

# **DATA AVAILABILITY AND TRANSPARENCY BILL 2020**

## **EXPLANATORY MEMORANDUM**

**DRAFT SEPTEMBER 2020**

# Contents

Data Availability and Transparency Bill 2020 .....	4
1 – Overview .....	4
The legislative scheme .....	5
Scope .....	6
Interaction with other schemes .....	6
Enabling safe data sharing .....	7
Sharing data for certain reasons – the permitted purposes .....	7
Sharing data safely – the Data Sharing Principles .....	8
Sharing data with the right people – Accreditation scheme .....	8
Better management and transparency .....	9
Integrity of the scheme .....	9
Oversight by the National Data Commissioner .....	9
Avenues for redress – complaints and review of decisions .....	9
Dealing with breaches – penalties and consequences .....	10
Periodic reviews of the operation of the Bill .....	11
2 – Notes on Clauses .....	12
Chapter 1 – Preliminary .....	12
Part 1.1 – Introduction .....	12
Part 1.2 – Definitions .....	14
Chapter 2 – Authorisation to share data .....	18
Chapter 3 – Responsibilities of data scheme entities .....	32
Part 3.1 – Introduction .....	32
Part 3.2 – Responsibilities of data scheme entities .....	33
Part 3.3 – Data breach responsibilities .....	36
Chapter 4 – National Data Commissioner etc. ....	39
Part 4.1 – Introduction .....	39
Part 4.2 – National Data Commissioner .....	39
Part 4.3 – National Data Advisory Council .....	44
Chapter 5 – Regulation and enforcement .....	47
Part 5.1 – Introduction .....	47
Part 5.2 – Accreditation .....	47
Part 5.3 – Complaints .....	49
Part 5.4 – Assessments and investigations .....	52

## Explanatory Memorandum: Data Availability and Transparency Bill 2020

Part 5.5 – Regulatory powers and enforcement .....	54
Chapter 6 – Other matters .....	60
Part 6.1 – Introduction .....	60
Part 6.2 – Review of decisions.....	61
Part 6.3 – Treatment of certain entities .....	63
Part 6.4 – Data sharing scheme instruments .....	66
Part 6.5 – Other matters .....	70

DRAFT

# Data Availability and Transparency Bill 2020

The following abbreviations are used throughout this explanatory memorandum:

ADSP	Accredited data service provider
Commissioner	National Data Commissioner
Council	National Data Advisory Council
<i>Criminal Code</i>	Schedule to the <i>Criminal Code Act 1995</i> (Cth)
Data sharing scheme	The framework of instruments and operational processes to enable and regulate data sharing established by this Bill.
<i>FOI Act</i>	<i>Freedom of Information Act 1982</i> (Cth)
Guide to Framing Commonwealth Offences	Attorney-General's Department, 'Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers' (Sept, 2011)
<i>Privacy Act</i>	<i>Privacy Act 1988</i> (Cth)
<i>PGPA Act</i>	<i>Public Governance, Performance and Accountability Act 2013</i> (Cth)
<i>Regulatory Powers Act</i>	<i>Regulatory Powers (Standard Provisions) Act 2014</i> (Cth)

## 1 – Overview

1. In 2018, the Australian Government committed to reform the way it shares public sector data. Reforms are necessary to realise the benefits of greater data availability and use identified by a Productivity Commission inquiry, supporting economic and research opportunities and the Government's vision for streamlined and efficient service delivery.
2. The Data Availability and Transparency Bill is central to these reforms. The Bill authorises and regulates controlled access ('sharing') of Commonwealth data, with safeguards in place to manage risk and streamline processes. This pathway for sharing is optional. Existing mechanisms and arrangements for sharing continue to be available.
3. The Bill takes a principles-based approach to data sharing, providing parties with flexibility to tailor sharing arrangements, and ensuring the scheme can respond to evolving technologies and community expectations. Modernising the approach to sharing public sector data will empower government to deliver effective services and better-informed policy, and support research and development.
4. The Department of the Prime Minister and Cabinet (PM&C) developed the Bill and its underlying policy positions through extensive co-design and engagement with experts, stakeholders, and the community. Discussion papers were released in 2018 and 2019 to test policies with the public and seek input to refine positions. These papers were supported by 76 public roundtables across Australia to consider policy evolutions and strengthen safeguards. Further consultation will be undertaken on an exposure draft of the Bill over eight weeks in 2020.
5. In developing the Bill, PM&C has taken a privacy by design approach to identify, minimise and mitigate privacy impacts wherever possible. Two independent PIAs were undertaken to identify strengths and weaknesses in the early policy positions and planned legislative framework, and the draft Bill itself. Privacy safeguards were also strengthened in response to

guidance and advice from the National Data Advisory Council and privacy experts, including the Office of the Australian Information Commissioner.

6. This is a draft of the explanatory memorandum, intended to assist interpretation of the exposure draft Bill. It will be updated to reflect the final version of the Bill introduced to Parliament.

## The legislative scheme

7. The Bill establishes a new data sharing scheme which will serve as a pathway and regulatory framework for sharing public sector data. ‘Sharing’ involves providing controlled access to data, as distinct from open release to the public.
8. To oversee the scheme and support best practice, the Bill creates a new independent regulator, the National Data Commissioner (the Commissioner). The Commissioner’s role is modelled on other regulators such as the Australian Information Commissioner, with whom the Commissioner will cooperate.
9. The data sharing scheme comprises the Bill and disallowable legislative instruments (Regulations, Minister-made rules, and any data codes issued by the Commissioner). The Commissioner may also issue non-legislative guidelines that participating entities must have regard to, and may release other guidance as necessary.
10. Participants in the scheme are known as data scheme entities:
  - Data custodians are Commonwealth bodies that control public sector data, and have the right to deal with that data.
  - Accredited users are entities accredited by the Commissioner to access to public sector data. To become accredited, entities must satisfy the security, privacy, infrastructure and governance requirements set out in Ministerial Rules.
  - Accredited data service providers (ADSPs) are entities accredited by the Commissioner to perform data services such as data integration. Government agencies and users will be able to draw upon ADSPs’ expertise to help them to share and use data safely.
11. The Bill does not compel sharing. Data custodians are responsible for assessing each sharing request, and deciding whether to share their data if satisfied the risks can be managed.
12. The data sharing scheme contains robust safeguards to ensure sharing occurs in a consistent and transparent manner, in accordance with community expectations. The Bill authorises data custodians to share public sector data with accredited users, directly or through an ADSP, where:
  - sharing is for a permitted purpose – government service delivery, informing government policy and programs, or research and development;
  - the data sharing principles have been applied to manage the risks of sharing; and
  - the terms of the arrangement are recorded in a data sharing agreement.
13. Where the above requirements are met the Bill provides a limited statutory authority to share public sector data, despite other Commonwealth, State and Territory laws that prevent sharing. This override of non-disclosure laws is ‘limited’ because it occurs only when the Bill’s requirements are met, and only to the extent necessary to facilitate sharing.
14. If the Bill’s requirements are not satisfied, it does not give legal authority to share the data. In this instance, the situation ‘rebounds’ so the protections and penalty frameworks of the original non-disclosure law apply. Where there are no applicable non-disclosure provisions to rebound

to, the Bill includes penalties and offences provide an avenue of redress for unauthorised sharing. This approach ensures there are always protections for data shared or created under this scheme.

15. The override is also limited by the Regulations, which list certain secrecy and non-disclosure provisions that will not be overridden by the Bill. If a provision is not listed, it remains at the discretion of the data custodian whether to share data. Provisions that do not impose duties of non-disclosure, such as those relating to data handling or security like the Australian Privacy Principles, are not overridden and continue to apply to data shared under this scheme.
16. Robust transparency and accountability mechanisms are embedded in the Bill to promote integrity and trust in the scheme. For example, details of accredited entities and sharing projects will be made publicly available, allowing Australians to better understand how government data is being used. The Commissioner also reports annually to Parliament on the operation of the scheme, and the Bill prescribes periodic reviews of the scheme to ensure it continues to operate in accordance with needs and expectations.

## Scope

17. To maximise benefits, a wide range of data and entities are within scope of the data sharing scheme.
18. The Bill authorises data custodians to share public sector data with accredited entities from all levels of government as well as industry, research, and other private sectors.
19. 'Public sector data' encompasses all data held and created by or on behalf of the Commonwealth. The concept of data includes facts, statistics, and other information that are capable of being communicated, analysed or processed via physical or electronic means.
20. The Australian Government has separately established a Consumer Data Right to boost competition and to enhance consumers' access to and control of their data in the private sector.
21. The Bill's in-built safeguards encourage agencies to manage the risks of sharing, rather than avoid sharing altogether. Exclusions from the scheme have been granted, however, where strictly necessary to balance the impetus for greater access to public sector data with other legitimate interests. For instance, the Bill does not authorise sharing that would infringe intellectual property rights or international agreements, or where intelligence entities or their data are involved. The Bill also excludes sharing of operational data and evidence before courts, tribunals, and certain agencies with oversight or integrity functions to protect the independence and confidentiality of their core functions. Specific provisions will also be exempted to ensure especially sensitive data handled under other legislation, such as My Health Record information, is not shared through this scheme.

