galexia

Australian Government

Department of the Prime Minister and Cabinet

Galexia Privacy Impact Assessment on the Proposed *Data Sharing and Release (DS&R) Bill* and Related Regulatory Framework

[FINAL]

28 June 2019

(GC540)

Contact: Galexia
Level 11, 175 Pitt St, Sydney NSW 2000
Ph: +61 2 9660 1111
www.galexia.com
Email: manage@galexia.com

Document Control

Client

This document has been written for the Department of the Prime Minister and Cabinet (DPMC).

Document Purpose

This is a Privacy Impact Assessment (PIA) on the proposed policy settings and related legislative reforms surrounding the *Data Sharing & Release Framework*.

Document Identification

Document title	DPMC – PIA on Proposed *Data Sharing & Release Bill* and Related Regulatory Framework
Document filename	gc540_dpmc_dsr_bill_galexia_PIA_v7_20190628_FINAL.docx
Client Details	**Department of the Prime Minister & Cabinet** <www.pmc.gov.au>
Client contact	e: datalegislation@pmc.gov.au
Consultant Details	**Galexia** <www.galexia.com> Level 11, 175 Pitt St, Sydney NSW 2000, Australia p: +612 9660 1111 e: manage@galexia.com
Galexia Contact	**Peter van Dijk** (Managing Director) m: +61 419 351 374
Galexia Reference	GC540
Project email	dsr@galexia.com

Contents

1. Executive Summary

Galexia has completed this Privacy Impact Assessment (*PIA*) on the proposed policy settings and related legislative reforms surrounding the *Data Sharing & Release Framework.*

This PIA has been prepared prior to the finalisation of the *Data Sharing & Release Bill*, so that the development of the legislative package will be able to benefit from recommendations and advice in this PIA – and subsequent feedback and consultation in the release of a subsequent discussion paper in July/August 2019. This is part of the Department of the Prime Minister & Cabinet's iterative approach to the development of the *Data Sharing & Release Framework*.

This report has been prepared based on information available as at June 2019, including:

- The Issues Paper (July 2018);[1]
- Internal Policy Papers and meetings with the DPMC team (from July 2018 to June 2019);
- Drafting instructions;
- Public Submissions to the Issues Paper;
- Additional written submissions provided by some stakeholders;[2] and
- Targeted stakeholder consultation.[3]

The purpose of this PIA is to assist in identifying and managing privacy issues that are raised by the proposed framework for the sharing and release of data that will be facilitated by the *Data Sharing & Release Bill*. The key proposals are:

1) To enable a range of data sharing and data release activities for permitted purposes; and
2) To create an effective governance framework for the proposed data sharing and the release of public sector data.

This PIA has been conducted in accordance with PIA Guidelines issued by the Office of the Australian Information Commissioner.[4]

This PIA considers alignment with privacy legislation, user acceptance and public perception issues. This PIA makes a broad range of recommendations for mitigating privacy risks, including changes to the design and content of the proposed legislative framework, practical privacy compliance steps and enhanced privacy governance arrangements.

Information contained in this PIA is based on:

- Meetings with the Department of the Prime Minister & Cabinet (DPMC), including senior management, policy staff and the privacy compliance team;
- Meetings with Commonwealth, State and Territory Privacy Commissioners (further details included in Appendix 3 – Stakeholder Consultation);
- Meetings with Privacy and Consumer Advocacy Organisations (further details included in Appendix 3 – Stakeholder Consultation);
- Documentation related to the proposal (further details included in Appendix 2 – Key documents);
- General research and literature review on privacy and data sharing / data release issues; and
- Review of relevant privacy legislation and guidelines.

[1] Department of the Prime Minister and Cabinet, *New Australian Government Data Sharing and Release Legislation: Issues paper for consultation* (4 July 2018) <www.pmc.gov.au/resource-centre/public-data/issues-paper-data-sharing-release-legislation>.

[2] <www.pmc.gov.au/public-data/data-sharing-and-release-reforms/submissions>.

[3] Refer to Appendix 3 – Stakeholder Consultation.

[4] Office of the Australian Information Commissioner, Australian Government, *Guide to undertaking privacy impact assessments* (May 2014) <www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments>.

As this PIA does not concern a specific set of personal data or a specific data sharing or data release proposal, it has been designed to provide high level advice that could help develop the legislative framework to accommodate a range of data sharing and data release scenarios.

Galexia's advice in this PIA concentrates on the following areas:

- **High level privacy protections in the proposed Bill** – This PIA assesses the high level privacy protections that are likely to appear in the proposed Bill or other parts of the proposed regulatory framework, and makes some recommendations for strengthening these protections;
- **Privacy legislation alignment** – This PIA assesses the proposed sharing / release of data against the Australian Privacy Principles (*APPs*) in the *Privacy Act 1988,* and makes some recommendations for how alignment could be further enhanced; and
- **Governance** – This PIA considers key privacy governance steps that could be implemented to ensure the ongoing protection of privacy once the data sharing / data release arrangements are operational.
- **Social licence** – This PIA considers the key factors that might influence the development of community trust, confidence and acceptance – known as a social licence.

2. Summary of Key Findings and Recommendations

2.1. Key Policy Positions

2.1.1. Overview

Privacy issues identified in this PIA can be split into Key Policy Positions that need to be addressed in the development of the proposed *Data Sharing & Release Regulatory Framework* (discussed in this section), or more specific privacy issues that relate to compliance with specific APPs in the *Privacy Act* (discussed in the next section).

These high level recommendations for the Key Policy Positions are based on draft policy papers and drafting instructions that were made available at the time of preparing this report (June 2019).

Iterative approach to the development of the *Data Sharing & Release Framework*

The Department of the Prime Minister & Cabinet (the Department) has approached the Privacy Impact Assessment as an iterative process and a critical component to their privacy-by-design approach to developing the policy and legislative reforms. For this reason, the Department sought to conduct an independent PIA on the framework prior to legislation.

The iterative and consultative approach to designing the legislative framework is designed to facilitate privacy protections. A range of perspectives are considered throughout the design process and are built into the final products. This approach is crucial to design a legislative framework that meets users' needs and community expectations now and into the future, and to build public support for government data initiatives.

This PIA of the proposed framework is an integral part of the design process for the reform package. This PIA was commissioned at the start of the design process, and advice provided to the Department during the PIA process has informed development of positions proposed in the framework. The findings of this PIA will inform development of the draft legislation, ensuring privacy protections are built into the final framework.

Privacy positive measures

The *DS&R Framework* is being developed in a way that is designed to 'build in' privacy protections, and the proposed legislative reforms include a number of positive privacy measures. These include:

- a range of measures to increase openness and transparency, beyond those already required in the *Privacy Act*;
- the inclusion of a purpose test that limits data sharing activities to short set of permitted purposes that are generally low risk and within community expectations;
- the inclusion of a list of precluded purposes;
- the complete exclusion of law enforcement and national security related activities;
- limitations on some commercial access to and use of the data;
- the inclusion of a data minimisation requirement, beyond the data minimisation requirement for collection that is already required in the *Privacy Act*;
- the inclusion of an accreditation regime for participants;
- incorporation of the Data Sharing Principles / Five Safes Framework, which include additional privacy safeguards; and
- the inclusion of a compliance monitoring and enforcement regime, with appropriate sanctions.

Additional recommended high level privacy enhancements

However, there are three Key Policy Positions where the proposed *Data Sharing & Release Bill* would benefit from further high level privacy enhancements:

- **Key Policy Position 1: Distinguishing between data *sharing* and data *release***
  The requirements in the Bill for data sharing and data release should be split, so that each activity has its own stand-alone set of requirements, tailored for that activity;
  - Recommendation 1: Splitting data sharing and data release requirements
  - Recommendation 2: Enhanced privacy safeguards for data release
- **Key Policy Position 2: Compliance activities**
  The Bill should continue to exclude compliance activities related to an individual as an approved purpose for data sharing or data release;
  - Recommendation 3: Exclusion of compliance activities
- **Key Policy Position 3: Covering the States and Territories**
  The Bill should include an equivalence test for organisations that are already subject to appropriate State and Territory privacy legislation, subject to additional measures regarding data breach notification requirements.
  - Recommendation 4: Additional Data Breach Notification requirements

2.1.2. Key Policy Position 1: Distinguishing between data sharing and data release

Recommendation 1: Splitting data sharing and data release requirements

The requirements in the Bill for data sharing and data release should be split, so that each activity has its own stand-alone set of requirements, tailored for that activity.

This issue primarily arises out of stakeholder submissions and consultations, where it has become clear that there is some confusion between the concepts of **data sharing** and **data release.** It has also become clear that privacy concerns are much stronger regarding data release than data sharing.

The Issues Paper (July 2018)[5] proposed to treat data sharing and data release as a package of activity that will be governed by certain common requirements in the Bill. These included the Purpose Test and the safeguard principles (now known as the Data Sharing Principles[6]). Some differentiation was envisaged in the application of the Data Sharing Principles, but this would be left to Rules or Guidance developed by the regulator.

During the course of consulting stakeholders and refining the proposed Framework, the Department has considered several alternative options for managing the distinction between data sharing and data release.

Currently, the proposed Framework is being developed on the basis that data release will **not** be the subject of a specific authorisation in the Bill. It is proposed that the legislation will support release of public sector data without providing an authority to release it, as this would unnecessarily duplicate existing mechanisms. The proposed National Data Commissioner will champion greater release of data through their advocacy and guidance functions. This will include working within government and with other regulators to improve the culture and practices around release, and developing best practice guidance.

The Framework is likely to define the two activities as follows:[7]

- **Data sharing**: means providing access to data to specific recipients in a controlled manner.
- **Data release:** means disclosing data publicly (such as through tables published on an open data portal).

Galexia's view is that the legislation should include a clear split between data *sharing* and data *release*.

The two activities should be separate parts of the legislation and subject to separate, customised requirements. While there may be some overlap and duplication, this is unlikely to be a significant burden. The benefits of this approach are numerous:

- The split will deliver greater clarity over the distinction between data sharing and data release;
- The split will allow requirements to be customised to the particular privacy risks of data sharing and data release; and
- The split may allow a different approach to implementation, including the start date and / or transitional arrangements.

We note that some key stakeholders oppose including data release in the *DS&R Framework* at all, as they have concerns about the re-identification of data that has been released in the form of unit level records. However, in this PIA, Galexia supports a clear split in the legislation, with separate regimes for **data sharing** and **data release**.

[5] Department of the Prime Minister and Cabinet, *New Australian Government Data Sharing and Release Legislation: Issues paper for consultation* (4 July 2018) <www.pmc.gov.au/resource-centre/public-data/issues-paper-data-sharing-release-legislation>.

