a Data Sharing Agreement between the sharer and the recipient, with written agreement from the Data Custodian.

While positive for privacy, restricting on-sharing may also limit the potential benefits that can be realised from data sharing. Whether it is appropriate to permit on-sharing of information may be dependent on the classification of the data subject to the sharing, and the parties involved.

For example, an accredited data user may have integrated shared data with an existing data set or another shared data set and, in so doing, created a new data asset. Restrictions on the additional sharing of this new data asset, or requirements that this new data asset be destroyed at the end of the originally specific purpose for which the data was shared, may result in the destruction of a valuable data asset.

In this circumstance a general restriction on sharing of information could conflict with the underlying intention of the legislation, to improve public services, policies and research outcomes from sharing data.

We recommend that an assessment of acceptable on-sharing be included in Data Sharing Agreements and, where relevant, in the accreditation process for data recipients.

Interaction with the Privacy Act

One of the objectives of the DS&R legislation is to remove barriers and encourage increased data sharing. However, the interactions between the Privacy Act, the inclusion of a Sensitive Data Code[52], the Data Safeguard Framework and the purpose test create a challenge, for both understanding, and compliance with the intent of the legislation. Without the elevation of an ultimate measure or harmonisation of the legislation the competing requirements risk only increasing uncertainty around the sharing and release of data.

The introduction of the Data Sharing and Release legislation will result in three key legislative privacy schemes:

- The *Consumer Data Right, 2019.*
- The *Privacy Act, 1988.*
- The Data Sharing and Release legislation.

During the creation and introduction of the Consumer Data Right, a decision to unify the intent of the two acts and have consistent language and direction saw the *Privacy Act 1988* amended so that it applied to additional parties, i.e. those parties which needed to be covered under the Consumer Data Right.

We recommend that consideration be given to adopting a similar approach for the DS&R legislation and aligning the privacy requirements in these three pieces of the legislation.

Q9. Do the safeguards address key privacy risks?

While privacy is important, it should not be given priority over other factors such as the identity of the data recipients and the purpose for which data is being shared.

The discussion paper notes that all entities handling personal information will be required to be subject to equivalent legal privacy obligations, including individuals and small businesses who may be exempt from the Privacy Act. For State and Territory users, they will be required to be covered by the Commonwealth Privacy Act, or a State or Territory law that provides equivalent protection to the Privacy Act. Noting the Department's agreement with Recommendation 4 from the PIA, we support this requirement as a measure to promote consistency and privacy safeguards.

In accordance with this measure, it is recommended that consideration be given to extending the application of the Australian Government Agencies Privacy Code 2017 to entities participating in data sharing who are otherwise not required to comply with this Code. The application of the Code to all authorised users will ensure that mutually stringent privacy requirements are in place to safeguard personal information that is shared or released.

Consent (Section 4.6)

There is a genuine paradox surrounding consent: the discussion paper highlights the dilemma that consent requirements presents.[53]

Obtaining consent contributes to developing public trust, confidence and acceptance of the data sharing and release framework.

However, requiring consent for all data sharing will lead to biased data that delivers the wrong outcomes.

Given the nature and common circumstances of collection of the personal information held by government agencies, consent may be an important privacy safeguard and help build social licence and trust within the community. Consent requirements also help the community understand its rights across a range of complex legislation and creates consistent messaging and understanding about the level of custodianship individuals have over their personal information. A consistent consent framework also supports the government's

[52] Discussion Paper, page 32
[53] Discussion Paper, page 33

broader open data agenda by having consent requirements for citizen's data which are consistent with the consent requirements applied to customer data.

It is important to ensure that the DS&R legislation does not enable improper bypassing of existing consent requirements. For example, it may ordinarily be appropriate for (or required of) an entity to gain an individual's consent to collect sensitive information under APP 3.3. Where this is the case, in order to avoid gaining consent an entity may instead rely on the DS&R legislation to collect sensitive information in accordance with APP 3.4(a), under which entities may collect sensitive information without consent where the collection is authorised by, or under, an Australian law.