## Interaction with other schemes

22. The Bill establishes an alternate pathway for the sharing of government data. All existing pathways and mechanisms for data sharing will continue to operate unaffected as the Bill does not replace or change these arrangements.
23. Existing legal obligations and policies for handling government data will continue to apply, including the Australian Privacy Principles in the *Privacy Act*, records management requirements under the *Archives Act 1983*, and the Protective Security Policy Framework.
24. While the Bill focuses on data sharing, it also preserves established legal pathways for open data release. The Bill supports but does not provide authority to release data, as there are already a range of legal mechanisms for this. Outputs created through the sharing process may be

released, where the data custodian agrees and the release has the support of an existing legal authority.

25. Operational tools for sharing data can be adapted to facilitate release. For example, the data sharing principles can be used to mitigate the risks of releasing data under other laws. The Commissioner's advocacy function also allows the Commissioner to work with agencies to address cultural barriers to improving data availability and use more broadly.

## **Enabling safe data sharing**

26. The Bill enables controlled sharing of data for the prescribed purposes, with accredited people and with safeguards in place. The Bill allows for building valuable data assets such as integrated data assets that can be re-used to deliver benefits effectively. Sharing is underpinned by strong transparency and accountability measures while the National Data Commissioner provides oversight to build trust in the data sharing scheme.

## **Sharing data for certain reasons – the permitted purposes**

27. The Australian Government collects and uses data for a wide range of purposes, to support government agencies to fulfil their functions. The Bill focuses on three specific purposes in line with community needs and expectations, allowing other government functions to continue under existing laws.
28. The Bill authorises data sharing for the purposes of:
  - delivery of government services;
  - informing government policy and programs; and
  - research and development.
29. Government services are government activities that provide coordinated and structured advice, support, and services to individuals. Sharing data for this purpose could enable improved designs of systems, engagement, and processes involved in delivery of services, including improving user experiences through simplified or automated systems like pre-filled forms and reminders to submit or verify details.
30. Sharing data to inform government policy and programs is a permitted purpose and is interpreted broadly. Data shared under this purpose could help enable the discovery of trends and risks to inform public policy making, enable modelling of policy and program interventions, and provide a holistic understanding of cross-portfolio impacts and 'wicked problems'.
31. The third permitted purpose enables sharing for research and development. This term includes activities to advance knowledge and contribute to society. Sharing for these purposes will enable accredited academics, scientists, and innovators in the public and private sectors to access public sector data to gain insights which could enhance Australia's socio-economic wellbeing.
32. The Bill precludes sharing public sector data for certain purposes, such as compliance and assurance activities, and other enforcement-related purposes. The Bill also does not authorise data sharing for purposes that relate to or could jeopardise national security, including the prevention or commission of domestic terrorism and espionage. While these are legitimate functions of government, they require specific oversight and redress mechanisms that are better dealt with through dedicated legislation. Existing legislation governing these activities will continue to operate alongside the Bill.

33. The Minister may preclude additional purposes through a rule making power to address any future risks that may emerge.

### **Sharing data safely – the Data Sharing Principles**

34. Once a data custodian is satisfied a proposed project is for a permitted purpose, it must apply the Data Sharing Principles to assess risks of sharing in a holistic manner, and set controls to effectively manage identified risks. The principles are a framework for best practice risk management, which enables parties to adapt controls to suit the needs and context of each sharing arrangement.
35. The principles are structured to consider risks arising across five key elements of the sharing process – project, people, settings, data and outputs:
- The project principle considers the intended use of the shared data, including public interest, consent and ethics requirements.
  - The people principle considers users accessing the data to ensure they can be trusted and have the right skills for the project.
  - The settings principle assesses if data is shared in a safe environment.
  - The data principle assists in navigating what data is appropriate for sharing. Only the amount and detail of data that is reasonably necessary to achieve the project should be shared.
  - The outputs principle ensures the results and outcomes of the projects are agreed, including whether they are appropriate for publishing.
36. The principles work together: overarching conceptual issues are considered under the project principle, while the other principles address technical and operational matters. Controls can be dialled up and down among the principles to suit the overall needs of each project, for instance a tightly controlled access environment such as a secure lab may support analysis of detailed (rather than aggregate) data. The data custodian is responsible for considering each principle and setting controls that manage risks overall.
37. The controls under the principles and the party responsible for implementing them are detailed in a publicly available data sharing agreement. The Commissioner has oversight of agreements, and powers to monitor and enforce data scheme entities' compliance with their responsibilities under this Bill.

### **Sharing data with the right people – Accreditation scheme**

38. The Bill empowers the Commissioner to accredit entities as accredited users and/or ADSPs in accordance with criteria established in Ministerial rules. Accreditation serves as a gateway into the data scheme as entities must be accredited before they can access data.
39. The accreditation process involves assessment of prospective recipients of data and their capacity to keep data safe. However, accreditation does not guarantee data will be shared with a user for a particular project, as the custodian may determine the risks of sharing in that instance cannot be properly controlled or mitigated.
40. The Commissioner will be able to control system-wide risks presented by individuals and organisations by revoking or amending accreditation. The Commissioner may also receive security advice about individuals and organisations seeking accreditation.



## **Better management and transparency**

41. The Government currently shares data for a range of valuable projects, but recognises the need for a more consistent and streamlined approach to sharing. To achieve this outcome, the Bill contains a range of measures to support good data governance and encourage public trust through transparency.
42. Data sharing agreements are a key governance and transparency measure. All sharing arrangements under the Bill must be recorded in a data sharing agreement that includes a set of minimum mandatory terms. These standardised terms will support greater consistency and clarity of obligations, and reduce the need for complex negotiations.
43. To promote transparency of sharing arrangements, the Commissioner will publish public registers of data sharing agreements and accredited entities. These registers will provide insight into what data is being shared and why, who is accessing data, and how it is being safely shared.
44. The Commissioner will also report annually on how the data scheme is operating to highlight system-wide opportunities and areas for improvement.

## **Integrity of the scheme**

### **Oversight by the National Data Commissioner**

45. The Bill establishes the National Data Commissioner as an independent statutory office holder charged with overseeing the data sharing scheme as its regulator and champion. Australian Public Service staff and contractors will assist the Commissioner to perform their functions. Staff will be drawn from the Department responsible for administering the Bill, however contractors will be used where this affiliation may give rise to conflicts of interest.
46. As champion of the data sharing scheme, the Commissioner will provide advice, advocacy and guidance to ensure the scheme operates as intended. The Commissioner will also work with data scheme entities to build data capability, promote best practice data sharing and use, and address cultural barriers to sharing.
47. The Bill establishes a National Data Advisory Council as a source of expertise to support the Commissioner in their guidance, advice and advocacy functions. Members of the Council will be appointed by virtue of their depth of experience and expertise relevant to the data sharing scheme. The Council may advise the Commissioner on issues such as ethical data use, privacy, community expectations, technical best practice, and industry and international developments. The Commissioner may also seek advice from the Council on issues relating to the broader data environment.
48. As regulator, the Commissioner has oversight of the scheme and is empowered to monitor, investigate, and enforce compliance with the Bill by data scheme entities. A range of mechanisms are embedded in the Bill to deter and address non-compliance, while allowing the Commissioner to act proportionally according to the circumstances of each case. Options range from working with the entity to address the situation such as by entering enforceable undertakings, to issuing a direction for the entity to comply or seeking judicial penalty. These powers have been modelled on other regulators with similar mandates, and apply the learnings from recent inquiries into effective regulatory action.

### **Avenues for redress – complaints and review of decisions**

49. The Bill provides means for data scheme entities to raise issues about breaches or decisions under the scheme, and existing avenues for redress continue to be available.

50. A complaints mechanism enables data scheme entities to complain to the National Data Commissioner, separately or as a class action, about potential breaches of the legislation. This triggers the Commissioner's regulatory powers to investigate and address the situation.
51. Regulatory decisions made by the Commissioner may be reviewed for their merits or legality through standard administrative review processes.
52. Data sharing decisions by data custodians will not be reviewable on their merits under this scheme. Such decisions are best made by data custodians as they have a full understanding of the risks of and public interest in sharing their data.
53. It is important to distinguish administrative review from the regulatory oversight and powers exercised by the National Data Commissioner with respect to data sharing activities and entities.
54. Existing avenues for redress in other schemes continue to be available, including where the situation involves sharing or shared data. For example a person affected by a decision based on shared data may seek review of that decision, where legislation governing that decision sets review rights. A person may also complain about government activities to the Commonwealth Ombudsman, or to the Australian Information Commissioner about suspected mishandling of their personal information.
55. The Bill also supports a 'no wrong door' approach by empowering the Commissioner to transfer matters and information to other regulatory bodies, such as the Australian Information Commissioner. Other regulators will have reciprocal powers to transfer matters to the National Data Commissioner. This approach means anyone who files a complaint or raises an issue can be connected with the appropriate service or regulator.