[6] Department of the Prime Minister and Cabinet, Australian Government, *Best Practice Guide to Applying Data Sharing Principles* (19 March 2019) <www.pmc.gov.au/resource-centre/public-data/data-sharing-principles>.

[7] Information available from the Department, 21 June 2019.

This PIA recommends that the following additional privacy safeguards could be considered for data release:

1) **Additional public interest test**
Any authority for data release could directly incorporate consideration of the public interest.

2) Data custodian veto mechanism
For data release (not data sharing) the original data custodian should retain a veto power over the potential release of data that it provided. For example, the original data custodian would have the right to prevent the data release if they had concerns over privacy or security.

3) Enhanced sanctions
The current proposed Framework includes a combination of two approaches to sanctions and penalties.

- The first approach is that if a Data Sharing Entity acts in a manner not authorised by the legislation, they lose the authority to share or release data under the Bill and the action would 'rebound' to the prohibitions and penalty framework in the original data custodian's secrecy or non-disclosure provisions.
- The second approach is that where there are 'gaps', the legislation would provide its own penalty regime. The penalty regime in the proposed legislation differentiates between lesser and serious breaches, with corresponding penalties.

This PIA suggests that if data release is authorised by the legislation, any breach related to data release should be considered a serious breach for the purpose of the penalty regime.

Recommendation 2: Enhanced privacy safeguards for data release

If data release is authorised by the legislation, then additional legislated enhanced privacy safeguards for data release will be required. These should include:

1) An additional public interest test;
2) A data custodian veto power; and
3) Enhanced sanctions.

2.1.3. Key Policy Position 2: Compliance activities

Recommendation 3: Exclusion of compliance activities

The Bill should exclude compliance activities related to an individual as an approved purpose for data sharing or data release.

This issue primarily arises out of stakeholder submissions and consultations, where it has become clear that there is little support for including compliance activities. Stakeholders are concerned that the privacy risks associated with compliance are much greater, as the consequences for individuals can be significant.

During the development of the *DS&R Framework* there has been consideration of – both including and excluding – compliance activities. At the time of preparing this report (June 2019) the Department envisages the full exclusion of compliance activities.

Galexia has several concerns regarding any potential inclusion of compliance activities that target individuals in the Bill.

The inclusion of *'compliance'* as a purpose is probably the most contentious issue in the design and implementation of the *DS&R Bill*, and raises a number of challenges:

- Compliance is difficult to define;
- There is limited support amongst stakeholders for the inclusion of compliance as an allowable purpose;
- Compliance requires greater identification of individuals – and therefore raises the privacy risk profile of the *DS&R Bill*;
- Compliance implies that there are likely to be consequences for individuals or small groups – and this is a departure from the other allowable purposes;
- Compliance appears to be a poor fit for the Five Safes / Data Sharing Principles Framework – which is designed to operate for general research / public benefit activities;
- Compliance activities will place significant pressure on data quality, especially in areas such as data matching from diverse sources;
- Compliance activities will place considerable pressure on the timeliness of data, which is not such a major issue in other permitted purposes such as research and program evaluation;
- Compliance is likely to require the collection and sharing of a greater quantity of data and may undermine or sideline the data minimisation principle; and
- Compliance has consequences for individuals – and is therefore likely to lead to significant complaints and disputes.

Overall, there is a risk that the inclusion of compliance that targets individuals will undermine wider support for the Bill. If compliance of this type is included, it is unlikely that the Bill will achieve any form of social licence or community acceptance, despite high levels of support for other activities covered by the Bill.

It is possible that there is some confusion regarding compliance activities targeted at an entire program or a large cohort of the population, rather than activities targeted at an individual or a small group. There may be some limited support for the former activity (for example, a data sharing activity that helps identify a broad pattern of fraud, that can then be separately addressed through other mechanisms). However, the Bill will have to clearly and carefully distinguish between the two.

The development of the legislation includes some proposed definitions:[8]

- ***Compliance activity:*** *is an action to examine, assess, inspect and investigate compliance with applicable legislation and organisational frameworks.*
- ***Assurance activity:*** *is an administrative action to assess specific individuals' and organisations' eligibility, entitlement, or liability for government programs and services.*

We note that data sharing for compliance purposes can still be achieved by other mechanisms. Compliance and assurance activities are important functions of government, but are more appropriately handled under dedicated legislative systems.

The Department's current position is that both compliance and assurance activities would NOT be permitted purposes in the legislation. Instead, activities would need to fall within the four categories of permitted purposes, one of which is Service Delivery.

If this approach is followed in the legislation, stakeholder concerns (and confusion) regarding compliance should be addressed.

[8] Department of the Prime Minister and Cabinet, Office of the National Data Commissioner, *Data Sharing Legislation – Policy Positions* (22 February 2019) [INTERNAL DOCUMENT].

2.1.4. Key Policy Position 3: Covering the States and Territories

The objective of the *DS&R Framework* is to allow organisations to participate in data sharing and data release activities that may not traditionally be covered by the requirements of the Commonwealth *Privacy Act* – such as small businesses or entities covered by State legislation. This is an important issue because many universities and university based research centres fall into these categories.

The Department intends for all participants covered by the *DS&R Framework* to have equivalent privacy obligations by being covered by the *Privacy Act 1988* or a comparable privacy regime. The proposed approach is to require specified participants (Data Custodians, Accredited Data Service Providers, and Accredited User Organisations) to meet one of the following requirements:[9]

> *Commonwealth and non-government entities must be subject to the Privacy Act 1988;*
>
> *State and Territory entities must either be subject to jurisdictional privacy legislation, or enter a Data Sharing Agreement, which provides:*
>
> > *1. protection for personal information;*
> >
> > *2. for monitoring compliance with the law or Agreement; and*
> >
> > *3. a means of redress for individuals if their personal information is dealt with in a manner contrary to law or the Agreement.*

This is a positive development, and this PIA broadly supports this approach.

However, one concern with the proposal to categorise State and Territory legislation as equivalent is that State privacy legislation does not currently include the type of data breach notification requirements that apply to organisations covered by the Commonwealth *Privacy Act*. If State and Territory legislation is to be considered equivalent, the proposed *Data Sharing & Release Bill* would need to add an additional requirement to bind participants to strict data breach notification requirements.

Some States and Territories may already be considering developing data breach regimes, but until these are implemented the Bill should impose these requirements directly. Developing the exact method for implementing this recommendation is likely to require further discussion with the States and Territories and detailed legal advice which is beyond the scope of this PIA.

Recommendation 4: Additional Data Breach Notification requirements

The Bill should include a mechanism for imposing a Data Breach Notification requirement where the entities involved operate in a State or Territory where such a requirement does not yet exist.

[9] Department of the Prime Minister and Cabinet, Office of the National Data Commissioner, *Data Sharing Legislation – Policy Positions* (22 February 2019) [INTERNAL DOCUMENT].

2.2. Summary of alignment with Australian Privacy Principles (APPs) and Other Privacy Components – Findings and Recommendations

The findings are high-level as this PIA does not concern a specific set of data or research proposal. It has been designed to provide high level advice that could assist the development of the legislative framework to accommodate a range of data sharing and data release activities. This PIA uses the APPs in the *Privacy Act* as a heading structure, but the *Data Sharing & Release Framework* will involve compliance with a range of privacy safeguards, not just the APPs.

These findings and recommendations are based on draft policy papers and drafting instructions available at the time of preparing this report.

The following table summarises the main findings, with links to further information and detailed discussion in the text:

Australian Privacy Principle (APP) / Privacy Component	Alignment	Findings Summary	Recommendation
Is the data 'personal information'?		Some of the data that is proposed to be shared / released will be linked to an individual, or can be linked to the correct individual. This PIA considers the sharing and release of both de-identified data and identified data, but the focus of this PIA is on identified data. Some key APP provisions (notably APP 1 and APP 11) need to be addressed for both identified and de-identified data. Some of the data also falls into the category of sensitive information. This has implications for compliance with APP 3 and APP 6 (discussed below).	
APP 1 – Openness and Transparent Management	Further Measures Possible	APP 1 requires Agencies to be open and transparent about their use of data sharing and the potential release of some data to external users such as researchers. Similarly, any entity that is accredited to receive data or carry out data integration activities as part of the proposed *Data Sharing & Release Bill* will also need to be open and transparent about their use of shared data and the source of data. In order to enhance openness and transparency, Agencies and any third party entity that is accredited to receive data or act as a Data Service Provider should be required to maintain a user friendly public information resource. **Note:** There is a further discussion of potential governance arrangements to assist in privacy compliance in Section 19. Governance (below.) These governance arrangements will also address openness and transparency and assist in compliance with APP 1.	**Recommendation 5. Improved openness in Privacy Policies about data sharing / release** Agencies and accredited entities should be more open about data sharing and the potential disclosure of some data to external users. **Recommendation 6: Establish user friendly public information resources** The National Data Commissioner and any third party entity that is accredited to receive data or act as a Data Service Provider should be required to maintain a user friendly public information resource that lists: 1) Core data sharing and data release activities; 2) Data sources; and 3) A register of data sharing agreements.
APP 2 – Anonymity and Pseudonymity	Compliant	APP 2 is unlikely to play a significant role in the proposed *Data Sharing & Release Bill*.	