However, Deloitte also agrees that, where personal data is shared for a permitted purpose, requiring consent may lead to biased data. Although supporting the consideration of consent where practical and feasible, Deloitte agrees a legal requirement to gain consent for all instances of data sharing would compromise realising the purposes of the DS&R legislation.

The discussion paper proposes that the DS&R legislation does not require consent for sharing of personal information, and instead places the responsibility on Data Custodians and Accredited Users to safely and respectfully share personal information where reasonably required for a legitimate objective.[54]

However, the discussion paper notes that consent may be built into the application of the Data Sharing Principles, including by making consent a requirement if it is practical and feasible. This is because the PIA indicated that the Data Sharing Principles are 'stronger and more relevant' that some of the *Privacy Act 1988* requirements.[55]

Deloitte supports the inclusion of sharing of personal information without consent for legitimate objectives but are concerned that the responsibility for assessment falls on Data Custodians and Accredited Users. This will require appropriate training and clarity on the assessment process.

We support the development of guidance to build consent into the Data Sharing Principles, where it is practical and feasible. Noting that a yet-to-be-developed Sensitive Data Code is to provide additional safeguards for sensitive data, guidance that supports gaining consent where possible should consider the different kinds of data that may be subject to sharing.

[54] Discussion Paper, page 32
[55] Discussion Paper, page 32

5 Building trust through transparency

Deloitte supports the development of Data Sharing Agreements for the purpose of defining and publicising details of data sharing arrangements, however it will be important that the detail required in these agreements does not present a new barrier to participating in data sharing.

Data Sharing Agreements (Section 5.3)

Proposed mandatory terms of the Data Sharing Agreements

The discussion paper notes that Data Sharing Agreements will be required for all data shared under the DS&R legislation and outlines a range of specific mandatory terms that these agreements will need to include. Data Sharing Agreements will be required to:

- '**Describe in detail'** how the data sharing meets the purpose test.
- Provide a '**detailed description'** of the data being shared.
- Provide a '**detailed description'** of safeguards to protect data.
- Provide a '**detailed description**' of how output would be handled.
- Require identification of under which legislation the data was originally collected.

While the intention of requiring these and other disclosures in the Data Sharing Agreement is to build trust, there is a risk that the breadth of requirements and the level of detail which is being prescribed reinforce existing cultural barriers to data sharing in the public sector.

The discussion paper also notes that previous consultation has highlighted that in order to create a more efficient data sharing system, these agreements should be 'simple, streamlined and consistent'.[56]

The inclusion of mandatory requirements for Data Sharing Agreements to include 'detailed descriptions' of information does not appear to be consistent with the development of 'simple, streamlined and consistent' agreements or a more efficient data sharing system.

There is also a risk that prescriptive mandatory requirements for detailed descriptions reinforce the existing 'need to know' culture in the public sector with its aversion to data sharing, and prevent the emergence of a culture which is based on 'responsibility to share' where there is a clear public benefit.

By introducing several gates, the new legislation will require data producers and data users to master the art of creating a business case to justify participation in both data sharing and data use.

While Deloitte support the objective of establishing Data Sharing Agreements it will be important that this does not create a new barrier to data sharing.

The need to satisfy the ambiguously worded purpose test, the application of theoretical safeguards, the determining of specific risk mitigation controls and creating the Data Sharing Agreement will require skills and education that a large number of Commonwealth staff do not currently possess. Without training and resourcing of participants, the act of data sharing and release will revert to those individuals with formal data training, or specific roles within crucial departments. In this circumstance, the intent of the legislation to broaden the application of data sharing and use may not be realised.

For example, it is possible some agreements will require a disproportionate amount of time to prepare and result in prohibitive costs. There may also be a risk that, should the development of Data Sharing Agreements be too onerous on participants, they may result in effectively institutionalising barriers that already exist to public sector data sharing, and therefore conflict with the underlying intentions of the legislation.

[56] Discussion Paper, page 36

To help avoid this the Commissioner could gather information on factors, such as the level of detail included in the Data Sharing Agreements, the length of time taken to complete them, and the key factors contributing to this, to assess whether the level of information required for Data Sharing Agreements is appropriate and consistent with the intent of the DS&R legislation.