### **Dealing with breaches – penalties and consequences**

56. The Bill contains penalty frameworks to deter non-compliance with its requirements and to protect data shared or created through the scheme.
57. If sharing or use of public sector data occurs in a manner not authorised by this Bill, other non-disclosure laws are not overridden and their penalties apply.
58. This Bill enables sharing by overriding non-disclosure provisions in other laws, where sharing is for a permitted purpose and safeguards are in place. If these requirements are not met the situation 'rebounds' so the original non-disclosure provisions and penalties apply. Where there are no applicable non-disclosure provisions to rebound to, the Bill contains 'gap coverage' penalties to ensure redress is always available for unauthorised sharing.
59. The Bill also includes civil penalties and criminal offences to cover situations which are unique to the data sharing scheme, such as where a data scheme entity has not complied with conditions of its accreditation. The maximum penalties set in the Bill balance those in more established frameworks, such as the *Privacy Act*, with more contemporary offences for mishandling government and consumer data.
60. The Bill also provides a framework for mitigation and reporting of unauthorised access to data that has been shared or created under this scheme (a data breach). Data scheme entities have responsibility to mitigate harm arising from data breaches, and to report serious data breaches to the National Data Commissioner.
61. If a serious data breach involves personal information, it must also be reported to the Australian Information Commissioner. The Bill preserves the Australian Information Commissioner's oversight of data breaches involving personal information by engaging the notifiable data breach scheme under Part IIIC of the *Privacy Act*. Responsibility for notification rests with the Data Custodian or an accredited entity covered by the *Privacy Act* involved in sharing. A copy

of the statement provided to the Information Commissioner must be given to the National Data Commissioner, to ensure their continuing oversight over the data sharing scheme.

### **Periodic reviews of the operation of the Bill**

62. The Bill is drafted as principles-based legislation to ensure it remains relevant and adaptable to evolving technology and public expectations. The Bill will also be reviewed periodically to ensure the data sharing scheme operates as intended, and to provide opportunity for improvement.
63. The first review will occur three years after commencement of the Bill to allow initial issues to be identified and addressed. Periodic reviews will also occur every ten years from commencement to address any emerging issues in the longer term. Review reports will be tabled in each House of the Parliament by the responsible Minister.

## 2 – Notes on Clauses

### Chapter 1 – Preliminary

#### Part 1.1 – Introduction

1. This Part sets out the preliminary matters for the operation of this Bill, including its short title, commencement, objects, and geographical jurisdiction.

##### Clause 1 – Short title

2. Once enacted, the short title of the Act will be the *Data Availability and Transparency Act*.

##### Clause 2 – Commencement

3. The entire Bill will commence the day after Royal Assent is received, as set out in the table.
4. This approach establishes the National Data Commissioner (the Commissioner) and empowers them to implement the data sharing scheme created by the Bill.
5. In practice, the data sharing scheme will be operational once the Commissioner is appointed, and the instruments and systems underpinning the data sharing scheme have been implemented, in particular the accreditation framework (refer clause 74).

##### Clause 3 – Objects

6. The ultimate intent in enacting this legislation is to improve how Australia shares public sector data to drive service delivery, evidence-based policy, research and innovation.
7. This clause sets out specific objectives of the legislation to achieve the Government's intent, addressing priorities identified in the Productivity Commission report on Data Availability and Use for establishing a scheme to enable and regulate sharing of public sector data.
8. Together, these objectives encourage greater sharing of public sector data with robust safeguards to protect privacy and data security while enhancing integrity and transparency to build community confidence. Establishment of the National Data Commissioner to administer and regulate the data sharing scheme is a central to achieving these objectives.
9. Substantive provisions elsewhere in the Bill should be read in light of these objectives.

##### Clause 4 – Simplified outline of this Act

10. This clause provides a succinct overview of the crucial concepts and content of the Bill, which establishes the National Data Commissioner as regulator of a new data sharing scheme for sharing public sector data.
11. Simplified outlines are included to assist readers to understand the substantive provisions of this Bill. However, readers should rely on the substantive provisions of this Bill as these outlines are not intended to be comprehensive.

##### Clause 5 – Act binds the Crown

12. This clause provides that the Bill binds the Crown in each of its capacities. Consistent with standard practice, this does not render the Crown liable to criminal prosecution, though it may be subject to civil penalty.
13. The shield of the Crown does not extend to government business enterprises, or to Commonwealth employees acting outside their lawful authority.

**Clause 6 – Extension to external Territories**

14. This clause operates with clause 7 to ensure the authorisations, safeguards, and regulatory aspects of the data sharing scheme apply consistently throughout Australia's mainland and external territories, as well as extraterritorially.
15. The geographic scope of the Bill – where it applies – as established by clauses 6 and 7 is consistent with similar legislative frameworks such as the *Privacy Act*.

**Clause 7 – Extraterritorial operation**

16. This clause extends the application of this Bill and relevant parts of the *Regulatory Powers Act* to conduct, matters, and things outside of Australia. The clause applies to both civil contraventions and criminal offences.
17. Establishing extraterritorial application of this Bill is necessary given foreign entities may be accredited, and technological advances mean that data is increasingly stored offshore and may be accessed remotely. Extending the application of the Bill in this way ensures the safeguards inherent in the data sharing scheme apply consistently to all participants and situations, and are capable of adapting to emerging and future needs.
18. Consistent with relevant schemes such as the *Privacy Act* and the *Criminal Code*, subclause (1) and clause 122 provide that the Bill and applicable sections of the *Regulatory Powers Act* have extraterritorial effect.
19. Subclause (2) makes clear that any extraterritorial exercise of regulatory power by the Commissioner must be in accordance with international law and agreements, including Commonwealth laws giving effect to such agreements. The Commissioner would act in cooperation with relevant regulators in foreign jurisdictions.

**Clause 8 – Application of this Act**

20. This clause sets out the circumstances in which the Commonwealth has authority to share and regulate sharing of public sector data under this Bill. Each subclause invokes relevant powers of the Commonwealth under the *Australian Constitution*.
21. For sharing to be authorised under the Bill, it must be supported by one or more of these subclauses, and meet the other requirements in Chapter 2 (especially clauses 13 and 15).
22. Data may be shared to inform Commonwealth policy, programs, or service delivery. This includes sharing for the recipient's own purposes (within the limits of clause 15).
23. Subclauses (a), (c) and (d) describe circumstances where sharing occurs with or through particular types of accredited entities. Subclauses (b), (e), (f) and (g) support sharing by a data custodian with any kind of accredited entity, both government (Commonwealth, State, or Territory) and non-government.
24. Subclause (a) supports sharing where the intermediary or the recipient (or both) accessing the shared data is a Commonwealth or Territory body. This clause may apply where sharing involves an ADSP that is such a body (regardless of the nature of the end user), or where a custodian shares directly to an accredited user that is a Commonwealth or Territory body. This subclause could cover situations where data is shared with a Commonwealth or Territory government agency to inform design of policies, programs, or services within its legislative power, or to conduct research or development activities.
25. Subclause (b) covers sharing for the purpose of informing policy, programs, or service delivery where those activities are conducted by, or involve, the Commonwealth government. This could support sharing between Commonwealth entities. It could also support sharing where the Commonwealth government is 'involved', such as where the accredited user is a non-government

organisation like a charity that is delivering a government program or service on behalf of the Commonwealth – for instance disaster relief or directly implementing support services. Similarly, a Commonwealth data custodian sharing with an accredited State government authority to inform the design of a joint Commonwealth-State infrastructure program could be in scope of this subclause. In this latter example, however, sharing could not be taken to ‘include’ the Commonwealth government if the sharing were to inform the State authority’s own policies, programs or services. Alternate bases of support for this type of sharing are addressed below.

26. Subclause (c) is relevant where data is shared for research and development purposes with an accredited user that is a trading or financial corporation formed within the Commonwealth, or a foreign corporation. This subclause could support sharing with a research institute to inform Commonwealth research and development, or its own independent research and development.
27. Subclause (d) covers sharing with an accredited user where that user is a foreign person and the sharing is done in accordance with an international agreement binding on Australia. This provision could operate where there is a bilateral treaty for information sharing between Australia and a foreign government, or an inter-governmental agreement for research cooperation.
28. Subclause (e) covers data sharing by means of electronic communication – that is, transfer of information via the internet or a telecommunications network. This subclause covers electronic transmission of data to accredited users (from all levels of government, as well as non-government entities) to inform any of the purposes in clause 15. For example, a data custodian could rely on this subclause to transfer data from its computer or server to that of a State government authority for the recipient’s own policies, programs and services, or for research and development, as the application is not restricted to *Commonwealth* government purposes. Transfer of information through non-electronic means, such as printed paper, could be supported by other subclauses in clause 8.
29. Subclause (f) may apply where data is shared for statistical purposes such as the compilation or analysis of statistics, or to enable research that is statistical in nature. Subclause (g) is relevant where census or statistical information such as from a survey or administrative source is shared. Both subclauses could support sharing with or through accredited entities, whether government (any level) or non-government.

## Part 1.2 – Definitions

30. This Part contains key definitions used throughout the Bill.

### Clause 9 – Definitions

31. This clause sets out definitions and terms used throughout the Bill. Some defined terms are signposts that refer readers to the clauses in which those terms are substantively defined.
32. Where possible, existing definitions have been used or adapted to ensure this Bill operates smoothly alongside other legislative schemes. Where a word is not defined, readers should rely on its ordinary meaning, when read in context of the provision it appears in as well as the Bill more broadly.
33. Key definitions from this clause are explained below in alphabetical order.
34. *Accreditation framework* – means the framework described in clause 74, which will be established by Ministerial rules (refer clause 74(1)).
35. *Breach* – conduct which contravenes or is inconsistent with requirements of this Bill. These requirements include those imposed by subordinate legislative instruments (regulations, rules, codes). A legislative breach is distinct from a data breach, which is defined in clause 34.