Australian Privacy Principle (APP) / Privacy Component	Alignment	Findings Summary	Recommendation
APP 3 – Collection of solicited personal information	**Further Measures Possible**	Data minimisation (APP 3.1) is likely to be a key privacy protection in the context of the *Data Sharing & Release Bill*. Where an individual or entity has been accredited to receive personal data, data minimisation should be applied to both the collection of data (e.g. from data custodians) and any subsequent disclosure of matched or linked data to third parties.	**Recommendation 7. Minimisation of data collection** The Bill should ensure that data minimisation is a clear requirement for data sharing. The Bill should include the word 'only' in the requirement: e.g. 'sharing **only** data that is reasonably necessary'.
APP 4 – Dealing with unsolicited personal information	**Compliant**	Unsolicited data is unlikely to play a major role in the proposed *Data Sharing & Release Bill*.	
APP 5 – Notification	**Further Measures Possible**	The *DS&R Bill* represents a significant change to the way data is used and disclosed by agencies. The Notice requirements in APP 5 are not subject to any exceptions or exclusions and will be an important part of the implementation of the *Data Sharing & Release Bill.* Options to consider include: • Developing a standard notice; • Guidance on when and how to issue notices; and / or • A prohibition on using data collected prior to the implementation of effective notices. It is possible that these measures will be implemented through regulatory action or guidance, rather than the *Data Sharing & Release Bill* itself.	**Recommendation 8: Improved openness in Notices about data sharing / release** Agencies and accredited entities should be more open in their Notices about the use of data sharing and the potential disclosure of some data to external users. The National Data Commissioner and the Office of the Australian Information Commissioner should consider the following options: 1) Development of a standard Notice template; 2) Development of Guidance on when and how to issue Notices; 3) A prohibition on using data collected prior to the implementation of effective Notices; and 4) Checking Notices for compliance.
APP 6 – Use or Disclosure	**Compliant**	The intention is that the sharing of relevant data will be authorised by the *Data Sharing & Release Bill*, and any use and disclosure will therefore be compliant with APP 6. In some cases, data will be released as de-identified information. This is another way in which the Framework can align with APP 6. However, some other rules will still apply, including APP 1, APP 11 and any Rules or binding guidance issued by the new regulator – the National Data Commissioner.	
APP 7 – Direct Marketing	**Compliant**	The use of data for commercial purposes such as direct marketing will not be listed as an allowable purpose. Commercial entities will be free to apply to become Accredited Data Authorities or Accredited Users, but the restricted 'purpose test' will override APP 7, so direct marketing will not be possible.	
APP 8 – Cross Border Disclosure	**Compliant**	This is an area where the *Privacy Act* continues to apply, and the *Data Sharing & Release Bill* is not required to address this issue.	

Australian Privacy Principle (APP) / Privacy Component	Alignment	Findings Summary	Recommendation
APP 9 – Government Related Identifiers	**Compliant**	This is an area where the *Privacy Act* continues to apply, and the *Data Sharing & Release Bill* is not required to address this issue.	
APP 10 – Quality of Personal Information	**Compliant**	The data quality requirements in APP 10 will be further enhanced by the inclusion of the Data Sharing Principles[10] in the *Data Sharing & Release Bill*, as well as likely guidance from the National Data Commissioner.	
APP 11 – Security	**Compliant**	Substantial risk assessment, security and de-identification measures will be included in the *DS&R Bill*. For example, the Five Safes Framework will be expanded and incorporated into the Bill in the form of Data Sharing Principles, complemented by guidelines developed by the new regulator – the National Data Commissioner. Security measures form a significant part of this proposed framework.	
APP 12 – Access	**Compliant**	This is an area where the *Privacy Act* continues to apply, and the *Data Sharing & Release Bill* may not be required to address this issue in detail.	
APP 13 – Correction	**Compliant**	This is an area where the *Privacy Act* continues to apply, and the *DS&R Bill* may not be required to address this issue in detail.	
Section 19. Governance		The proposed Framework includes proposed governance arrangements that are likely to enhance compliance with the *Data Sharing & Release Bill*. The cornerstone of these arrangements is the establishment of National Data Commissioner. The National Data Commissioner's proposed regulatory functions allow it to: 1) Accredit Data Sharing Entities (DSEs); 2) Handle complaints about the data sharing and release system and entities; 3) Assess and investigate compliance with the legislation; 4) Determine breaches of the legislation; and 5) Enforce the legislation and impose penalties. This PIA recognises that these governance arrangements, particularly the assessment powers, are likely to enhance overall compliance with the Bill and boost community confidence in data sharing and release.	

[10] Department of the Prime Minister and Cabinet, Australian Government, *Best Practice Guide to Applying Data Sharing Principles* (19 March 2019) <www.pmc.gov.au/resource-centre/public-data/data-sharing-principles>.

Australian Privacy Principle (APP) / Privacy Component	Alignment	Findings Summary	Recommendation
Section 20. Social Licence		It is likely to be difficult, but not impossible, to develop community trust, confidence and acceptance – known as a social licence – for the *Data Sharing & Release Bill.* The main obstacle is that the overall approach of the Bill imposes a mandatory scheme (for consumers) with no consent provisions. This will need to be balanced by a significant public benefit and strong privacy protections – and the successful communication of these. The key factors in determining a social licence will be: 1) The extent to which compliance is included as an allowable purpose; 2) The extent to which commercial access is allowed; 3) The treatment of sensitive data; and The extent to which other privacy and security measures can counter concerns regarding the lack of consent.	

3. Scope and Methodology

3.1. Scope

The scope of this PIA is limited to the following items:

In Scope	Out of Scope
• High level identification of potential compliance issues in the context of the Commonwealth privacy legal framework	• Compliance with specific sectoral legislation or State and Territory legislation (although some key issues may be identified and flagged for further review)
• Review of a small number of key documents	• Review of the entire suite of DPMC documentation
• Internal stakeholder consultation and some targeted external consultation with Privacy Commissioners and Privacy and Consumer Advocacy Organisations	• Comprehensive external stakeholder consultation or extensive public consultation (refer to Appendix 3 for details of DPMC consultations)
• Brief consideration of security issues relevant to privacy compliance	• Detailed security assessment

3.2. PIA Guidelines

This PIA is being conducted in accordance with the PIA Guidelines issued by the Office of the Information Commissioner.[11]

3.3. Privacy Legislation

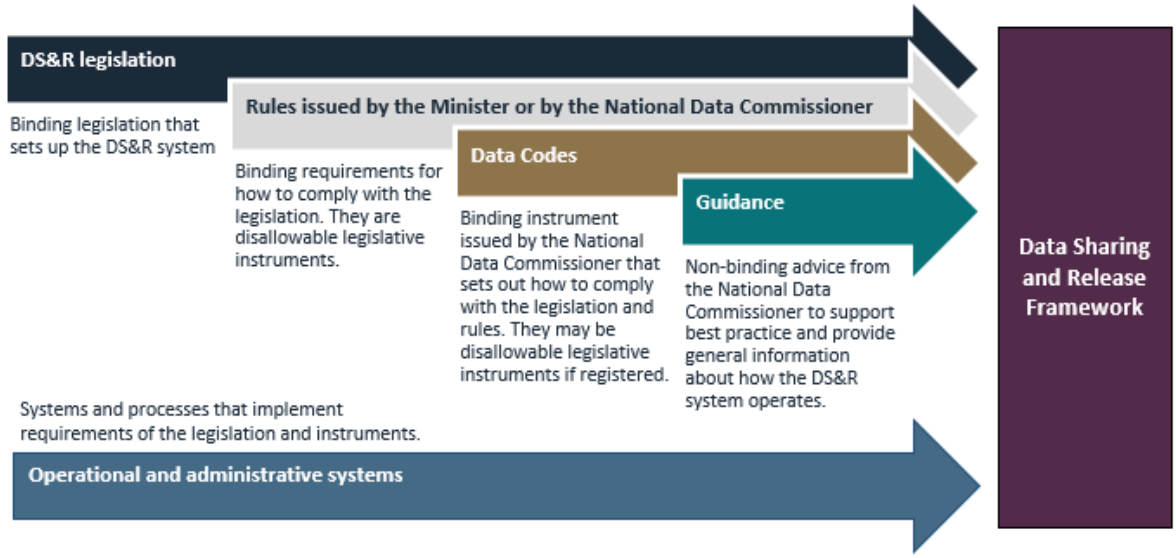
This PIA has been written in the light of current Commonwealth privacy legislation – primarily the *Privacy Act 1988*. The Act sets out the Australian Privacy Principles (*APPs*), which regulate the collection, use and disclosure of personal information by Commonwealth Agencies and private sector organisations.

[11] Office of the Australian Information Commissioner, Australian Government, *Guide to undertaking privacy impact assessments* (May 2014) <www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments>.

4. The Proposed Data Sharing & Release Bill Overview

4.1. Components of the proposed Data Sharing and Release Framework

The proposed *DS&R Framework* contains layers of legislation, supporting materials, and operational administrative systems. These aspects of the framework provide binding obligations as well as the advice and processes necessary to interpret and implement them.



(Diagram supplied by DPMC, June 2019)

4.2. Objectives of the proposed *Data Sharing & Release Bill*

It appears likely that the objectives of the proposed Bill will distinguish between data sharing and data release.

For data sharing it is proposed that the Bill overrides existing secrecy and confidentiality provisions, in order to allow data sharing – with some exceptions.

For data release the current proposal for the *Data Sharing and Release Framework* is that the legislation will not authorise release explicitly, but will encourage appropriate release as a function of the National Data Commissioner.

It is important to note that the Bill will include a clear statement saying that it does not **compel** data sharing or release.

4.3. Structure of the proposed legislative package

The key structural elements of the legislative package can be summarised as follows:

- The legislation consists of a core Bill and Rules, complemented by a variety of Binding Data Codes and guidance that are expected to be developed by the National Data Commissioner;
- The core Bill overrides existing secrecy and confidentiality provisions, with some exceptions;
- However, the Bill does not **compel** data sharing or data release;
- The Bill includes a list of permitted purposes and some precluded purposes;
- The Bill uses key *Privacy Act* definitions;
- The Bill allows the *Privacy Act* to continue to cover the *collection* of personal information;
- The scope of the Bill will allow organisations, that would not traditionally be covered by the *Privacy Act*, to participate – such as State and Territory entities;

- The Bill introduces new Data Sharing Principles[12] which are an expansion of the Five Safes framework;
- The Bill introduces a new regulator – the National Data Commissioner <www.datacommissioner.gov.au>;
- The National Data Commissioner may accredit three types of entity to participate in the system:
    - Accredited Data Service Providers which provide data services;
    - Accredited User Organisations which use shared data; and
    - Accredited User Individuals which use shared data;
- The Bill includes a rule-making power;
- The National Data Commissioner can issue binding Data Codes and non-binding guidelines; and
- The Bill includes a compliance monitoring and enforcement regime with appropriate sanctions.

4.4. Privacy protections in the proposed *Data Sharing & Release Bill*

This section provides an overview of the main privacy protections that will be contained in the proposed Bill, as distinct from privacy protections in the *Privacy Act* (which are described in detail later in this report).

4.4.1. Purpose Test

The proposed Purpose Test authorises data sharing that is reasonably necessary to inform:

- Research and development;
- Government policy;
- Program design, implementation, and evaluation; and
- Service delivery.

The reference to 'sharing data that is reasonably necessary' for one of the purposes is designed to incorporate the concept of data minimisation into the Purpose Test.

Overall, the Purpose Test acts as a key privacy safeguard. Many current data sharing activities are undertaken using a mix of the *Privacy Act* (which does not contain a Purpose Test) and public interest certificates which only contain a single high level 'public interest' test.