The lack of clarity around the minimum specifications required to enact an agreement formally may lead to individual organisations, or participants, engaging in unnecessary and costly legal activity based on perceptions of the minimum requirements needed to conform with the DS&R legislation.

In order to ensure data sharing is streamlined and agreements are efficiently developed, we recommend that the mandatory terms of the agreements are concise, and any guidance provided in relation to the development of these agreements promotes the use of clear, simple language.

One of the proposed mandatory terms for Data Sharing Agreements is that the agreement describes in detail how the data sharing meets the purpose test. As we have noted in sections 3.2 and 4.5, there are two objectives that the 'purpose' test should meet. The purpose should be defined in sufficient detail so that data is not improperly shared by Data Custodians, but not in such detail the data minimisation requirement limits the data made available or that the detailed purpose provided precludes unanticipated uses that emerge from the analysis of the shared data.

As noted in section 4.5, if Data Custodians interpret 'data that is reasonably necessary' too broadly, there is a risk that privacy will be compromised. However if 'data minimisation' is applied too strictly, together potentially with a restrictive interpretation of the purpose, then data may not be made available to data recipients which could result in data sharing and release practices which fail to 'unlock the full potential' of public sector data.

In addition to the permitted and precluded purposes, and the data minimisation requirement, the discussion paper also outlines a number of other parameters that Data Custodians are required to consider before sharing data: what project the data will be used for, how detailed the data is, how the data will be protected, who will use the data, and whether outputs can be published without identifying individuals or businesses.[57]

There is a risk that these requirements place an unfair burden on members of the public sector who are not equipped for this responsibility. The ability to assess the safe and secure environment for the data analysis and use may be out of the professional skills and expertise of the Data Custodian.

The requirement for all Data Sharing Principles to be satisfied prior to data being exchanged has contributed to the current low levels of data sharing in the public sector. The DS&R legislation intends to remove the uncertainty and concerns around breaching privacy and sharing principles that currently impede data sharing.

Another proposed mandatory term for Data Sharing Agreements is the inclusion of information on what happens to data after the agreement ends. It will be important that this requirement is flexible enough to enable the preservation of new data assets that are created as a result of the aggregation of data shared by one or more Data Custodians with an Accredited User.

Deloitte recommend that the National Data Commissioner develop guidance to assist participants in understanding the purpose test, the 'data minimisation' concept, and their impact on the level of detailed description required in a Data Sharing Agreement, together with the other requirements of a Data Sharing Agreement.

This provision of this guidance would support the objectives of the DS&R legislation of having 'a clear, consistent and transparent approach' to data sharing which 'unlocks the full potential' of public sector data.

Publication of Data Sharing Agreements on a public register

The discussion paper notes that Data Sharing Agreements will be published by the Commissioner on a searchable public register which is accessible by both participants, the government and the public. This is being done to promote transparency and accountability.

[57] Discussion Paper, page 29

According to the PIA, it is proposed that the Bill will require Data Sharing Agreements to be published:

- By the sharing entity (i.e. Data Custodian or Accredited Data Service Provider, or as agreed between the parties).
- As soon as practicable once the Agreement is made (i.e. Agreement signed by all parties).
- In the form and location prescribed by the National Data Commissioner.
- In full, unless a full or partial exception applies to the extent that the document contains protected or confidential information that cannot be redacted.

Deloitte supports the publication of these agreements as a measure to improve transparency and accountability, particularly where the type of data that is subject to the agreement concerns individuals.

We see their inclusion in a searchable register held by the National Data Commissioner as aligning with the principle of public by default, providing a mechanism to build and maintain public trust and also as an opportunity to empower the Commissioner through valuable insights into how the DS&R is being effected.

To promote simplicity, efficiency, and transparency, we recommend considering user-centric methods to both the creation of the Data Sharing Agreements and the presentation of the public register of Agreements.

It will also be important that the public register is supported by appropriate technology and processes and adequate resources, including personnel.

Public registers of Accredited Users and Accredited Data Service Providers (Section 5.4)

Deloitte supports the maintenance of a public register of accredited data users and accredited data service providers. The register of accredited data users – both organisations and individuals – would need close to real time updating to be effective.