36. *Commonwealth bodies* – this definition captures all bodies under the standard *PGPA Act* definitions of Commonwealth entities and companies, as well as other bodies under the *FOI Act*, such as statutory office holders and judicial bodies.
37. *Data service* – this definition describes what services an accredited data service provider may provide as an intermediary in sharing arrangements made under this Bill. The scope of services is broad in recognition of the diverse range of activities involved in sharing and managing data, where data custodians may seek support. The range of services, or conditions their provision, may be addressed through a data code or Ministerial rules (refer clauses 112 and 119). Data services performed by ADSP must involve the public sector data shared by the relevant data custodian, but are not limited to services involving only public sector data where supported by other legal authority (refer clause 10 definition of ‘ADSP enhanced data’) and clause 13(3)).
38. *Data sharing scheme* – this term encompasses the legislative framework established by the Bill and subordinate legislative instruments (regulations, rules, and data codes), as well as guidelines made under clause 113.
39. *Engage in conduct* – this definition clarifies that positive actions as well as failing or omitting to do something is considered ‘conduct’. This clarity is important for determining breach, for instance it means failure to do something in order to comply with a requirement of the data sharing scheme may be considered a breach.
40. *Entity* – this term is broadly defined to reflect the scope and objectives of the Bill. It covers all types of Australian and foreign entities capable of participating in the data sharing scheme. This includes individuals, government bodies, body corporate and body politics, and non-legal entities. Part 6.3 deals with how certain entities are treated under this scheme. Limits on participation are achieved through the definition of ‘data custodian’ in clause 11(2), restrictions on sharing in clause 17, and the accreditation framework set out in clause 74, which provides a gateway to participation in the data sharing scheme.
41. *Officer* – this definition clarifies the relationship between a data scheme entity and one type of person it acts through, for the purpose of attributing conduct to the entity under clause 109. Examples of ‘officers’ include persons who are employed in or appointed to decision-making roles, like Secretaries of government departments and heads of research institutes.
42. *Release* – in the context of this Bill, release means the data is made openly (i.e. publicly) available, so the entity that released the data retains no control over it. The aspect of control is critical to distinguish data release from data sharing.
43. *Share* – this definition captures all aspects of the process authorised by clause 13. The concept includes both providing and receiving controlled access to public sector data. The term ‘share’ is used throughout this Bill to refer to the process of providing controlled access under clause 13(1), however, it is sometimes used to describe individual activities, such as the process in clause 13(1), or specific activities authorised by clause 13(3).

#### **Clause 10 – Data definitions**

44. This clause contains definitions for key data-related terms used throughout the Bill, grouped together to assist readers to find and understand these concepts.
45. Subclause (1) defines ‘scheme data’ to mean public sector data and outputs that have been shared and created through the data sharing scheme, and which are protected by its safeguards and controls. Only data scheme entities may hold or have access to scheme data.
46. Subclause (2) defines ‘public sector data.’ This definition establishes the scope of government data that can be shared under the data sharing scheme. The term includes data that is collected, created, or held by a Commonwealth body, or on its behalf. Public sector data includes ‘personal

information' and 'sensitive information', as defined by the *Privacy Act*, as well as other types of data. Data created or enhanced by an accredited data service provider (ADSP) on behalf of a data custodian (refer clause 11(4)(b)) would also fall within this definition.

47. Subclause (3) defines 'ADSP-enhanced data' to mean results or products generated by an ADSP in the course of providing data services on behalf of a data custodian in relation to public sector data. For instance, where an ADSP integrates several datasets on behalf of a custodian to provide to an accredited user, the integrated dataset is 'ADSP-enhanced data'. This includes where the ADSP integrates public and non-public sector data on behalf of a data custodian, relying on the data custodian's legal authority to collect and use both datasets. In this circumstance, the integrated dataset is also 'public sector data' as it is data created on behalf of the Commonwealth (the data custodian).
48. Subclause (4) defines 'output.' This definition establishes what is considered under the outputs principle (refer clause 16(5)). The term 'output' means data that is the result or product of sharing authorised under Chapter 2 that is generated by an accredited user. This is an inclusive term to cover a range of results and products that incorporate or are founded upon the shared data such as an integrated dataset, tables or graphs of statistical information, an algorithm, a pre-filled form compiled using shared data, and a research paper or policy proposal. Outputs are subject to ongoing controls under the data sharing scheme, unless they exit the data sharing scheme under clause 20.
49. Subclause (5) sets out the definition of 'data.' This broad definition is intended to capture all forms of data and information, including copies of original data. This definition aligns with State data sharing legislation to promote consistency between related schemes. Data shared or created under this Bill may be a record for the purposes of the *Archives Act 1983*, and if so must be handled in accordance with that Act.

#### **Clause 11 – Entity definitions**

50. This clause identifies and defines the key roles entities have in the data sharing scheme. This clause is necessary to identify participants in the data sharing scheme and, accordingly, the extent of the Commissioner's regulatory powers.
51. Subclause (1) defines the term 'data scheme entities' to mean data custodians of public sector data and accredited entities, defined respectively in subclauses (2) and (3).
52. Subclause (2) defines which entities are considered data custodians for the purpose of the data sharing scheme. Data custodians are Commonwealth bodies (refer clause 9 definition) that control and have the right to deal with particular public sector data, and are not excluded entities under subclause (3).
53. In accordance with subclause (2)(a), the custodian must control the data itself, or through another body acting on its behalf. Physical possession (for instance, paper-based data stored on site) is sufficient but is not required. This reflects the reality of data management, as data may be collected and stored remotely or in electronic form, including cloud storage, in accordance with the conditions set by its custodian.
54. A right to deal with data in subclauses (2)(b) is a broad concept, encompassing the power to collect and handle that particular data for the entity's functions or activities. Such rights typically derive from legislation or contract, but may also be reflected in other arrangements like Memoranda of Understanding. A right to deal with data does not amount to ownership.
55. Subclause (2)(b)(i) recognises rights arising outside of this scheme, for instance under portfolio legislation, while subclause (2)(b)(ii) allows custodial rights to arise with respect to scheme data created by accredited entities that are Commonwealth bodies.



56. Subclause (2)(b)(ii) works with clause 18(1) (item 4) to allow a data sharing agreement to designate one of the (Commonwealth) parties as data custodian of any outputs or ADSP-enhanced data generated under the agreement. This approach is consistent with how custodians' rights may arise outside of the data sharing scheme, and provides flexibility so parties can set and streamline their sharing arrangements in a manner that does not compromise the original custodian's control.
57. Certain Commonwealth bodies are excluded from being data custodians for the purposes of this scheme, as provided by subclause (2)(c) and listed in subclause (3).
58. Subclause (3) lists entities that are excluded from the scheme. Excluded entities cannot be data custodians, and are unable to seek accreditation. As excluded entities are not data scheme entities, they are not able to use the authorisations and are not subject to the responsibilities and regulatory provisions of this Bill. Intelligence entities are excluded to preserve existing arrangements and frameworks that authorise and regulate their activities. Oversight agencies such as the Commonwealth Ombudsman and the Australian National Audit Office are excluded as they have oversight of the government and the Commissioner's activities under this Bill. Data originating with, held by or received from excluded entities may not be shared under this Bill (refer clause 17(2)(a)).
59. In most cases, the entity that collects data to fulfil its legislative functions or purposes (typically a Commonwealth department or agency) will be the custodian of that data.
60. The definition of data custodian must be read with clause 13(1) and clause 17, which qualify custodians' capacity to share data under this scheme. In particular, sharing must be in accordance with existing arrangements relating to the data, and have the agreement of all relevant custodians. Where multiple entities are authorised to collect and handle the data, such as where different departments use the same data for different functions, they should resolve custodianship prior to entering a data sharing agreement.
61. Subclause (4) defines accredited entities. The term 'accredited entity' refers to two kinds of data scheme entities: users and data service providers that are accredited under the accreditation framework (refer clause 74).
62. Accredited entities are authorised to collect and use data shared with them under clause 13, within the parameters set by their data sharing agreement (refer clause 18) and this Chapter.
63. Accredited users are entities that are capable of securely handling data shared with them under this scheme. Accreditation of users could occur at an agency or organisation level, as well as individuals within such bodies. These matters will be settled in the accreditation framework established in the rules (refer clause 74).
64. Accredited data service providers (ADSPs) are intermediaries in the sharing process that provide services which support sharing by data custodians with accredited users. ADSPs act on behalf of data custodians, as their agent. ADSPs play a crucial role in the scheme to fill gaps in resourcing and capability that would otherwise inhibit data availability and use.
65. A broad range of entities may apply for accreditation, consistent with the clause 9 definition of 'entity' – other than excluded entities (refer clause 11(3) and clause 73(1)(a)).
66. To become accredited, applicants are assessed by the National Data Commissioner to ensure they have appropriate capabilities to participate in the data sharing scheme. A single entity can have multiple roles: an entity may be accredited as both user and data service provider – and may also be a data custodian. A data custodian *must* be accredited as an accredited user to collect and use data under this scheme, including its own data. In such cases, it must be clear in which capacity the entity is acting, both in practical terms and on the face of the data sharing agreement (refer

clause 18). This is important where a data custodian is also acting as an accredited entity within the same sharing project.