4.4.2. Precluded Purposes

It is expected that the purposes for which data sharing will be precluded under the *DS&R Framework* will include:

- Commercial uses which infringe privacy or fair competition;
- Compliance and assurance activities; and
- National security and law enforcement activities.

This approach is a fairly straightforward method for restricting the types of data sharing that are of most concern to stakeholders.

The debate on the inclusion or exclusion of compliance is ongoing, and this PIA supports its exclusion (See Recommendation 3: Exclusion of compliance activities). The other categories are more settled.

[12] Department of the Prime Minister and Cabinet, Australian Government, *Best Practice Guide to Applying Data Sharing Principles* (19 March 2019) <www.pmc.gov.au/resource-centre/public-data/data-sharing-principles>.

4.4.3. Data Sharing Principles

The Bill will include a reference to a set of Data Sharing Principles. The five Data Sharing Principles are:

1) ***[Project]*** *Data sharing is for an appropriate project or program of work.*
2) ***[People]*** *Data is available to authorised users.*
3) ***[Setting]*** *The environment in which the data is shared reduces the risk of unauthorised use or disclosure.*
4) ***[Data]*** *Appropriate protections are applied to the data.*
5) ***[Output]*** *Outputs are appropriate for further sharing or release.*

However, the detailed requirements of the Principles will not be set out in the proposed Bill. They are the subject of recent Best Practice Guidelines.[13]

4.4.4. Data minimisation requirement

A data minimisation requirement is now included as part of the Purpose Test, and must also be considered when applying the Data Principle (the fourth Principle in the Data Sharing Principles). This will be a mandatory part of the test to only share the amount of identifiable data that is reasonably necessary.

Galexia's preference is for the wording of the data minimisation requirement to be strengthened. Our view is that there is a risk that the data minimisation requirement will be 'lost' or downplayed in the current approach.

Adding the words 'reasonably necessary to perform' to the Purpose Test is unlikely to restrict or minimise the sharing of data in a sufficient way.

A stronger approach would be to include the word 'only' in the requirement – e.g. 'sharing **only** data that is reasonably necessary'.

This PIA includes a recommendation on this issue (Refer to Recommendation 7. Minimisation of data collection)

4.4.5. Restriction on on-sharing data

For sharing or on-sharing of data to be authorised under the *DS&R Framework*, the same requirements must be met. The proposed sharing must meet the purpose test and be consistent with the Data Sharing Principles, be subject to a Data Sharing Agreement between the sharer and the recipient Data Sharing Entities, and have written agreement from the Data Custodian. In exceptional circumstances, sharing or on-sharing may occur where a listed exception in the *Privacy Act* (refer to sections 16A and 16B) applies.

The on-sharing limitation must also be considered when applying the Data Sharing Principles – particularly the People Principle and the Outputs Principle.

[13] Department of the Prime Minister and Cabinet, *Best Practice Guide to Applying Data Sharing Principles* (19 March 2019) <www.pmc.gov.au/resource-centre/public-data/data-sharing-principles>.

4.5. Implementation

While most of the privacy requirements and safeguards will be included in the proposed Bill, some of the safeguards may be implemented through other mechanisms.

The Bill includes the establishment of a National Data Commissioner. It is proposed that the National Data Commissioner will be able to issue guidance in various forms, including:[14]

- **Binding Data Codes**
  Binding codes of practice (likely to be disallowable legislative instruments) which deal with issues such as:
    - How to apply, or further requirements for complying with, the legislation (especially the purpose test, Data Sharing Principles);
    - Matters directly relating to the legislation (such as accreditation, reporting requirements, charging, form or terms of Data Sharing Agreements, and management of breaches and complaints); and
    - Other relevant matters.
- **Best Practice Guidance**
  Non-binding guidelines, which Data Sharing Entities must have regard to when using the legislation. Best practice guidance might deal with:
    - Any aspect of the data sharing and release system; and
    - Incidental data-related matters (such as release, data management and curation, technical matters and standards, and emerging technologies).

[14] Department of the Prime Minister and Cabinet, Office of the National Data Commissioner, *Data Sharing Legislation – Policy Positions* (22 February 2019) [INTERNAL DOCUMENT].

5. Is the data 'personal information'?

5.1. The Law

A starting point for our discussion of privacy compliance is whether or not the data that is proposed to be shared or released is personal information.

The Commonwealth *Privacy Act* states at *section 6* that:[15]

> ***Personal information*** *means information or an opinion about an identified individual, or an individual who is reasonably identifiable:*
>
> *(a) whether the information or opinion is true or not; and*
>
> *(b) whether the information or opinion is recorded in a material form or not.*

5.2. Office of the Australian Information Commissioner (OAIC) Guidance

In May 2017, the OAIC provided guidance on personal information:

> Office of the Australian Information Commissioner, Australian Government, *What Is Personal Information?* (5 May 2017) <www.oaic.gov.au/privacy/guidance-and-advice/what-is-personal-information>.

5.3. Data Sharing & Release Bill – Overview

The proposed data sharing / data release arrangements incorporate a mix of personal information and sensitive personal information.

5.4. 'Personal information' finding

The Privacy Commissioner warns that:[16]

> *where it is unclear whether an individual is 'reasonably identifiable', an organisation should err on the side of caution and treat the information as personal information.*

For the *Data Sharing & Release Bill*, some of the data that is being proposed to be shared will be linked to an individual, or can be easily linked to the correct individual.

An additional question is whether or not some of the data falls into the category of sensitive information.

[15] See also <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-b-key-concepts/#personal-information>.

[16] Office of the Australian Information Commissioner, Australian Government, *Guide to securing personal information* (2015) <www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information>.

Sensitive information[17] means:

> *(a) information or an opinion about an individual's:*
>
> > *(i) racial or ethnic origin; or*
> > *(ii) political opinions; or*
> > *(iii) membership of a political association; or*
> > *(iv) religious beliefs or affiliations; or*
> > *(v) philosophical beliefs; or*
> > *(vi) membership of a professional or trade association; or*
> > *(vii) membership of a trade union; or*
> > *(viii) sexual orientation or practices; or*
> > *(ix) criminal record;*
> > *that is also personal information; or*
>
> *(b) health information about an individual; or*
>
> *(c) genetic information about an individual that is not otherwise health information; or*
>
> *(d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or*
>
> *(e) biometric templates.*

It is likely that most of these categories of sensitive information (perhaps with the exception of biometrics[18]) will be shared at some point under the Bill.

The presence of sensitive information has implications for APP 3 and APP 6 (discussed below). It also raises the overall security profile of the proposed data sharing or release (see APP 11 below).

During the development of the Bill some consideration has been given to the treatment of sensitive information and various options have been considered. The expectation is that the *Data Sharing & Release Framework* will leverage existing protections under the *Privacy Act 1988* and *Australian Government Agencies Privacy Code 2017*.[19] Any further conditions for sensitive information may be introduced through a Binding Data Code, developed by the National Data Commissioner <www.datacommissioner.gov.au>. Stronger penalties will apply to breaches involving sensitive information.

[17] Section 6 of the *Privacy Act 1988*.

[18] We note that the Department is still finalising exclusions for the *DS&R Framework*.

[19] The Australian Government Agencies Privacy Code was registered on 27 October 2017 and commenced on 1 July 2018. <www.oaic.gov.au/privacy/privacy-for-government-agencies/australian-government-agencies-privacy-code>.

6. APP 1. Open and transparent management of personal information

6.1. APP 1. Proposed *Data Sharing & Release Bill* – Overview

APP 1[20] requires Agencies to be open and transparent about their use of data sharing and the potential release of some data to external users such as researchers. Similarly, any entity that is accredited to receive data or carry out data integration activities as part of the proposed *Data Sharing & Release Framework* will also need to be open and transparent about their use of shared data and the source of data.

APP 1 will continue to apply to entities participating in the *DS&R Framework* arrangements, including data custodians, recipients and accredited Data Service Providers.

Some additional openness and transparency requirements may need to be included in the Bill.

In order to enhance openness and transparency, Agencies and any third party entity that is accredited to receive data or act as a Data Service Provider should be required to maintain a public information resource that provides more information than the minimum amount required under the *Privacy Act*.

Currently, the focus in the *DS&R Framework* is on the publication of Data Sharing Agreements and it is proposed the Bill will include the following requirements:[21]

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

The publication of Data Sharing Agreements is an excellent step towards transparency. However, the format of the agreements is unlikely to be very public friendly. This PIA therefore makes some additional recommendations on openness.

Publication of the Data Sharing Agreements is not the only transparency tool included in the proposed *DS&R Framework*. Additional transparency measures include the development of a public register of all Data Sharing Agreements and the publication of Annual Reports by the National Data Commissioner.

Note: There is a further discussion of potential governance arrangements to assist in privacy compliance in Section 19. Governance (below) These governance arrangements will also address openness and transparency and assist in compliance with APP 1.

[20] More information: <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-1-app-1-open-and-transparent-management-of-personal-information>.

[21] Department of the Prime Minister and Cabinet, Office of the National Data Commissioner, *Data Sharing Legislation – Policy Positions* (22 February 2019) [INTERNAL DOCUMENT].

6.2. APP 1. Finding

Some additional openness and transparency requirements may need to be included in the Bill.

As a first step, Agency privacy policies should consistently and comprehensively inform the public about potential data sharing and data release activities. This could be achieved through guidance or even template wording from the National Data Commissioner and the Office of the Australian Information Commissioner (OAIC). The National Data Commissioner should play a role in checking that Agency privacy policies are open and transparent about the nature and scale of data sharing and data release activities.

Recommendation 5: Improved openness in Privacy Policies about data sharing / release

Agencies and accredited entities should be more open about data sharing and the potential disclosure of some data to external users.

A second important step is the establishment of a network of user friendly public information resources regarding data sharing and data release. During the development of this PIA the need for public education regarding data sharing was a consistent theme raised by stakeholders.

Recommendation 6: Establish user friendly public information resources

The National Data Commissioner and any third party entity that is accredited to receive data or act as a Data Service Provider should be required to maintain a user friendly public information resource that lists:

1) Core data sharing and data release activities;
2) Data sources; and
3) A register of data sharing agreements.

7. APP 2. Anonymity and Pseudonymity

7.1. APP 2. Proposed *Data Sharing & Release Bill* – Overview

The application of APP 2[22] is limited to situations where an individual may be required to identify themselves to an APP entity 'in relation to a particular matter'. It is unlikely that this situation will arise in the context of the Data Sharing and Release Bill.

7.2. APP 2. Finding

APP 2 is unlikely to play a major role in the proposed *Data Sharing & Release Bill*.