However, we note that the accreditation of individuals and their inclusion on a public register introduces several challenges. These are discussed in Operational framework for accreditation (Section 6.4)

Annual reports on the data sharing system (Section 5.5)

Deloitte supports the publishing of an annual report on the operation and integrity of the data sharing system. We note that this will operate in parallel with the register of data sharing requests and the register of accredited data users and accredited data service providers.

As noted in section 2.5, Deloitte recommend that the annual report on the data sharing system also report on the uses to which data sharing was applied and best practices and success stories.

The inclusion of these matters in an annual report would result in data sharing and release being seen as more than a compliance exercise and contribute to the desired cultural change by highlighting the benefits that were realised from data sharing and release.

Data breach scheme (Section 5.6)

The discussion papers note that the 'Data Sharing and Release legislation requires a different kind of notification scheme for the vast range of data falling outside the *Privacy Act 1998* notifications scheme'.[58]

We support the development of a data breach scheme for the DS&R legislation, and recommend, where possible, that the scheme be consistent with but strengthen the Notifiable Data Breaches Scheme (NDBS) in the *Privacy Act 1988*.

While noting that the NDBS will continue to apply to personal information shared under the legislation, and that different processes may be required for different kinds of public sector data that is not personal information, aligning the data breach scheme where possible with the NDBS promotes consistency.

The development of prescribed notification obligations and accompanying guidance, like that published by the Office of the Australian Information Commissioner, is important. For example, the processes for responding to data breaches which will be set out in individual Data Sharing Agreements, should provide clarity on the obligations of each party and which party is responsible for which response actions.

[58] Discussion Paper, page 37

6 National Data Commissioner's oversight of the Data System

We support the intention to appoint a National Data Commissioner. The independence given to the statutory authority for this office is significant and essential. However, the responsibility for the Commissioner to simultaneously advocate, regulate and oversee the data sharing system could compromise the effectiveness of this role.

Objectives and functions of the National Data Commissioner (Section 6.2)

Deloitte supports the creation of an independent National Data Commissioner to drive change and support best practice. This will be an important role in achieving the government's vision that open data will become 'one of the next great enablers of modern digital economies and better government'.[59]

The discussion paper highlights the importance of the public service culture making the paradigm shift from 'need to know' to 'responsibility to share' where there is a clear public benefit. We believe that this is an important objective for the legislation and for the role of the Commissioner.

However existing mandates and directives have failed to realise this paradigm change despite it being an intent since the original adoption of data sharing and release in the public sector. This may be, in part, because this ambition is ambiguous and calls for participants to make judgement calls rather than defer to guidelines and rules.

We recommend that the data sharing and release framework consider whether greater and more prescriptive direction and clarity is required to ensure the desired paradigm shift occurs.

National Data Commissioner as advocate

The discussion paper highlights the role of the National Data Commissioner to 'advocate', 'champion', 'drive', 'promote' and 'support' greater data sharing and release. These are important roles in contributing to the paradigm shift from 'need to know' to 'responsibility to share'.

However, there is a risk that the Commissioner's role as an advocate compromises its effectiveness in its role as a regulatory authority and its role to objectively assess the effectiveness of the data sharing system.

Even if these other roles are not compromised, perceptions of a conflict of interest may undermine the community's and the public sector's confidence in the data sharing system.

The Commissioner will have responsibility for training accredited users, accredited data service providers and data custodians. There is a risk that this will result in a conflict or the perception of a conflict with the Commissioner's role as a regulatory authority and compromise its ability to enforce regulations or prosecute breaches of the DS&R legislation where the actions of individuals or organisations have been based on training provided by the Commissioner.

The Commissioner will have responsibility for advising government agencies on how to apply the data sharing principles. There is a risk that this will result in a conflict or the perception of a conflict with the Commissioner's role as a regulatory authority and compromise its ability to enforce regulations or prosecute breaches of the DS&R legislation where the actions of individuals or organisations have been based on advice from the Commissioner on how to apply the data sharing principles.