## **Chapter 2 – Authorisation to share data**

- 67. Chapter 2 of the Bill authorises data custodians to share public sector data with accredited users in permitted circumstances. Authorisation to share is subject to the controls set in this Chapter.
- 68. Within the circumstances of clause 8, data custodians may share public sector data with accredited users in accordance with the controls established by this Part. Key requirements are specified in clause 13, and expanded upon in subsequent clauses. Where these requirements are met, this Bill overrides other laws to the extent that they restrict sharing, except for situations and laws prescribed by clause 17.
- 69. Data custodians have discretion whether to use this authorisation to share public sector data; there is no duty to share, and other pathways for sharing data continue to operate.
- 70. Data scheme entities must comply with legislative instruments (refer clause 25), and have regard to the Commissioner's guidelines (refer clause 26) when engaging with the data sharing scheme.

### **Clause 12 – Simplified outline of this Chapter**

- 71. This clause provides a simplified outline of the authorisation provisions of Chapter 2 of the Bill. This simplified outline is intended to assist readers to understand the substantive provisions of the Chapter, but is not comprehensive. Readers should rely on the substantive provisions.

### **Clause 13 – Authorisations to share data**

- 72. This clause enables data scheme entities to share public sector data by providing authorisations and requirements for each component of the sharing process.
- 73. Specifically, this clause authorises data custodians to provide, and accredited entities to obtain access to, public sector data in a controlled manner that meets the requirements of the subclauses. These requirements apply in all sharing situations, including where sharing involves one or more datasets, data custodians, and/or accredited entities.
- 74. In short, sharing is authorised where it is for a permitted purpose, safeguards to manage risk and ensure custodian oversight are in place, and the terms of sharing are set out in a data sharing agreement. These requirements are provided at a high level in subclauses 13(1) and (3), and detailed in later clauses in Chapter 2.
- 75. Subclause (1) authorises data custodians to provide controlled access to public sector data to accredited users, directly or through an ADSP. Paragraphs (a) to (d) set out high-level requirements that must be satisfied in order for sharing to be authorised.
- 76. Paragraph (a) contains several elements. The sharing purpose must be a permitted purpose and not a precluded purpose (refer clause 15), and only data that is reasonably necessary for the purpose in (a) may be shared (a concept known as 'data minimisation').
- 77. The 'data minimisation' requirement in paragraph (a) applies to the total amount of data shared as well as the type of data involved. If a small amount of data would meet the user's needs, no more than that should be shared. However, a large amount may be justifiably required, such as to identify national trends that inform policy or to input into service delivery systems. Similarly, sharing a certain amount of identifiable data, like street addresses, may be reasonably necessary to pre-fill government forms or to create an integrated dataset for use by researchers. What is reasonably necessary and proportionate to the purpose of sharing will be determined on a case-by-case basis by the data custodian, as the entity with the best knowledge of the data involved.

The custodian may also consider data minimisation, and apply any other treatments and other protections to control risks associated with sharing, under the Data Principle in clause 16.

78. Paragraphs (b), (c) and (d) ensure that sharing is in accordance with the data sharing principles and a valid data sharing agreement (refer clauses 16 and 18), and is not otherwise excluded by clause 17.
79. Paragraph (e) provides additional rules for sharing a dataset that has multiple data custodians. Each custodian must authorise the sharing, either individually in the data sharing agreement, or by authorising one to act on the others' behalf for the purposes of this Bill (whether on a one-off or an enduring basis). In the latter case, evidence of that authority to act must be attached to the data sharing agreement made by the authorised custodian. This approach enables a streamlined approach to reduce red tape, at custodians' discretion, while ensuring custodians retain oversight of their data.
80. Subclause (2) clarifies that the requirements of subclause (1) apply to both stages of sharing where an ADSP is involved.
81. In practice, this means the terms of sharing must be consistent with the purpose test and data sharing principles, and articulated in the data sharing agreement, for the first stage where the data custodian shares to the ADSP as well as the second stage where the ADSP makes data available to the accredited user.
82. While both stages of sharing will be for the same overall purpose, different controls may be placed under the data sharing principles to reflect differences in context and risks in each stage. For instance, a data custodian may engage an ADSP to provide an accredited user with secure access to data for research purposes. Controls for the transfer of data to the ADSP would differ from the controls to manage the risks and conditions of the ADSP providing access to users. This is also the case where the ADSP transforms the data it receives from the custodian prior to providing access to the user, such as by integrating multiple datasets from the custodian together into a single asset, or creating an extract so the user only accesses a subset of the larger dataset provided to the ADSP. The data sharing agreement must set out parties' responsibilities and safeguards for each stage of the sharing.
83. Importantly, the drafting of this clause means only custodians are authorised to share, and data must always be made available to at least one accredited user. If a data custodian intends to receive data through a sharing project it must do so as an accredited entity, as identified in the data sharing agreement.
84. Subclause (3) authorises accredited entities to collect and use public sector data that is shared with or through them under subclause (1) – where consistent with the purpose test, data sharing principles, and the terms agreed by the data custodian. 'Use' has its ordinary meaning here, which in the context of this scheme could cover all forms of handling data such as analysing data, as well as sharing or release within the limited circumstances of clause 20.
85. Data integration may also be an authorised use of public sector data under subclause (3). As the Bill provides authority for the integration of public sector data, separate legal authority is also needed to support integration with any non-public sector data under a data sharing agreement. Refer also clause 10(3) definition of 'ADSP enhanced data'.
86. Subclause (3) operates as an authorised legislative exception to the prohibitions on collecting, using, and disclosing personal information where sharing is related to the entities' functions and activities in Australian Privacy Principles 3 and 6 in Schedule 1 of the *Privacy Act*.
87. Subclause (3)(b) provides that an accredited entity is not authorised to collect and use public sector data while its accreditation is suspended. Refer to Part 5.2 for provisions on accreditation.

**Clause 14 – Sharing must be authorised**

88. Under this clause, a person may be liable for a civil penalty or a criminal offence for sharing data in an unauthorised manner. This clause aims to deter non-compliance and build confidence in the scheme, without discouraging participation. It does not impose retrospective liability.
89. This Bill provides limited statutory authority to override non-disclosure provisions in other laws that prevent sharing, where the requirements of Chapter 2 are met (refer clauses 13 and 22). If these requirements are not met, sharing is not authorised by this Bill and the situation ‘rebounds’ so the protections and penalties of the non-disclosure laws apply.
90. The penalties and offences in this clause are designed to capture instances of unauthorised sharing where there are no applicable penalties to which the conduct can rebound. This approach ensures there are always protections for data shared or created under this scheme. For example, the Bill may be used to share and integrate data to create an enriched dataset that is more sensitive than the individual source datasets. The penalties in this clause provide gap coverage where there are no existing penalties for unauthorised sharing, collection, or use of the individual source datasets.
91. Where appropriate, penalties may be sought under this clause rather than under other laws through operation of the rebound approach. In this case, standard processes such as those in section 4C(1) of the *Crimes Act 1914* will apply to manage situations where the same conduct could be prosecuted under multiple Commonwealth laws. Where conduct may attract a civil penalty or criminal offence (under clause 14 or another ‘rebound’ provision), sections 88-90 of the *Regulatory Powers Act* will apply to any proceedings, penalty orders and convictions.
92. Subclauses (1) and (2) apply to unauthorised sharing. While these provisions are expressed to apply to persons, they must be read in conjunction with part 6.3 (treatment of certain entities) as individuals’ conduct may be attributed to the data scheme entity for which they act.
93. Subclause (1) provides for a civil penalty where a person relies, or purports to rely, on the authorisation to share in clause 13(1) but the sharing is not authorised. This could occur in a range of circumstances, such as if a person shares public sector data with non-accredited recipients, or for a precluded purpose (refer clause 15). It could also occur where a person’s right to share particular data is qualified by a pre-existing agreement between their employer and another entity, and the sharing contravenes that earlier agreement (refer clause 17). The phrase ‘purportedly relies on’ relates to use of a data sharing agreement to facilitate the sharing transaction, as data sharing agreements must specify that sharing occurs under this Bill and in accordance with its requirements (refer clause 18(1) item 2).
94. Subclause (2) creates a criminal offence for the same circumstances as (1): the person shared public sector data under or purportedly under this Bill, in a manner that resulted in the sharing being unauthorised.
95. Each element of the offence is set out in paragraphs (2)(a) to (c), relying on default fault elements from the *Criminal Code*. This is consistent with the *Guide to Framing Commonwealth Offences* (para 2.2.4). Paragraphs (a) and (b) establish conduct elements of the offence, the relevant fault element being intention. Paragraph (c) specifies recklessness as the fault element as this paragraph relates to the circumstances or results of the conduct.
96. Subclauses (3) and (4) are directed towards persons who collect and use data in an unauthorised way but must be read in conjunction with part 6.3 (treatment of certain entities). As with subclauses (1) and (2), the rebound approach applies in practice here.
97. Subclauses (5) and (6) clarify that the civil penalty and criminal offence for unauthorised collection and use apply irrespective of other laws.