[22] More information: <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-2-app-2-anonymity-and-pseudonymity>.

8. APP 3. Collection of solicited personal information

8.1. APP 3. Proposed *Data Sharing & Release Bill* – Overview

APP 3 sets out the requirements for the collection of personal information. The Office of the Australian Information Commissioner has issued guidelines on APP 3[23] that warn there are privacy risks associated with:

- Collecting personal information about a group of individuals, when information is only required for some of those individuals;
- Collecting more personal information than is required for a function or activity; or
- Collecting personal information that is not required for a function or activity but is being entered in a database in case it might be needed in the future.

The OAIC has also provided guidance about de-identification and data analytics:

- *De-identification and the Privacy Act*, Office of the Australian Information Commissioner (OAIC), March 2018 <www.oaic.gov.au/privacy/guidance-and-advice/de-identification-and-the-privacy-act>
- *Guide to Data Analytics and the Australian Privacy Principles*, Office of the Australian Information Commissioner (OAIC), March 2018 <www.oaic.gov.au/privacy/guidance-and-advice/guide-to-data-analytics-and-the-australian-privacy-principles>
- *De-identification Decision-Making Framework*, Office of the Australian Information Commissioner (OAIC) and Data61 (CSIRO), September 2017 <www.oaic.gov.au/privacy/guidance-and-advice/de-identification-decision-making-framework>

APP 3 contains a number of significant exceptions that are relevant to data sharing and release. The proposed disclosure of data to accredited third parties will be specifically authorised by the proposed legislation. The recipients will therefore be able to 'collect' this data by relying on the exception in APP 3.4.

However, the application of the legal exception in APP 3.4 does not remove the requirement to minimise data collection (APP 3.1).

Data minimisation is also an important best practice in the research context, as can be seen in the following principles and guidelines:

- **High Level Principles for Data Integration Involving Commonwealth Data for Statistical and Research Purposes**[24]

  Principle 6: Preserving Privacy and Confidentiality

  The number of unit records and data variables to be included in an integrated dataset should be no more than required to support the approved purposes.

- **Guide to Data Analytics and the Australian Privacy Principles**[25]

  Limiting the collection of personal information

[23] More information: <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-3-app-3-collection-of-solicited-personal-information>.

[24] Refer to the National Statistical Service, Australian Bureau of Statistics <www.nss.gov.au>.

[25] Office of the Australian Information Commissioner, Australian Government, *Guide to Data Analytics and the Australian Privacy Principles* (March 2018) <www.oaic.gov.au/privacy/guidance-and-advice/guide-to-data-analytics-and-the-australian-privacy-principles>.

> *APP 3.1 states that organisations must not collect information unless it is reasonably necessary or directly related to one or more of its functions or activities. This principle may appear to challenge the concept of using 'all the data' for 'unknown purposes'. However, just because data analytics can discover unexpected or 'interesting' correlations, this does not mean that the new personal information generated is necessary to the legitimate functions and activities.*
>
> *While APP 3 does place restrictions on what data may be collected, this does not need to be a barrier for data analytics. APP 3 is intended to operate objectively and practically by allowing organisations to collect personal information that is reasonably necessary (from the point of view of a reasonable person) to pursue its legitimate functions or activities.*

The proposed legislation underpinning the *Data Sharing & Release Framework* recognises the importance of data minimisation, and includes a data minimisation requirement in the Purpose Test. The inclusion of the data minimisation requirement follows the Department's consultation and engagement with stakeholders and the provision of earlier Galexia advice (as part of the Department's iterative approach to the conduct of this PIA and the development of the Framework).

The Purpose Test authorises data sharing that is reasonably necessary to inform:

- Research and development;
- Government policy;
- Program design, implementation, and evaluation; and
- Service delivery.

In addition, it is expected that the *DS&R Framework* will include a definition of the term 'collect' that reflects the latest approaches to privacy management in the data sharing environment. The proposed definition is:[26]

> ***Collect:*** *is a broad verb that includes gathering, acquiring, generating, and obtaining information from any source by any means. This includes directly collecting information from people (e.g. in a survey, Census, or administrative process), creating new information from data already held (e.g. through data integration, or an audit log), and receiving data that is shared by another entity.*

However, this PIA's preference is for the wording of the data minimisation requirement to be strengthened in the Bill to ensure it is a clear and strong privacy safeguard. There is a risk that the data minimisation requirement will be 'lost' or downplayed in the current approach.

Adding the words 'reasonably necessary to perform' to the Purpose Test is unlikely to restrict or minimise the sharing of data in a sufficient way.

A stronger approach would be to include the word 'only' in the requirement – e.g. 'sharing only data that is reasonably necessary'.

The following table summarises some of the key issues regarding collection of personal data from the perspective of the *Data Sharing & Release Bill*:

[26] Department of the Prime Minister and Cabinet, Office of the National Data Commissioner, *Data Sharing Legislation – Policy Positions* (22 February 2019) [INTERNAL DOCUMENT].

APP 3. Collection of solicited information	Action / Status	Commentary
A. Is collected information reasonably necessary for, or directly related to, one or more of the entity's functions or activities?	**Further Measures Possible**	This requirement will cover the original collection of data. The proposed Bill extends the data minimisation requirement to cover further collection by accredited participants, as they collect data from multiple sources and potentially match it (and any subsequent on-sharing or disclosure). However, there is a risk that the data minimisation requirement will be lost or downplayed in the current structure of the Bill, as it is not stated in clearer language and included as a stronger privacy safeguard. This PIA includes a recommendation to address this issue (refer to Recommendation 7 below).
B. Is NO sensitive information about an individual collected (unless a relevant exception applies, such as the receipt or explicit and specific consent)?	**Compliant**	It is likely that significant sensitive data will be collected and shared / released by authorised third parties. The collection of sensitive data can be achieved by relying on exceptions contained in APP 3.4 (a) (where the collection of the information is required or authorised by or under an Australian law) In this case, the planned legal authority will be specified in the proposed *Data Sharing & Release Bill*. The accredited third parties will then be able to rely on APP 3.4 in order to receive the data.
C. Is personal information collected only by lawful and fair means?	**Compliant**	This requirement will continue to apply and will not be impacted by the Bill.
D. Is personal information about an individual collected only from the individual (unless a relevant exception applies)?	**Compliant**	This requirement will continue to apply to the original collection of data, and will not be impacted by the Bill.

8.2. APP 3. Finding

APP 3.1 has a test of 'reasonable necessity' for the collection of personal information.

In this PIA we are recommending that the Bill include a mandatory requirement to minimise the collection of personal data and sensitive personal data.

Where an individual or entity has been accredited to receive personal data, data minimisation should be applied to both the sharing of data (e.g. by data custodians) and any subsequent release of data. This PIA's strong preference is that this requirement is included as a clear and strongly worded provision in the Bill.

Recommendation 7. Minimisation of data collection

The Bill should ensure that data minimisation is a clear requirement for data sharing. The Bill should include the word 'only' in the requirement – e.g. 'sharing **only** data that is reasonably necessary'.

9. APP 4. Dealing with unsolicited personal information

9.1. APP 4. Proposed *Data Sharing & Release Bill* – Overview

The application of APP 4[27] is limited to situations where an agency or organisation receives unsolicited personal information.

If the agency or organisation is a data custodian they will continue to be covered by APP 4 and the Data Sharing & Release Bill will have no impact.

For other Data Sharing Entities such as Accredited Data Service Providers and Accredited Users, it is very difficult to see any circumstances in which they would receive unsolicited information about an individual.

9.2. APP 4. Finding

APP 4 is unlikely to play a major role in the proposed *Data Sharing & Release Bill*.

[27] More information: <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-4-app-4-dealing-with-unsolicited-personal-information>.

10. APP 5. Notification of the collection of personal information

10.1. APP 5. Proposed *Data Sharing & Release Bill* – Overview

APP 5[28] requires Agencies to provide consumers with clear Notices about their use of data sharing and the potential release of some data to external users such as researchers.

APP 5 contains no exceptions.

Stakeholders were concerned that consumers will be unaware of the nature, scope and scale of data sharing and data release. Current agency privacy Notices do not refer to large scale or widespread data sharing or data release.

The expectation is that data sharing entities will ensure their privacy notices reflect their participation in the *Data Sharing & Release Framework*. This is a matter of compliance with the *Privacy Act* by Agencies, and the National Data Commissioner and the Office of the Australian Information Commissioner will work together to ensure compliance.

The compliance of notices with APP 5 can be assessed using the following checklist. Note: The table concentrates on issues relevant to the *Data Sharing & Release Bill*:

APP 5. Notification	Action / Status	Commentary
A. Does the entity provide notice of its identity and contact details?	**Compliant**	This requirement will continue to apply, and will not be impacted by the Bill.
B. Does the entity provide notice of third party collection? (if relevant)	**Compliant**	This requirement will continue to apply, and will not be impacted by the Bill.
C. Does the entity provide notice of the fact that the collection is required or authorized? (if relevant)	**Compliant**	This requirement will continue to apply, and will not be impacted by the Bill.
D. Does the entity provide notice of the purpose of collection?	**Compliant**	This requirement will continue to apply, and will not be impacted by the Bill.
E. Does the entity provide notice of the main consequences (if any) for the individual if all or some of the personal information is not collected?	**Compliant**	This requirement will continue to apply, and will not be impacted by the Bill.
F. Does the entity provide notice of any other APP entity, body or person, or the types of any other APP entities, bodies or persons, to which the APP entity usually discloses personal information of the kind collected?	**Further Measures Possible**	This will be the main APP 5 requirement impacted by the Bill. It may be difficult to ensure that all data subjects are aware of the full impact of the *DS&R Bill* unless there are some enhancements to the Notice process. Current practice is for privacy notices to only provide very limited information on the potential sharing of data. This PIA includes a recommendation to address this issue (refer to Recommendation 8 below).

[28] More information: <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-5-app-5-notification-of-the-collection-of-personal-information>.

APP 5. Notification	Action / Status	Commentary
G. Does the entity provide notice that the privacy policy contains information about how the individual may access their personal information and seek the correction of such information?	**Compliant**	This requirement will continue to apply, and will not be impacted by the Bill.
H. Does the entity provide notice that the privacy policy contains information about how the individual may complain?	**Compliant**	This requirement will continue to apply, and will not be impacted by the Bill.
I. Does the entity provide notice of whether the entity is likely to disclose the personal information to overseas recipients (and if so, where)?	**Compliant**	This requirement will continue to apply, and will not be impacted by the Bill.