[59] Department of the Prime Minister and Cabinet, 2017

National Data Commissioner as regulatory authority

The discussion paper also outlines the role of the Commissioner to 'regulate the system in a manner that promotes trust' and notes that the Commissioner will be granted 'regulatory powers necessary to enforce the legislation, including monitoring and investigatory measures'.[60]

In general, the approach of the Commissioner in undertaking its regulatory responsibilities should:

- Ensure relevant requirements in new regulations are **consistent** with equivalent requirements in existing regulations.
- **Align** regulations with international standards, unless there is a strong rationale to do otherwise.
- Encourage the **design** of less prescriptive regulation.
- Ensure that there are appropriate and **effective enforcement** mechanisms consistent with an emphasis on outcome-based regulation.
- Maintain a **culture** which emphasises outcome-based regulation.
- Boost the **accountability** of regulators.
- Encourage regulated entities to actively explore better ways of meeting the objectives of regulation.

The Commissioner will have the power to accredit users – both organisations and individuals – and data service providers. There is a risk that this will result in a conflict or the perception of a conflict with the Commissioner's role as an advocate for data sharing.

The Commissioner will have responsibility for monitoring compliance with the DS&R legislation, including conducting assessments and investigations. There is a risk that this will result in a conflict or the perception of a conflict with the Commissioner's role as an advocate for data sharing.

The Commissioner will have responsibility for determining whether there have been breaches of the DS&R legislation, enforcing the legislation and imposing penalties. It is not clear that it is appropriate to have a single role responsible for determining both whether there has been a breach of the law and what the penalty should be. We recommend that the process for determining whether there has been a breach of the DS&R legislation is reviewed to ensure that it is consistent with other equivalent legislative requirements, including the approach taken by the OAIC. In addition, there is a risk that this will result in a conflict or the perception of a conflict with the Commissioner's role as an advocate for data sharing and its role overseeing and assessing the effectiveness of the data sharing system.

The Commissioner will have the power to issue binding guidance, as well as non-binding guidance and advice, on the application of the Data Sharing and Release framework.

The discussion paper notes that the Data Codes, which will be the form in which the binding guidance is issued, will be legislative instruments. For the issue of legislated binding data codes to be effective, it will require a regulator that assesses compliance with the legislation and has the ability to apply penalties for non-compliance.

The overlap of, and the distinction between, the 'Rules' and binding guidance issued by the Commissioner and non-binding guidance may create further uncertainty.

However, the discussion paper also notes that 'the National Data Commissioner will not be able to compel or overturn decisions to share or not to share'. Given the paradigm shift that the DS&R legislation is seeking to create and the vision for it to be an 'enabler of modern digital economies and better government' we recommend that the Commissioner (or any alternate body undertaking the regulatory or oversight role) be given greater powers to review the decisions of government departments about sharing data. The existence of an independent review process is likely to contribute to more thoughtful and reasoned consideration by government departments making decisions to share or not to share data.

The discussion paper also notes that the Commissioner's activities will be 'aimed at voluntary compliance with the legislation' escalating to a 'graduated enforcement model'. This is a delicate balance. For the legislation to be effective there needs to be both effective enforcement and accountability of participants, and regulators. However, to support the cultural shift to 'responsibility to share', the enforcement of the

[60] Discussion Paper, Section 6.2, page 39, and Section 7.5, page 50

DS&R regulation needs to not contribute to the culture of fear that has impeded efforts to date to drive greater benefits from data sharing.

In addition, the discussion paper notes the collaboration with other regulators including the Office of Australian Information Commissioner (OAIC), the Commonwealth Ombudsman and the Australian Competition and Consumer Commission (ACCC) and its international counterparts to minimise duplication and regulatory burdens.

We support these actions and the contribution they have to ensuring the requirements of the new DS&R legislation are **consistent** with equivalent requirements in existing regulations and **aligned** with international standards.

Equally, it will be important that in the DS&R legislation, there is a clear delineation of roles and responsibilities of the Commissioner and other regulators.

National Data Commissioner as assessor

The Commissioner has a further role in overseeing and assessing the effectiveness of the data sharing system. This would seem to require the Commissioner to self-assess its effectiveness as an advocate and as a regulatory authority. To promote greater accountability of the Commissioner as regulator consideration could be given to undertaking an independent review of the Commissioners' performance within the data sharing system.