98. The effect of subclause (5) is that contravention of the Bill may be established even if other legislation authorises that conduct. This clause prevents current and future laws affecting the operation and scope of the Bill. In particular, it prevents another law from expanding the permitted purposes for sharing in clause 15. Subclause (5) works in conjunction with clause 22, which provides for a limited override of other non-disclosure laws to enable sharing. Together, these provisions establish and protect the operation and scope of the DAT Bill despite any contrary laws, existing or future.
99. Subclause (6) prevents persons from using (which includes sharing) the data in any of the permitted general or health situations set out in sections 16A and 16B of the *Privacy Act*. Intent is to prevent persons from using sections 16A or 16B to circumvent this Bill's prohibition on sharing data for enforcement and national security purposes (refer clause 15(2)-(3)). Pathways for sharing data in exceptional circumstances such as sections 16A and 16B of the *Privacy Act* will continue to operate outside the data sharing scheme.
100. Subclause (7) clarifies that a person will not contravene clause 14 where the disclosure of scheme data was authorised by clause 121. A defendant will bear an evidential burden to raise evidence that suggests a reasonable possibility their disclosure was authorised by clause 121. This burden is justified as the evidence required would be peculiarly within the defendant's knowledge and not available to the prosecution (see *Guide to Framing Commonwealth Offences* at 4.3.1-2).
101. Similarly, providing controlled access to outputs, or releasing outputs, in accordance with clause 20 will not attract a penalty under clause 14 as this is an authorised use of data for the purposes of clause 13(3).
102. The consequences for breach of a civil penalty or criminal offence provision in this Bill – up to 300 penalty units or up to two years imprisonment, respectively – align with similar laws and the *Guide to Framing Commonwealth Offences*. Consistent with the Guide, the Bill sets maximum penalties; a court will determine what is appropriate on a case-by-case basis. The maximums set by this clause balance the penalties in more established frameworks, such as the *Privacy Act*, with more contemporary offences for mishandling government and consumer data. This approach is in keeping with the intent for this scheme to align with other applicable frameworks, without duplicating them, as well as with community expectations.
103. Multiple persons may be responsible for a single breach of clause 14. For example, if a data custodian shares data through an ADSP to an accredited user, but the sharing occurs in an unauthorised way, persons who shared the data on behalf of the data custodian and the ADSP may be liable for their actions. A court would determine whether responsibility rests with the individual or the data scheme entity in accordance with part 6.3, and would also determine the extent of each party's liability.
104. Where an individual employed or otherwise associated with an ADSP (refer part 6.3) is involved in unauthorised sharing, the stage of the sharing (refer clause 13(2)) will determine the applicable subclause in clause 14. Where the individual provides unauthorised access to public sector data, subclauses (1) and (2) are relevant; subclauses (3) and (4) may apply where the individual collects or uses data from a data custodian in an unauthorised manner.

### **Clause 15 – Data sharing purposes**

105. Building on clause 13, this clause establishes three purposes for sharing public sector data, and related requirements. For clarity, it also specifies precluded purposes for which sharing is not authorised by this Bill.
106. Subclause (1) provides that public sector data may be shared for delivery of government services, to inform government policy and programs, and for research and development purposes. Sharing may occur for one or more of these purposes.

107. Subclause (1)(a) enables sharing for delivery of government services, meaning government activities that provide coordinated and structured advice, support, and services to those engaging with the government. Data sharing under this purpose could improve design of systems, engagement, and processes involved in delivery of government services, including improving user experiences through simplified or automated systems like pre-filled forms and reminders to submit or verify details like a tax return. This purpose supports sharing for services delivered by or on behalf of government, such as through contractors; it does not extend to services undertaken by non-government enterprises for their own purposes, even if these are in the public interest. Similarly, assurance and compliance activities related to service delivery – such as determining a person’s eligibility for a welfare payment – are not a permitted purpose for data sharing under this Bill, despite being valid activities of government. Refer subclause (3), ‘enforcement related purposes’, however note subclause (4) and clause 20.
108. Sharing to inform design and implementation of government policy and programs is permitted under subclause (1)(b). Both terms should be construed broadly, using their ordinary meaning. For instance, a ‘government policy’ is a rule or principle that guides government decisions, usually related to a specific topic such as education. Similarly, a ‘government program’ refers to an organised system of services, activities, or opportunities to achieve a goal or outcome. Data sharing under this purpose could help enable the discovery of trends and risks to inform policymaking, and provide a holistic understanding of ‘wicked problems.’ Additionally, it could enable modelling of policy and program interventions, program risk analysis and impact measurement, and evaluation of the effectiveness of policies and programs. Outcomes from such sharing could help ensure the government is spending money effectively, and identify program gaps, challenges and successes to inform new or improved initiatives. Data sharing for these purposes will not directly target individuals.
109. Subclause (1)(c) supports sharing for research and development, a term encompassing activities to advance knowledge and contribute to society. Sharing for these purposes will enable accredited academics, scientists, and innovators in the public and private sectors to access public sector data to conduct research.
110. Sharing for purposes that are consistent with clause 15(1) but have other applications may be permissible. For instance, a research project to improve pharmaceutical treatments for heart disease may deliver both profit for the researcher as well as serving the public interest. The mere fact of private sector involvement or profit does not infringe clause 15, provided sharing is for a permitted purpose, is not for a precluded purpose, and is otherwise consistent with this Chapter. In addition, other frameworks controlling anti-commercial or anti-competitive outcomes continue to apply, such as the *Competition and Consumer Act 2010* and the APS Code of Conduct. Refer also to clause 15(4), below.
111. Subclause (2) sets out precluded purposes for sharing under this Bill. If an entity needs to acquire data for such activities, that entity must do so outside of this scheme.
112. Subclause (2)(a) and (b) preclude sharing for enforcement related purposes defined in subclause (3) and for purposes that relate to or prejudice national security, as defined. These activities are best performed and managed under dedicated legislation that provides tailored protections and redress mechanisms to ensure procedural fairness.
113. Subclause (2)(c) precludes sharing for purposes prescribed in rules made by the Minister. This provision enables the Minister to prescribe additional precluded purposes but not permitted purposes. This approach is intended to manage unintended expansions or interpretations of clause 15, and to ensure the scheme continues to operate as intended and in line with community expectations.

114. Subclause (3) defines enforcement related purposes, a term that includes a range of compliance and law enforcement activities. The listed activities include operational activities and investigations that detect and determine an individual's liability for misconduct, as well as subsequent proceedings. While these activities are legitimate functions of Government they are best carried out under dedicated laws. The definition of 'enforcement related purposes' is adapted from the same concept in the *Privacy Act*, and should be interpreted similarly. Subclause (3) should be read with subclause (4).
115. Subclause (4) clarifies that public sector data may be shared under subclause (1) for a permitted purpose that relates generally to compliance and enforcement. For instance, policy and program development in the areas of crime prevention, public safety, and emergency management or planning would be permitted under subclause (1). Using tax data to develop a policy or program to protect the public revenue would likewise be permissible. These examples can be distinguished from data sharing to support police operations, or to identify and punish fraudulent individuals – both of which constitute enforcement related activities for which sharing is precluded by subclause (2).

#### **Clause 16 – Data sharing principles**

116. This clause operates in conjunction with other limitations on sharing to ensure data is only shared where it is appropriate to do so. For clarity, 'sharing' includes providing controlled access to data as well as collecting and using data, consistent with clause 16(7) and the definition in clause 9.
117. This clause establishes the data sharing principles, a key safeguard to manage risks of sharing public sector data based on the internationally recognised five safes framework.
118. Applying the data sharing principles involves considering each principle in context of the other principles, to manage risk holistically. Each sharing arrangement will require different controls or safeguards to be set under each of the principles to manage overall risk.
119. The principles are structured to support custodians to consider risks arising across five key elements of the sharing process: the proposed project, the setting in which data is shared and accessed, and the persons, data and outputs involved. Within each element, controls can be set to manage impacts of strategic, operational, privacy, ethical, and security risks. The principles work together as well as separately: while every principle must be considered, controls may be set under one or all of them as appropriate to mitigate risks overall. This approach ensures the risks of data sharing are managed effectively and holistically, and provides the foundation of data management throughout the sharing process.
120. The Bill takes a principles-based approach in establishing the data sharing principles. This will ensure the principles remain applicable as technology, data management practices, and community expectations evolve over time. The Commissioner may make data codes and guidelines to provide further detail on how to apply the data sharing principles.
121. Subclause (1) establishes the project principle, which addresses the intended purpose or use of sharing the data. The project principle requires consideration of a number of factors to ensure data is only shared for appropriate projects or programs of work. These factors include but are not limited to public interest, ethics, and use of consent and ADSPs. These requirements align with data and ethical principles used by the research sector to improve data management and guide responsible data use.
122. Subclause (1)(a) requires observance of applicable ethics processes. This includes, for example, observance of established academic ethics approval processes, and seeking independent advice on the ethical implications of sharing as appropriate. Use of ethics processes help ensure research and other projects have beneficial results while minimising risk of harm to relevant people, including data subjects.