10.2. APP 5. Finding

The *DS&R Bill* represents a significant change to the way data is used and disclosed by agencies. The Notice requirements in APP 5 are not subject to any exceptions or exclusions and will be an important part of the implementation of the *DS&R Bill*.

The Bill should include some additional measures on Notice.

The National Data Commissioner should also play a role in checking that privacy Notices are open and transparent about the nature and scale of data sharing and data release activities.

Recommendation 8: Improved openness in Notices about data sharing / release

Agencies and accredited entities should be more open in their Notices about the use of data sharing and the potential disclosure of some data to external users. The National Data Commissioner and the Office of the Australian Information Commissioner should consider the following options:

1) Development of a standard Notice template;
2) Development of Guidance on when and how to issue Notices;
3) A prohibition on using data collected prior to the implementation of effective Notices; and
4) Checking Notices for compliance.

11. APP 6. Use or disclosure of personal information

11.1. APP 6. Proposed *Data Sharing & Release Bill* – Overview

The proposed *DS&R Bill* involves a significant expansion of the use and disclosure of personal data.

The OAIC's Guidelines on APP 6[29] warn against the unexpected or surprise use of data.

It is proposed that the use and disclosure of data will be specified in the Bill and cover two categories of use and disclosure:

- **Category 1: Data sharing**
  The *DS&R Framework* allows the provision access to data to specific recipients in a controlled manner; and
- **Category 2: Data release**
  The *DS&R Framework* will not specifically authorise the release of data. However, the proposed Bill will provide the National Data Commissioner with a role to encourage best practice in the release of data – such as providing open access to data through tables published on an open data portal.

Alignment with APP 6 can be achieved in a number of ways. For data sharing proposal, the most pragmatic approach is to recognise the *Data Sharing & Release Framework* as providing suitable 'legal authority' for a disclosure under the exception listed in APP 6.2 (b).

In addition to the application of APP 6, participants may also need to make a decision for each potential request about whether or not the data should be shared or released as de-identified information or identified information.

If the data is to be released as de-identified information, the application of the *Privacy Act* does not entirely disappear. This is because the risk of re-identification of the data must still be considered.

If de-identified data is released, and it is subsequently found to be re-identifiable, the approach of the OAIC is to classify this as a breach of APP 6 (unless another exception applies).

The following table summarises the key compliance tasks relevant to APP 6:

APP 6. Use or Disclosure	Action / Status	Commentary
A. Has the entity clearly defined the primary purpose of collection and identified any secondary purposes?	**Compliant**	This provision will be over-ridden by the stricter Purpose Test in the Bill.
B. Will the entity only disclose personal information for a secondary purpose with consent (or a relevant exception)?	**Compliant**	The intention is that the sharing of relevant data will be authorised by the *DS&R Bill,* and any use and disclosure will therefore be compliant with APP 6. In some cases, participants may choose to only disclose de-identified information. This is another way for the release to comply with APP 6. However, some other rules will still apply, including APP 1, APP 11 and any Rules or binding guidance on de-identification issued by the new regulator.
C. Is any biometric information only disclosed for a secondary purpose in accordance with Clause 6.3 and the relevant OAIC Guidelines?	**n/a**	*Not applicable*

[29] More information: <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-6-app-6-use-or-disclosure-of-personal-information>.

APP 6. Use or Disclosure	Action / Status	Commentary
D. Is a written note made of any disclosures that are made relying on the law enforcement exception?	**n/a**	*Not applicable*

11.2. APP 6. Finding

The intention is that the sharing of relevant data will be authorised by the *DS&R Bill*, and any use and disclosure will therefore be compliant with APP 6. The application of APP 6 will therefore be very limited, so the real pressure for compliance in the use and disclosure of data shifts to compliance with the Purpose Test and the Data Sharing Principles in the proposed Bill.

Data may be released as de-identified information. This is another way in which the release can comply with APP 6. However, some other rules will still apply, including APP 1, APP 11 and any Rules or binding guidance on de-identification issued by the National Data Commissioner.

12. APP 7. Direct marketing

12.1. APP 7. Proposed *Data Sharing & Release Bill* – Overview

Stakeholders consulted during this PIA were very concerned about any potential commercial exploitation of data that might be shared under the Data Sharing & Release Bill. While these concerns were fairly broad, they naturally included concerns about direct marketing.

APP 7[30] allows direct marketing in some limited circumstances, but stakeholders were looking for a prohibition on direct marketing in the context of the *DS&R Bill*.

The proposed *DS&R Framework* is likely to include two restrictions on the use of data for commercial purposes such as direct marketing:

- Commercial purposes will **not** be listed as an allowable purpose for sharing (although commercial access to data that fits the permitted government policy and research purposes may be allowed);
- Commercial uses which infringe privacy or fair competition will be listed as a precluded purpose.

Commercial entities will be free to apply to become Accredited Data Service Providers or Accredited Users, but the restricted Purpose Test will override APP 7, so direct marketing will not be possible.

12.2. APP 7. Finding

The use of data for commercial purposes such as direct marketing will not be listed as an allowable purpose.

Commercial uses which infringe privacy or fair competition will also be a precluded purpose under the Bill.

These tests will over-ride APP 7, and this will restrict the relevance of direct marketing in the context of the *DS&R Bill*.

[30] More information: <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-7-app-7-direct-marketing>.

13. APP 8. Cross-border disclosure of personal information

13.1. APP 8. Proposed *Data Sharing & Release Bill* – Overview

There is no expectation that the Bill will contain any specific restrictions on cross border data transfers beyond the existing provisions of the *Privacy Act*.

During the development of this PIA some stakeholders, including community advocates and privacy regulators, expressed concerns that data could be shared or on-shared under the Bill to jurisdictions where privacy safeguards would be difficult to enforce.

However, it is unlikely that a specific approach for cross border transfers would be developed just for the *DS&R Framework*. APP 8[31] itself was the subject of complex debate, and agencies and organisations have now become used to its application.

13.2. APP 8. Finding

This is an area where the *Privacy Act* continues to apply, and the *DS&R Bill* may not be required to address this issue.

14. APP 9. Adoption, use or disclosure of government related identifiers

14.1. APP 9. Proposed *Data Sharing & Release Bill* – Overview

APP 9[32] states that an organisation must not adopt a government related identifier of an individual as its own identifier. In addition, an organisation must not use or disclose a government related identifier of an individual unless the use or disclosure is reasonably necessary for the organisation to verify the identity of the individual.

APP 9 does not apply to agencies unless they are engaging in prescribed commercial activities.

14.2. APP 9. Finding

This is an area where the *Privacy Act* continues to apply, and the *DS&R Bill* is not required to address this issue.

[31] More information: <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information>.

[32] More information: <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-9-app-9-adoption-use-or-disclosure-of-government-related-identifiers>.

15. APP 10. Quality of personal information

15.1. APP 10. Proposed *Data Sharing & Release Bill* – Overview

The *DS&R Framework* is, in part, designed to improve the quality of data available to participants and researchers. Potential improvements include:

1) Providing researchers and planners with the 'whole picture';
2) Allowing the sharing and potential matching of some data that would otherwise remain in silos; and
3) Facilitating some potential sharing / matching of Commonwealth, State and Territory data.

These steps, if implemented, would have a positive impact on the quality of data available to the research community.

In addition, the proposed National Data Commissioner will have new powers in relation to guidance and advocacy that are likely to have a positive impact on data quality.

However, the implementation of the Framework also raises some risks in terms of data quality.

Some of the potential risk areas include:

1) Basing research output on information supplied by third parties may lead to errors. These could be errors of mistaken identity, incorrect information or out of date information;
2) Making links between diverse data sets is a difficult process, and some incorrect matches are likely to emerge; and
3) Where data is shared between multiple parties the data may be stored in multiple locations, leading over time to multiple data sets with slightly different data.

It is proposed that the legislation address these concerns through the application of the proposed Data Sharing Principles.

The two Principles that are likely to be relevant to data quality are:

- ***[Data]*** *Appropriate protections are applied to the data.*
- ***[Output]*** *Outputs are appropriate for further sharing or release*

The following table summarises compliance with APP 10[33], but it is very important to note that the data quality issues needs to be assessed on a case by case basis for each large scale data sharing or data release activity.

APP 10. Data Quality	Action / Status	Commentary
A. Has the entity taken such steps (if any) as are reasonable in the circumstances to ensure that the personal information collected is accurate, up-to-date and complete?	**Compliant**	These requirements are likely to be met by application of the proposed Data Sharing Principles in the Bill. In particular the **Data** Principle is likely to include measures that help to ensure that collected data is accurate, up to date and complete.

[33] More information: <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-10-app-10-quality-of-personal-information>.

APP 10. Data Quality	Action / Status	Commentary
B. Has the entity taken such steps (if any) as are reasonable in the circumstances to ensure that the personal information **that the entity uses or discloses** is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant?	**Compliant**	These requirements are likely to be met by application of the proposed Data Sharing Principles in the Bill. In particular the **Output** Principle is likely to include measures that help to ensure data is accurate, up to date, complete and relevant for the purpose of data sharing or data release.

15.2. APP 10. Finding

The data quality requirements in APP 10 will be further enhanced by the inclusion of the Data Sharing Principles in the *Data Sharing & Release Bill*, as well as likely guidance from the new regulator – the National Data Commissioner.

Interestingly, the data quality provisions in the Five Safes / Data Sharing Principles are actually slightly stronger and more relevant to research / planning than the APP 10 requirements for data quality. It is therefore possible that the application of the Data Sharing Principles will be a privacy enhancement when compared to APP 10 *Privacy Act* compliance for organisations.

16. APP 11. Security of personal information

16.1. APP 11. Proposed *Data Sharing & Release Bill* – Overview

The *DS&R Framework* raises significant security risks. As the Framework involves the disclosure of data to authorised third parties, using a diverse range of transfer and storage methods, the management of security risks is complex.

Data being exchanged under the Framework may include sensitive data. The scale of the data involved is also significant. It will be important for security settings to match the potential harm of any breaches.

In relation to compliance with APP 11,[34] the proposed Bill faces some potential difficulties. These include:

1) The security risk profile of the data potentially covered by the Framework is extremely high, as the data may contain sensitive information that would have an impact on both individuals and the reputation of the Government if it was made available;
2) In the research and policy development context, one of the main security protections is the de-identification of some data, but this can carry risks of potential re-identification;
3) The exchange of data between parties requires either a transfer mechanism or a process for granting authorised access – these are likely to be seen as weak points in the overall security of the data; and
4) The implementation of the Framework is likely to lead to copies of some data being held in multiple locations, increasing the overall security risk and making the investigation of any breaches or unauthorised disclosure difficult.