There is an opportunity for the Commissioner to make an early assessment of systemic barriers to greater data sharing and initiate or advocate for actions to address them.

These three proposed roles of advocate, regulatory authority and assessor seem to introduce a significant risk of actual or perceived conflict. For example, there is a risk that perceptions of the effectiveness of the Commissioner as a regulator are compromised by its activities in its role as an advocate.

We recommend that further consideration be given to the breadth of the roles assigned to the Commissioner. If these three potentially conflicting roles are retained by the Commissioner, we recommend that clear definitions and expectations are set out for each of the roles of advocate, regulatory authority and assessor to support the ability of the Commissioner's role and the framework to achieve the cultural transformation intended through the introduction of the DS&R legislation.

Oversight through accreditation (Section 6.3)

The introduction of an accreditation scheme will result in significant additional obligations for the office of the National Data Commissioner.

As an advocate for data sharing the Commissioner will be required to promote and support best practice data sharing.

As a regulator the Commissioner will be required to assess, monitor and possibly amend or revoke accreditation across the entire Commonwealth public sector. These obligations will then extend to subsequent jurisdictions and entities as they are permitted to participate.

The efforts required to create, maintain, monitor and regulate a federal, and then national, data sharing and release accreditation scheme will require significant resources, staff and funds if this role is to be effective.

Two examples highlight the challenges that this change in role will present.

The ACCC's remit has recently been extended to include accreditation of data recipients under the Consumer Data Right legislation and the maintenance of a register of accredited data recipients. This required the development of new capability and skills in the ACCC and the development of a new accreditation process and system.

Secondly, the maintenance and operation of a single accreditation process in a single state for weapons licensing has presented significant challenges, with the processing of monitoring of a single form currently several months behind schedule.

Another consideration of the accreditation process and registry will be around the technology platform utilised to facilitate the initial administration, the routine checks and the overall accessibility to every participant's details and responses for compliance. The need to either employ a self-regulatory system where participants are asked to self-disclose their skills, capacity to protect, data management experience and privacy knowledge, or the requirement to engage staff and automated technologies with a compliance checking parameter are both imperfect and will take substantial time to create and operate.

We support the requirement for all participants to have effective governance. A lack of governance clarity is currently a problem in the public sector and is one of the acknowledged barriers to data sharing and release. We support the requirement to have the right organisational authority, policies and administrative processes to support accountability and ethical decision making in data management and use as part of the accreditation process for organisations. However, the introduction of effective governance process and systems will be costly and labour intensive and will require appropriate funding for government organisations.

Operational framework for accreditation (Section 6.4)

Deloitte supports the need to identify and authorise Data Custodians and users involved in data sharing and provide clarity on their roles and responsibilities within the National Data System.

The discussion paper notes the intention to introduce a dual-level accreditation under which both organisations and specific individuals will need to be accredited by the Commissioner. The discussion paper proposes that the accreditation of individuals will be valid for three years and that of organisations for five years.

The dual-level accreditation proposal is based on specific feedback from earlier consultations and is intended to provide independent system-wide assurance to Data Custodians when assessing data requests.

We have significant concerns with this proposed approach.

The accreditation of individuals will require the creation of a register of accredited individuals. However, this raises several practical questions: Should an individual's accreditation continue if they have changed roles? If they have changed employer? Which employer will be responsible for vouching for an accredited individual user? What obligations will employers have to notify the Commissioner of changes to this register? What information will be retained to enable the authentication of an accredited individual requesting access to data?

The mere act of accrediting a Data Custodian or user does not ensure that these individuals are 'properly qualified to handle personal information'.

Individuals are employed by organisations and are typically required to follow an organisation's standard operating procedures. If a department has a legitimate need to either share, release or use data, then it is not clear that it is also necessary to accredit the individual user who is acting on behalf of the accredited organisational user. In addition, it is unclear what the consequences would be for an accredited individual who has breached the DS&R legislation as a result of following an organisation's standard operating procedures.