123. Where the data being shared includes personal information, subclause (1)(b) requires consent for sharing to be sought from the individuals concerned unless it is unreasonable or impracticable for the data scheme entities to do so. The standard of consent required is that set by the *Privacy Act*. The ‘unreasonable or impracticable’ language is drawn from section 16A of that Act, and should be interpreted using relevant guidance on consent made by the Australian Information Commissioner.
124. The question of whether seeking consent is reasonable or impracticable may depend on the amount, nature and sensitivity of the data involved, and whether individuals gave informed consent for uses including the proposed sharing at the point the data was originally collected. Where it is unreasonable or impracticable to seek consent, parties must still consider implementing other controls to protect privacy, under this and other data sharing principles.
125. Subclause (1)(c) requires that data sharing agreements include a description of how the public interest is served by the instance of sharing. This requirement works with the data sharing purposes (clause 15) to ensure that the public interest served by sharing is clearly considered and articulated before entering into data sharing agreements. This information will then be made publicly available via the data sharing agreement register (refer clause 116) to provide additional accountability and oversight.
126. Subclause (1)(d) requires that data custodians consider using ADSPs for data services. This requirement is intended to ensure data custodians consider and manage developing data management capabilities and infrastructure, particularly when sharing requires complex protections. More detailed requirements for use of ADSPs may be set in legislative instruments, including prescribing certain data services for which data custodians must use ADSPs (refer clause 28).
127. Subclause (2) establishes the people principle, which requires data custodians to ensure data is only shared with appropriate recipients. This requirement operates in conjunction with the accreditation framework (refer clause 74). Accreditation provides an assessment of people and entities, and their capability to handle public sector data under the data sharing scheme; the Commissioner may place conditions on an entity’s accreditation to reflect their capacity to handle particular kinds of data.
128. In addition to accreditation, in applying this principle data custodians should consider whether the accredited entity needs to possess particular or additional skills or resources specific to the proposed project or program of work.
129. Subclause (3) establishes the setting principle, which focuses on the setting(s) and manner in which sharing occurs. Data custodians must ensure public sector data is transmitted through and accessed in environments that have sufficient security controls to prevent unauthorised sharing or use of data. The strength of controls applied under this principle will depend on those under other principles, particularly the data principle. For instance, stricter access and security controls may be needed where detailed or identifiable data is shared, compared to aggregate data.
130. Subclause (4) establishes the data principle, which focusses on the nature of the data, and treatments necessary to control risks of sharing it while delivering the data needed to achieve the purpose of sharing. Under the data principle, data custodians consider what data is reasonably necessary to provide to the user in order to achieve the aim of the project - this consideration also ties into the requirement in clause 13(1)(a).
131. Relevant considerations under the data principle include whether to provide an entire dataset or a customised extract of particular variables, and the level of detail of (and any treatments applied to) that data. Particular treatments of data needed to make it suitable for the user are best determined by the data custodian. Treatments may involve statistical methods such as



aggregation, removal of direct identifiers (for example, through de-identification), encryption, as well as transformative methods such as cleaning data, or integrating multiple datasets to create a new comprehensive dataset for analysis. Decisions made under this principle will have regard to controls set under the other principles and the need for data provided to be useful, to achieve the purpose of sharing.

132. Subclause (5) establishes the outputs principle, which ensures the outputs of sharing projects are as agreed by parties in their data sharing agreement (refer clause 18). ‘Outputs’ is a broad term encompassing any product created from the shared data by the user (refer clause 10).
133. The reference to outputs being ‘as agreed’ reflects the parties’ joint understanding of the scope and purpose of their sharing project, as articulated in the data sharing agreement. Identifying what the outputs are and how they are to be treated is crucial to ensure data custodians retain control of their data, particularly where the shared data and outputs involve detailed records. For instance, the data custodian may wish to review statistical outputs to ensure accuracy, and may either prohibit or set exact requirements for when the output may exit the data sharing scheme in accordance with clause 20. Parties may amend their data sharing agreement to reflect changes to their intentions for outputs, for instance to add new agreed outputs.
134. Under subclause (6), sharing, collection, and use of data will be consistent with the principles where the data scheme entities are satisfied that the controls set across the principles work together to effectively manage risk. While both parties determine and agree to the controls in the data sharing agreement, the data custodian’s satisfaction would be particularly influential given their knowledge of and custodian responsibilities over the data. Once controls are set, both sharer and recipient(s) may be responsible for implementing these controls, as identified in their data sharing agreement under clause 18.
135. Subclause (7) clarifies that a reference to ‘sharing’ in this clause covers all aspects of that process authorised by clause 13, including provision of controlled access to data under clause 13(1) as well as collection and use of data under clause 13(3).
136. The terms governing the controls set in a data sharing agreement will be published (refer clause 116) to ensure there is transparency of entities’ data management and adherence to agreed safeguards.

#### **Clause 17 – When sharing is excluded from the data sharing scheme**

137. This clause works in conjunction with other limitations on sharing to ensure data is not authorised to be shared under clause 13(1) where it would be inappropriate to do so.
138. Subclause (2) excludes sharing in circumstances relating to national security and law enforcement. Subclause (2)(a) provides data held by, originating with, or otherwise received from an excluded entity (refer clause 11(3)) cannot be shared under this Bill. This includes summaries and extracts of such data, consistent with section 7(2A) of the *FOI Act* on which this clause is modelled. This subclause works in conjunction with clause 11(3) to carve out intelligence agencies and certain other entities, and their data, from the scheme.
139. Subclause (2)(b) lists agencies whose operational data cannot be shared under the scheme. This Bill does not define ‘operational data’, as decisions about whether data is operational or not are best made on a case-by-case basis by the agencies listed in this subclause. Where a listed agency has multiple functions, operational data relating to its intelligence and enforcement functions should be distinguished from data relevant to other functions, as only the former is excluded from sharing. For instance, the Department of Home Affairs (refer paragraph (b)(ii)) has a range of functions including immigration, intelligence, and enforcement functions. For the purposes of this clause, data relating to its intelligence and enforcement functions (performed by the Australian Border Force) is taken to be ‘operational data’ and is excluded

from sharing under this scheme. Unless it is sensitive intelligence data, immigration data, such as data on visas, is not considered operational data for the purposes of this clause, so is not excluded from this scheme. The agencies specified in this subclause may otherwise share, collect, and use non-operational data under this scheme.

140. Subclause (3) protects existing arrangements relating to data that is within the control of a data custodian and could otherwise be shared under this scheme.
141. Subclause (3)(a)(i) excludes the sharing of data that is subject to copyright or intellectual property rights, unless the rights holder agrees to the sharing. If the rights holder has agreed, those rights would not be infringed and the proposed sharing can proceed under clause 13(1).
142. Subclause (3)(a)(ii) excludes sharing where the data custodian is party to a contract or other agreement outside the scheme, such as a Memorandum of Understanding, which would be infringed by the proposed sharing. This means a data custodian cannot use this scheme to share information it has received under another arrangement unless that arrangement allows it. This provision interacts with clause 13(1)(d), which requires that, if there are other custodians of the data, they all must agree for the proposed sharing to be authorised by this Bill.
143. Subclause (3)(a)(iii) and (iv) exclude sharing that is contrary to a common law duty, such as a duty of confidence, or a privilege such as legal professional privilege or Parliamentary privilege.
144. Subclause (3)(b) excludes sharing where the concerned data is commercial information and sharing that data would found an action for breach of a contractual or equitable obligation of confidence. This provision relies on existing legal tests for establishing a breach of confidence, and aligns with language used in section 45 of the *FOI Act*.
145. The threshold in subclause (3)(b) is where the sharing would found an action for breach of confidence brought by a person other than the Commonwealth. This threshold is intended to protect commercial-in-confidence information broadly, rather than only commercial information that would likely be detrimental to the public interest if shared. This is the relevant threshold for action brought by the Commonwealth, see *Commonwealth v Fairfax* (1980) 147 CLR 39 at 51.
146. Note that subclause (3)(b) does not exclude sharing of commercially sensitive information where there is no duty of confidence attached, provided risks of sharing such data can be managed through application of the data sharing principles (refer clause 16).
147. Subclause (4) excludes sharing that contravenes the regulations made under this Bill.
148. Subclause (4)(a) means sharing is not authorised where it would breach a specific legislative provision that prohibits the data custodian, or persons it acts through (refer clause 109), from disclosing the data, and is listed in the regulations. This approach recognises there are circumstances where certain secrecy or non-disclosure provisions should not be overridden by clause 22, for instance where they protect highly sensitive data collected by the Commonwealth. Some of the listed provisions complement the exclusion in subclause (2)(a) to make it abundantly clear that protections around national security and law enforcement data remain in place. Listing these provisions in regulations gives flexibility to add or remove provisions in response to need, while still being a disallowable instrument that is subject to Parliamentary scrutiny.
149. Subclause (4)(b) excludes entities listed in the regulations from participating in data sharing under the scheme as data custodians. Such restrictions may be necessary to respond to risks presented by their participation, or to exclude an entity from the scheme as a data custodian without affecting its participation as an accredited entity.
150. Subclause (4)(c) provides scope for the regulations to prevent sharing in other circumstances, to cater for future needs.

151. Subclause (5) ensures Australia's international commitments are upheld, including those arising under bi- or multi- lateral agreements. It also ensures that where the Australian Government has collected data from a foreign government, that data cannot be shared through this scheme unless the foreign government has agreed to the sharing.
152. Subclause (6) excludes sharing of data that could prejudice judicial proceedings and other inquiries, or compromise efficacy of orders. Under subclause (6)(a) custodians are not authorised to share data that is being held as evidence before a court, or data is that evidence acquired by a body described in subclause (6)(b) in exercising their powers of inquiry. Data 'held' as evidence means only the copy of the data that has been tendered in court proceedings and marked as evidence is excluded from sharing. Similarly, only a copy of the data specifically obtained by a court or other body through an exercise of powers described in subclause (6)(b) cannot be shared; the exclusion is not intended to prevent sharing and use of other copies of the same data.
153. Subclause (6)(c)(i) excludes sharing of data that is subject to certain orders made by a court or tribunal (defined in clause 9), such as a warrant containing a non-disclosure requirement. Similarly, subclause (6)(c)(ii) excludes sharing of data about the existence or content of orders referred to in subclause (6)(c)(i) where there is a Commonwealth law that limits or prevents a person from disclosing such information.
154. Subclause (7) excludes sharing where the Commissioner has suspended the accreditation of an accredited user or ADSP. In this case, the entity retains its status as a data scheme entity, meaning it continues to be subject to the requirements and regulatory provisions of this scheme. Sharing activities with or by an entity with suspended accreditation could attract penalty for unauthorised sharing under clause 14.
155. Subclause (8) excludes the Commissioner or a member of the Commissioner's staff (refer clause 46) from engaging in this scheme as data scheme entities. This measure is intended to preserve the independence of the Commissioner and to avoid actual and perceived conflicts of interest.