The *DS&R Framework* does include measures to help manage these risks and prevent unauthorised access to data.

The key security measures that are proposed to be included in the Bill are:

1) A strong accreditation scheme – for high risk integration projects, the proposed *DS&R Framework* will require custodians to use accredited data service providers. This is a considerable enhancement of existing privacy protections as it enshrines a key aspect of the *Arrangements for the Integration of Commonwealth Data for Statistical and Research Purposes*[35] into law;
2) Application of the Five Safes / Data Sharing Principles, which include security measures;
3) Sanctions and penalties for breaches, including stronger sanctions where a breach involves sensitive information;

The following table provides a very high level summary of potential compliance with APP 11.

APP 11. Security	Action / Status	Commentary
A. Has the entity taken such steps as are reasonable in the circumstances to protect the information from misuse, interference and loss?	**Compliant**	These requirements are likely to be met by application of the proposed Data Sharing Principles and other security measures included in the Bill. In particular the **Setting** Principle and the **Data** Principle are likely to include measures that protect information against misuse. This will be backed up by strong accreditation measures and sanctions.

[34] More information: <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-11-app-11-security-of-personal-information>.

[35] More information: <toolkit.data.gov.au/Data_integration_-_Commonwealth_Arrangements.html>.

APP 11. Security	Action / Status	Commentary
B. Has the entity taken such steps as are reasonable in the circumstances to protect the information from unauthorised access, modification or disclosure?	**Compliant**	These requirements are likely to be met by application of the proposed Data Sharing Principles and other security measures included in the Bill. In particular the **Setting** Principle, the **Data** Principle and the **Output** Principle are likely to include measures that protect information against unauthorised access and disclosure. This will be backed up by strong accreditation measures and sanctions.
C. Does the level of security in the application match the potential harm caused by breaches of privacy?	**Compliant**	The Bill includes measures that help to align security measures against potential harm. For example, stronger sanctions can be applied where a security breach involves the disclosure of sensitive information. In addition, the Five Safes / Data Sharing Principles are specifically designed to apply a sliding scale of security controls based on risk.
D. Will detailed access trails be retained and scrutinised for security breaches?	**Compliant**	The application of the accreditation process and the Five Safes / Data Sharing Principles will ensure that full access trails are retained.
E. Will a data retention policy / destruction schedule be developed which requires retention of personal information only for the period required for use?	**Compliant**	The data retention requirements in APP 11 will continue to apply, and will not be significantly impacted by the Bill. However, additional data retention requirements are likely to be included in data sharing agreements.
F. Is personal information de-identified as soon as possible?	**Compliant**	The de-identification of data is a significant part of the entire data sharing and release framework, especially through the implementation of the Five Safes / Data Sharing Principles. The Bill also includes restrictions on the release of identified data.

16.2. APP 11. Finding

Substantial risk assessment, security and de-identification measures will be included in the *DS&R Framework*. For example, the Five Safes Framework will be expanded and incorporated into the Bill in the form of Data Sharing Principles, complemented by guidelines and codes developed by the new regulator – the National Data Commissioner. Security measures form a significant part of this proposed *DS&R Framework*.

Agencies will continue to be subject to existing security requirements under APP 11 and other Government security standards and frameworks.

Overall, the security provisions in the Five Safes / Data Sharing Principles, when combined with the other security measures in the Bill, are likely to be stronger and more relevant to research / planning than the APP 11 security requirements – the APP 11 requirements are very high level and are designed to apply to a wide variety of data practices.

17. APP 12. Access to personal information

17.1. APP 12. Proposed *Data Sharing & Release Bill* – Overview

The Bill does not have a major impact on Access requests under APP 12.[36]

APP 12. Access	Action / Status	Commentary
A. Can the individual ascertain whether the entity has records that contain personal information, the nature of that information and the steps that the individual should take to access their record?	**Compliant**	This is an area where the *Privacy Act* continues to apply, and the *DS&R Bill* may not be required to address this issue in detail.
B. If an agency holds personal information about an individual, does the agency, on request by the individual, give the individual access to the information? (unless relevant exceptions apply)	**Compliant**	This is an area where the *Privacy Act* continues to apply, and the *DS&R Bill* may not be required to address this issue in detail.
C. Will information be provided within 30 days?	**Compliant**	This is an area where the *Privacy Act* continues to apply, and the *DS&R Bill* may not be required to address this issue in detail.
D. Will accessing personal information be provided at no cost?	**Compliant**	This is an area where the *Privacy Act* continues to apply, and the *DS&R Bill* may not be required to address this issue in detail.

17.2. APP 12. Finding

This is an area where the *Privacy Act* continues to apply, and the *DS&R Framework* may not be required to address this issue in detail.

The proposed Bill does not have a significant impact on Access requests under APP 12.

[36] More information: <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-12-app-12-access-to-personal-information>.

18. APP 13. Correction of personal information

18.1. APP 13 and proposed *Data Sharing & Release Bill* – Overview

The following table summarises compliance with APP 13:[37]

APP 13. Correction	Action / Status	Commentary
A. UPON REQUEST Does the entity take such steps (if any) as are reasonable in the circumstances to correct that information?	**Compliant**	This is an area where the *Privacy Act* continues to apply, and the *DS&R Bill* may not be required to address this issue in detail.
B. UPON LEARNING OF INACCURACIES Does the entity take such steps (if any) as are reasonable in the circumstances to correct that information? (where the inaccuracy relates to a purpose for which the information is held)	**Compliant**	This is an area where the *Privacy Act* continues to apply, and the *DS&R Bill* may not be required to address this issue in detail.
C. UPON REQUEST ONLY Will corrections and annotations be disseminated to third parties to whom personal information has previously been disclosed?	**Compliant**	This is an area where the *Privacy Act* continues to apply, and the *DS&R Bill* may not be required to address this issue in detail.
D. Will requests for corrections be addressed within 30 days?	**Compliant**	This is an area where the *Privacy Act* continues to apply, and the *DS&R Bill* may not be required to address this issue in detail.

18.2. APP 13. Finding

This is an area where the *Privacy Act* continues to apply, and the *DS&R Bill* may not be required to address this issue in detail.

The Bill does not have a major impact on Access requests under APP 13.

[37] More information: <www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-13-app-13-correction-of-personal-information>.

19. Governance

19.1. Governance overview

The proposed Framework includes some governance arrangements that are likely to enhance compliance with the proposed privacy safeguards in the Bill.

The cornerstone of these arrangements is the establishment of the National Data Commissioner <www.datacommissioner.gov.au>.

The National Data Commissioner's proposed regulatory functions allow it to:

- Accredit Data Sharing Entities (DSEs);
- Handle complaints about the data sharing and release system and entities;
- Assess and investigate compliance with the legislation;
- Determine breaches of the legislation; and
- Enforce the legislation and impose penalties.

The National Data Commissioner will have discretionary powers to monitor DSEs' compliance with the legislation and Binding Data Codes through audit or 'assessment'.

19.2. Developing an Enhanced Governance Framework

In the data sharing and data release environment, participants are subject to more than compliance with the APPs, so a broader governance framework is required.

Additional compliance requirements in the research context already exist in:

1) **The *Privacy (Australian Government Agencies — Governance) APP Code 2017***;[38]
2) **Conditions imposed on the use of data supplied by other agencies** (usually set out in MOUs and letters of exchange);
3) **Conditions imposed by rulings and determinations**;
4) **Audit findings and recommendations**; and
5) **Best practice guidance** (e.g. the *Whole of Government Sensitive Unit Record Open Data Process*[39] developed by the Department of the Prime Minister and Cabinet).

[38] The Australian Government Agencies Privacy Code was registered on 27 October 2017 and commenced on 1 July 2018. <www.oaic.gov.au/privacy/privacy-for-government-agencies/australian-government-agencies-privacy-code>.

[39] Department of the Prime Minister and Cabinet, Australian Government, *Process for Publishing Sensitive Unit Record Level Public Data as Open Data* <blog.data.gov.au/news-media/blog/publishing-sensitive-unit-record-level-public-data>.

It is expected that the National Data Commissioner will be able to develop the following types of Guidance:[40]

- **Binding Data Codes**
  Binding codes of practice (likely to be disallowable legislative instruments) which deal with issues such as:
    - How to apply, or further requirements for complying with, the legislation (especially the purpose test, Data Sharing Principles);
    - Matters directly relating to the legislation (such as accreditation, reporting requirements, charging, form or terms of Data Sharing Agreements, and management of breaches and complaints); and
    - Other relevant matters.
- **Best Practice Guidance**
  Non-binding guidelines, which Data Sharing Entities must have regard to when using the legislation. Best practice guidance might deal with:
    - Any aspect of the data sharing and release system; and
    - Incidental data-related matters (such as release, data management and curation, technical matters and standards, and emerging technologies).

It is also expected that the new National Data Commissioner will have significant audit powers. These will include a discretionary power to monitor, audit and assess compliance with the *Data Sharing & Release Framework.*

[40] Department of the Prime Minister and Cabinet, Office of the National Data Commissioner, *Data Sharing Legislation – Policy Positions* (22 February 2019) [INTERNAL DOCUMENT].

20. Social Licence

The development of the *Data Sharing & Release Framework* is partly based on the findings and recommendations of the Productivity Commission Inquiry Report on *Data Access and Use* (2017).[41]

That Report suggested that it was important to develop public trust, confidence and acceptance (known as a 'social licence') for the data sharing and release regime. The report predicted that public trust and acceptance will develop if people:

- *have a sound basis for believing in the integrity and accountability of entities (public and private) handling data*
- *feel they have some control over how their own data is used and by whom, and an inalienable ability to choose to experience some of the benefits of these uses themselves*
- *better understand the potential community-wide benefits of data use.* (page 13)

This PIA notes that it is likely to be difficult, but not impossible, to develop a social licence for the *DS&R Framework*.

The major obstacle to developing a social licence is that the overall approach is basically a mandatory scheme (for consumers) with no consent provisions. Privacy and community advocates prefer schemes which involve consent – in the *Data Sharing & Release Framework* there are no opt-in or opt-out provisions. The Productivity Commission criteria for a social licence (discussed above) include a requirement for people to '*feel they have some control over how their own data is used and by whom*'. Although the proposed Framework includes numerous privacy safeguards and a significant public benefit, the Framework does not include measures for individual consent or control.

In order to achieve a social licence the scheme therefore needs to emphasise the public benefits of sharing data appropriately under the Framework, complemented by strong privacy protections. The successful communication of these will be essential.