The discussion paper notes that accredited organisations will need to have 'facilities, processes and governance' in order to be an accredited user. Individuals will require 'skills and training' and to have been touched by an accredited user organisation in order to be accredited themselves. Given that at least some of the training would be provided by the Commissioner, and the Commissioner's broader role in the education and upskilling of the public sector, this creates ambiguity on where responsibility for skills gap analysis and training falls between the individual, organisations, and the Commissioner.[61]

Another consideration for the accreditation process is the right of appeal if an applicant is denied accreditation or if a legitimate use-case proposed for the data is rejected. The discussion paper does not specify the appeals process or the jurisdiction.

[61] Discussion Paper, pages 17, 41 and 45

The discussion paper is also silent on the expected impost in achieving or maintaining accreditation or establishing and participating in any appeals process. These elements are important to ensuring the accreditation is streamlined and perceived to be fair, equitable and transparent to maintain public trust and operate as an effective element of the data sharing framework.

The discussion paper acknowledges that the government is 'continuing to address…questions and concerns' about the dual-accreditation proposal. As the discussion paper notes 'it is critical that we get this right'.

The definitions and parameters surrounding the satisfactory accreditation of Users and Data Service Providers must be clarified. It is unclear what the minimum acceptable level of technical and capability requirements will be.

The discussion paper states that 'High risk integration projects must be done by Accredited Data Service Providers to ensure existing protections around data integration are maintained and strengthened'.[62]

The inclusion of the term 'high risk data integration' lacks definition and clarity and may involve sensitivity of data, privacy concerns, the volume or complexity of the data, the entities involved in the transaction, the location of the participants, and/or the declared purpose/intent and outcomes of the use. The discussion paper notes that the Office of the National Data Commissioner will provide further guidance on what 'high risk data integration' involves.

While noting the concerns of data users outlined in the discussion paper, the adoption of joint legal responsibilities between both parties for managing the data sharing may also place an unfair burden on data custodians for the actions of the accredited users. We agree that Data Custodians should maintain liability for undertaking due diligence in the development and establishment of the data sharing agreement. However, liability for future actions that may not have been considered in the agreement should rest with the Accredited User. The requirement for the Data Custodian to lodge the Data Sharing Agreement is clear and supported under standard contract management principles. Guidance should also be provided in relation to the respective obligations of each of the parties.

Q10. Are the core principles guiding the development of accreditation criteria comprehensive? How else could we improve and make them fit for the future?

This question has been addressed in our comments above.

Q11. Are there adequate transparency and accountability mechanisms built into the framework, including Data Sharing Agreements, public registers and National Data Commissioner review and reporting requirements?

This question has been addressed in our comments above.

[62] Discussion Paper, page 44

Q14. What types of guidance and ongoing support from the National Data Commissioner will provide assurance and enable safe sharing of data?

As highlighted in our submission key areas that would benefit from increased clarity and guidance are:

- The Advisory Council - including the mechanism for member selection, recruitment processes and roles of the Committee Members, performance indicators and criteria for assessing the Council's operating effectiveness.
- Legislative overlap.
- The application of the Principles including permitted purposes, the data minimisation concept, classification of data and the level of detail required in Data Sharing Agreements.
- Consideration of consent.
- Accreditation of Users and Data Service Providers.
- The operation of joint legal obligations.
- Reporting obligations.

7 When things go wrong

Deloitte supports the graduated approach to enforcement under the Data Sharing and Release legislation given its contribution to achieving a paradigm shift in the culture of the Australian Public Service to data sharing and release.

The discussion paper highlights the importance of the public service culture making the paradigm shift from 'need to know' to 'responsibility to share' where there is a clear public benefit.

However, it also notes that 'government agencies are confused and uncertain about the existing mechanisms and lack the confidence to use them'. It further notes that the government 'currently shares public sector data through various laws and mechanisms developed at various points in time, with little consistency or a single point of oversight'.[63]

The discussion paper also notes the feedback received from earlier consultations on the importance of addressing 'the 'grey areas' between freedom of information, privacy and data sharing laws' and the need for 'consistent definitions to reduce possible confusion'.

We have noted the importance of appropriate and effective enforcement mechanisms consistent with an emphasis on outcome-based regulation and accountability of regulators.

This is a delicate balance.

If enforcement of the legislation is too loose, there is a risk that trust, and privacy are undermined as data holders share information inappropriately. This also risks undermining the credibility of, and confidence in the role of the Commissioner as regulator.

As has been recently highlighted by the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry, without enough enforcement there is a risk that compliance can be perceived as voluntary.

However, enforcement cannot be so strong as to deter data sharing under the legislation, or to be disproportionately punitive. If enforcement of the legislation is too strict, there is a risk that data holders will not have the confidence to share information with accredited data users. To support the cultural shift to 'responsibility to share', the enforcement of the DS&R legislation and regulations needs to not contribute to the culture of fear that has impeded efforts to date to drive greater benefits from data sharing.

We support the proposal to adopt a graduated enforcement approach where the Commissioner's activities will be 'aimed at voluntary compliance with the legislation' escalating to a 'graduated enforcement model' and guided by the principles of fairness, independence and accountability.

Deloitte acknowledges the need for the National Data Commissioner to build data sharing capacity and provide education and guidance in the first instance and supports the identification of annual priorities to assist in building capabilities and identifying areas where the risk of non-compliance is high.

We also support the objective set out in the discussion paper that, where possible, consistency with comparable legislation, including the *Privacy Act 1988* and the *Freedom of Information Act 1982*, should be a primary consideration.

Consideration should be given to how Data Custodians, Accredited Data Service Providers, and Accredited Users are to be assessed for compliance with the legislation and accreditation terms.

[63] Discussion Paper, page 17

Subject to our comments on the role of the National Data Commissioner in Section 6, we support the granting of regulatory powers to the National Data Commissioner, including monitoring and investigatory powers, to assess compliance with the Data Sharing and Release legislation, and emphasise the importance of these powers being exercised in a timely manner (for example, to assess compliance of Data Sharing Agreements at the time they are created).

There should be clear understanding and transparency between data and privacy regulators of how they will collaborate and work together.

Q12. Have we achieved the right balance between complaints, redress options and review rights?

This question has been addressed in our comments above.

Q13. Have we got our approach to enforcement and penalties right for when things go wrong? Will it deter non-compliance while encouraging greater data sharing?

We support the proposal to adopt a graduated enforcement approach where the Commissioner's activities will be 'aimed at voluntary compliance with the legislation' escalating to a 'graduated enforcement model' and guided by the principles of fairness, independence and accountability.

Contact us

Kylie Watson
Lead Partner, Federal Government Public Sector
Partner, Cyber, Data and Analytics
+61 2 6263 7450
kywatson@deloitte.com.au

Deanna Gibbs
Senior Manager, Federal Government Public Sector
+61 2 6263 7595
degibbs@deloitte.com.au

Paul Wiebusch
Lead Partner, Open Data
+61 3 9671 7080
pwiebusch@deloitte.com.au

Jamie Leach
Director, Open Data
+61 7 3308 7469
jleach@deloitte.com.au

Ellen Derrick
National Leader, Public Sector
+61 2 6263 7069
ederrick@deloitte.com.au

Ursula Brennan
Lead Partner, NSW Public Sector
+61 2 9322 5573
ubrennan@deloitte.com.au

Helena Hamilton
Lead Partner, Victorian Public Sector
Partner, Data
+61 3 9671 6323
helenahamilton@deloitte.com.au

Kellie Nutall
Lead Partner, Queensland Public Sector
Partner, Data
+61 7 3308 7075
knuttall@deloitte.com.au

Marion Burchell
Director, WA Public Sector
Director, Data
+61 8 9365 7841
mburchell@deloitte.com.au

John O'Mahoney
Partner, Deloitte Access Economics
+61 2 9322 7877
joomahony@deloitte.com.au

Danielle Kafouris
Partner, Data, Privacy and Security
+61 3 9671 7658
dakafouris@deloitte.com.au

Ben Walker
Director, Privacy
+61 413 623 772
bwalker@Deloitte.com.au

Deloitte.