The key factors in determining a social licence will be:

1) The extent to which compliance is included as an allowable purpose (fortunately this is precluded in the current proposal);
2) The extent to which commercial access to data is allowed (fortunately this is precluded in the current proposal);
3) The treatment of sensitive data; and
4) The extent to which other privacy and security measures can counter concerns over the absence of consent and the lack of control over consumers' own data.

At the time of preparing this PIA it appears likely that these issues will be addressed – either through current drafting instructions or as a result of the recommendations contained in this PIA. Galexia's view is that there is potential for a social licence to be developed for the Framework.

The development of a social licence is also heavily influenced by the extent to which the proposal is the subject of consultation with the community. To inform the design of the legislative framework, the Department of the Prime Minister & Cabinet has already engaged in extensive stakeholder consultation – Refer to Appendix 3 for further details.

However, a social licence also depends on how the *DS&R Framework* is implemented in practice.

[41] Productivity Commission Inquiry Report, Australian Government, *Data Access and Use* (2017) <www.pc.gov.au/inquiries/completed/data-access#report>.

Appendix 1 – Glossary and acronyms

Acronym	Description
APP	Australian Privacy Principle
DPMC	Department of the Prime Minister and Cabinet <www.pmc.gov.au>
DS&R	Data Sharing and Release
DSE	Data Sharing Entity
MOU	Memorandum of Understanding
NDC	National Data Commissioner <www.datacommissioner.gov.au>
OAIC	Office of the Australian Information Commissioner <www.oaic.gov.au>
PIA	Privacy Impact Assessment <www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments>

Appendix 2 – Key documents referred to

Public Documents

Productivity Commission

- Productivity Commission Inquiry Report, Australian Government, *Data Access and Use* (2017) <www.pc.gov.au/inquiries/completed/data-access#report>
- Department of the Prime Minister and Cabinet, *Data Availability and Use – The Australian Government's response to the Productivity Commission Data Availability and Use Inquiry* (2018) <dataavailability.pmc.gov.au>

Initial Issues Paper

- Department of the Prime Minister and Cabinet, *New Australian Government Data Sharing and Release Legislation: Issues paper for consultation* (4 July 2018) <www.pmc.gov.au/resource-centre/public-data/issues-paper-data-sharing-release-legislation>.
- Submissions <www.pmc.gov.au/public-data/data-sharing-and-release-reforms/submissions>

Internal Documents (Department of the Prime Minister and Cabinet, Office of the National Data Commissioner)

Data Sharing Legislation – Policy Position Documents

- 21 September 2018 <Policy Positions_Draft 21Sept2018.pdf>
- 13 December 2018 <PMC Policy Positions_Updated 13 Dec 2018_IDC.pdf>
- 22 February 2019 <Data Legislation Policy paper_22Feb2019.pdf>

Instructions for Drafting the Data Sharing and Release Bill

- *Tranche 1* (23 August 2018)
- *Tranche 2* (7 November 2019)
- *Tranche 3* (13 March 2019)

Appendix 3 – Stakeholder Consultation

Stakeholder Engagement by Galexia for this PIA

Galexia has undertaken a limited and targeted number of stakeholder meetings, directly engaging on issues arising from stakeholder submissions and the draft policy positions being developed by DPMC.

Community

- Australian Privacy Foundation (APF) <https://privacy.org.au>
- Consumers Health Forum of Australia (CHF) <https://chf.org.au>
- Consumer Research Policy Centre (CRPC) <https://cprc.org.au>
- Electronic Frontiers Australia (EFA) <https://www.efa.org.au>
- Federation of Ethnic Community Councils Australia (FECCA) <http://fecca.org.au>
- Information Governance ANZ (IGANZ) <http://www.infogovanz.com>

Regulators

- Office of the Australian Information Commissioner (OAIC) <https://www.oaic.gov.au>
- Office of the Information Commissioner Queensland <https://www.oic.qld.gov.au>
- Information and Privacy Commission NSW <https://www.ipc.nsw.gov.au>
- Office of the Victorian Information Commissioner <https://ovic.vic.gov.au>
- Office of the Information Commissioner Northern Territory <https://infocomm.nt.gov.au>

Broader Engagement by the Department for the *DS&R Framework* more Generally

To inform the design of the legislative framework, the Department of the Prime Minister & Cabinet released an Issues Paper in July 2018 and processed 108 responding submissions. They undertook three rounds of consultation within and external to government. The consultation work comprised bi- and multi- lateral meetings within government, workshops, and over 50 roundtable discussions to date with external participants from industry, research, and not-for-profit sectors as well as special interest advocacy groups on privacy and security.

Issues, concerns, and solutions raised during these consultations have helped shape the design of the legislative framework. In particular, consultation has led to evolution of policy positions underpinning the legislation to clarify purposes for data sharing, strengthen transparency mechanisms, and refine positions to support open release of data.

Further consultation will be undertaken as the legislative reform package develops.

The Department's consultation builds on consultation undertaken by the Productivity Commission to inform its recommendations on Data Availability and Use (which led to the proposed DS&R reforms), and the Government taskforce responding to the Productivity Commission's recommendations.

To date, the Department has held approximately 68 sessions, including:

- 16 high level governmental meetings (which include 9 co-design workshops), and
- 52 roundtables – The roundtables were attended by representatives from more than 250 organisations in government, academia, business or private sector, and civil society
    - 36 were held in 2018 and
    - 16 in 2019

Appendix 4 – DPMC Response to the Recommendations in the *Data Sharing & Release Bill* PIA

The Department of the Prime Minister & Cabinet has made the following responses and commentary to the recommendations – as at 28 June 2019.

Component / APP	Galexia Recommendation	DMPC Response
Key Policy Position 1: Distinguishing between data sharing and data release	**Recommendation 1:** Splitting data sharing and data release requirements The requirements in the Bill for data sharing and data release should be split, so that each activity has its own stand-alone set of requirements, tailored for that activity.	**Agree**
DPMC Comment: The Department agrees with this recommendation and notes that the proposed legislative framework already aligns with it. The framework authorises sharing, and will support but not create a new authorisation for the open release of data – the processes are distinct. Guidance and advice issued by the National Data Commissioner may be applicable to both processes – for instance, the Data Sharing Principles can be used to mitigate risks of both sharing and release – but there will be tailored considerations for each process.		
Key Policy Position 1: Distinguishing between data sharing and data release	**Recommendation 2:** Enhanced privacy safeguards for data release If data release is authorised by the legislation, then additional legislated enhanced privacy safeguards for data release will be required. These should include: 1) An additional public interest test; 2) A data custodian veto power; and 3) Enhanced sanctions.	**Agree in Principle**
DPMC Comment: The Department agrees in principle with this recommendation, noting that the *DS&R Framework* will support but not authorise open release of data, as noted in response to Recommendation 1.		
Key Policy Position 2: Compliance activities	**Recommendation 3:** Exclusion of compliance activities The Bill should exclude compliance activities related to an individual as an approved purpose for data sharing or data release.	**Agree**
DPMC Comment: The Department agrees with this recommendation. While compliance activities are a valid and important function of government, these activities are most appropriately handled under different legislation. Sharing data for compliance activities may occur under specific portfolio legislation, but will not be authorised by the *DS&R Framework*.		
Key Policy Position 3: Covering the States and Territories	**Recommendation 4:** Additional Data Breach Notification requirements The Bill should include a mechanism for imposing a Data Breach Notification requirement where the entities involved operate in a State or Territory where such a requirement does not yet exist.	**Agree**
DPMC Comment: The Department agrees with this recommendation, which aligns with policy intent that entities participating in the DS&R system will have equivalent privacy obligations, including in relation to notification and mitigation of suspected data breaches.		
APP 1 – Openness and Transparent Management	**Recommendation 5:** Improved openness in Privacy Policies about data sharing / release Agencies and accredited entities should be more open about data sharing and the potential disclosure of some data to external users.	**Agree**
DPMC Comment: The Department agrees with this recommendation, noting that while transparency and accountability are central to the *DS&R Framework*, Privacy Policies are regulated by the *Privacy Act* not the *DS&R Framework*. The National Data Commissioner will advocate for more transparency on data sharing, including by working with the Australian Information Commissioner to support best practice and agencies' compliance with the requirements of both systems, such as ensuring entities' Privacy Policies reflect their participation in the DS&R system.		

APP 1 – Openness and Transparent Management	**Recommendation 6:** Establish a user friendly public information resource The National Data Commissioner and any third party entity that is accredited to receive data or act as a Data Service Provider should be required to maintain a user friendly public information resource that lists: 1) Core data sharing and data release activities; 2) Data sources; and 3) A register of data sharing agreements.	**Agree in Principle**
DPMC Comment: The Department agrees in principle with this recommendation, noting that the *DS&R Framework* will require the establishment and maintenance of a public data sharing agreement register that will contain the recommended information on data sharing under the DS&R system. This means data release and data sharing activities relying on other authorisations will not be covered. As additional accountability measures, the National Data Commissioner will report on data sharing activities in the DS&R system in its annual report, and will advocate for greater transparency on data sharing and release activities more broadly.		
APP 3 – Collection of solicited personal information	**Recommendation 7.** Minimisation of data collection The Bill should ensure that data minimisation is a clear requirement for data sharing. The Bill should include the word 'only' in the requirement: e.g. 'sharing **only** data that is reasonably necessary'.	**Agree**
DPMC Comment: The Department agrees with this recommendation and has implemented it within the proposed framework. The purpose test incorporates the 'data minimisation' concept by authorising sharing of only data that is reasonably necessary to achieve an approved purpose.		
APP 5 – Notification	**Recommendation 8:** Improved openness in Notices about data sharing / release Agencies and accredited entities should be more open in their Notices about the use of data sharing and the potential disclosure of some data to external users. The National Data Commissioner and the Office of the Australian Information Commissioner should consider the following options: 1) Development of a standard Notice template; 2) Development of Guidance on when and how to issue Notices; 3) A prohibition on using data collected prior to the implementation of effective Notices; and 4) Checking Notices for compliance.	**Agree in Principle**
DPMC Comment: The Department agrees that entities should ensure Privacy Notices reflect their participation in the DS&R system. However, the Department notes that some agencies' Privacy Notices already inform people that their data may be shared for government and research purposes, which supports the use and reuse of data for these purposes. As such, option 3 of the recommendation may need further consideration. It should also be noted that Privacy Notices are a matter of compliance with the *Privacy Act*, so are within the remit of the Australian Information Commissioner rather than the National Data Commissioner. The National Data Commissioner intends to work together with the Australian Information Commissioner to support entities to comply with the respective legislative frameworks and consider the recommended options		