#### **Clause 18 – Data sharing agreement**

156. Data sharing agreements set out the terms and conditions for projects under the data sharing scheme. This clause establishes the formal requirements for data sharing agreements and their mandatory terms.
157. To ensure consistent practice and transparent sharing activities, all data sharing agreements must be in a written form approved by the Commissioner and contain clauses giving effect to the mandatory terms prescribed in the table in subclause 18(1). The Commissioner may also require use of a template and may allow use of other forms in order to support the transition of existing sharing arrangements to the data sharing scheme.
158. The Minister may set additional terms in rules to allow the scheme to evolve, for instance to cater for changes in technology or data management that should be reflected in terms of data sharing agreements.
159. Subclause (1) requires data sharing agreements to be made by authorised officers of the data scheme entities (refer clause 123). This approach provides security for data scheme entities, as only persons with sufficient authority to act on their behalf can commit them to sharing arrangements, while preserving their autonomy to arrange delegations and terms of sharing. Refer also part 6.3, treatment of certain entities.
160. The table in subclause (1) sets out terms that data sharing agreements must contain to ensure necessary information is agreed and recorded prior to sharing data (the mandatory terms). These terms are standard inclusions in other existing data sharing arrangements and contracts, and support robust and accountable sharing practices. To support accountability and transparency,

mandatory terms of data sharing agreements made under the data sharing scheme will be included in a publicly available register (refer clause 116).

161. Each agreement must include basic information such as the parties to the agreement (item 1). At minimum, the data custodian and accredited user must be identified, as well as any ADSPs involved. There is also scope for funding partners to be listed as parties to the agreement to recognise their interest in the arrangement, in accordance with subclause 18(3) which allows for the addition of bespoke terms.
162. Item 1 also requires parties to identify role/s they will perform under the agreement (i.e. data custodian and/or a type of accredited entity). This information is necessary to inform other terms that set out the obligations of the parties to the agreement by reference to their role/s in the sharing. Similarly, the agreement must identify the data that is covered by the agreement (item 3). Subclause (2) clarifies that data covered by the agreement includes all public sector data to be shared by the data custodian and any ADSPs, and outputs that are expected to be created or derived from it by accredited users.
163. Item 2 requires agreements to specify that sharing is to be done under this Bill. This makes intent to use the data sharing scheme clear on the face of the agreement, as necessary for the operation of the Bill's penalty provisions (refer clause 14). Item 2 interacts with item 5, which requires parties to identify other applicable laws, such as those authorising the initial collection of the public sector data to be shared, and any secrecy or non-disclosure provisions to be overridden by the operation of this Bill. These items ensure parties are aware of their legal responsibilities and liabilities in relation to sharing the data.
164. Under item 4, the agreement must identify which entity is the custodian for the scheme data covered by the agreement (refer clauses 10 and 18(2)) to ensure the chain of custody continues and the custodian's right to share the data is apparent to all parties.
165. Items 6 and 7 require parties to explain how sharing complies with key requirements of the authorisation to share in clause 13. In particular, the agreement must identify which of the permitted purposes for sharing apply (item 6), and detail how the data scheme entities will apply controls to manage risks under the data sharing principles (item 7). Similarly, to satisfy item 11, parties must set out what actions will be taken to respond to and mitigate data breaches, in accordance with their responsibilities in part 3.3.
166. Where an ADSP is involved in the sharing, the agreement must specify the services the ADSP has been engaged to provide, and any limitations on its activities (item 8). For instance, if the ADSP is engaged to provide secure access to data for accredited users, this should be reflected in the relevant data sharing agreement. The agreement should also identify specific users (or classes of users), and any conditions placed by the data custodian on the data that can be made available to them. The ADSP must adhere to these conditions: it only acts on behalf of the data custodian, and is unable to use or share data other than in accordance with the terms of the data sharing agreement, and may not release data. This limitation preserves the role of ADSPs as an intermediary in the sharing process.
167. Items 9 and 10 require that outputs may only exit the scheme or be released as agreed in accordance with clause 20. Other sharing or release of outputs must be prohibited.
168. Under item 9, data sharing agreements must either prohibit an accredited user from sharing the output in any circumstance, or allow the output to be shared in specified circumstances in accordance with the requirements in clause 20(1). In the latter case, the circumstances in which an accredited user may share the output are restricted to one of the three situations described in clause 20(1)(b).

- 169. Item 10 is drafted similarly to item 9 with respect to release. It requires agreements to either: prohibit release of outputs by an accredited user, or allow an accredited user to release outputs in circumstances agreed to by the custodian that meet the requirements in clause 20(3).
- 170. Data sharing agreements may be varied, for instance to include additional accredited users, outputs, or dimensions to a sharing project within the parameters of Chapter 2. Items 12 and 13 require that agreements specify their duration or review arrangements, and how variation and termination is to be managed. Copies of data sharing agreements, including variations, must be given to the Commissioner (refer clause 32).
- 171. Item 14 requires the parties to detail how scheme data covered by the agreement will be dealt with when the agreement ends. Parties may also include information to comply with their record management obligations under other regimes such as the *Archives Act 1983* and Australian Privacy Principle 11.2.
- 172. Subclause (2) defines ‘data covered by a data sharing agreement’ for the purposes of the table in subclause (1).
- 173. Subclause (3) provides that data sharing agreements may cover matters in addition to those itemised in the table. This approach enables parties to tailor agreements to their specific circumstances and to cover other matters which may be relevant, such as handling of freedom of information requests relating to the shared data. Note the requirements of the data sharing scheme and the Commissioner’s regulatory oversight apply only to the content of items required by this clause and those prescribed in rules.

#### **Clause 19 – Compliance with mandatory terms of data sharing agreement**

- 174. This clause establishes a civil penalty for data scheme entities failing to comply with the mandatory terms of data sharing agreements to which it is a party. Compliance with matters set out in mandatory terms of data sharing agreements is essential to ensure public sector data shared is appropriately protected and in alignment with requirements of the data sharing scheme.
- 175. While data sharing agreements bear a resemblance to contracts, their legal nature will depend on the type of entities party to the arrangement (i.e. government or non-government). This clause is designed to ensure all data scheme entities have a statutory obligation to comply with the mandatory terms of data sharing agreements, while creating consequences for parties that fail to do so.
- 176. This penalty is unique to the data sharing scheme so does not rebound back to other legislation (refer clause 14).
- 177. The consequences for breach of this clause (up to 300 penalty units) align with analogous laws and the *Guide to Framing Commonwealth Offences*. Consistent with the *Guide*, the Bill sets maximum penalties; a court will determine what is appropriate on a case-by-case basis. The maximums set balance the penalties of older frameworks, such as the *Privacy Act*, with more contemporary penalties for mishandling government and consumer data. This approach is in keeping with intent for this scheme to align with other applicable frameworks, without duplicating them, as well as with community expectations.

#### **Clause 20 – Exit from data sharing scheme of shared or released output**

- 178. This clause establishes the limited circumstances under which an output may exit the scheme as an authorised use of outputs under clause 13(3). Following the process established in this clause, an output may ‘exit’ the scheme and is no longer ‘scheme data’ (refer clause 10) regulated by this Bill.

## Explanatory Memorandum: Data Availability and Transparency Bill 2020

179. Subclause (1) enables an accredited user to provide individuals and businesses with outputs containing data about themselves to check the data is accurate by validating or correcting it (or in other circumstances prescribed in the rules and within the scope of this Bill).
180. Before the accredited user provides access, the data custodian must have first determined that doing so is consistent with the purpose test and data sharing principles, and articulated this in the data sharing agreement (refer clauses 13(3) and 18(1) item 9). For clarity, the relevant data custodian is the custodian of the shared data from which the output was created, irrespective of other arrangements for custody of the output itself (refer clause 11(2)(b)(ii) and clause 18(1) item 4).
181. The exit mechanism in subclause (1) is intended to support the use of outputs created for permitted purposes in clause 15 – particularly government service delivery for which accurate, up-to-date information is essential. This clause supports pre-filling forms (to be validated by the individual or business) and a single point-of-contact to engage with multiple government agencies. The focus of subclause (1)(b) on individuals' and businesses' control and active validation of their data is consistent with the privacy-positive approach of this Bill, and supports a user-centric model of service delivery.
182. Where the output relates to an individual, the accredited user may alternatively provide access to the individual's responsible person (e.g. parent or guardian), within the meaning of the *Privacy Act*, for validation or correction (refer subclause (1)(b)(ii)). This approach maintains processes and safeguards in existing frameworks to facilitate efficient government service delivery, while ensuring personal information is not provided in a manner that jeopardises the safety or welfare of the individual.
183. Other circumstances or requirements for exit may be prescribed in rules, per subclause (1)(b)(iii), to ensure the Bill can respond to future needs while maintaining data custodian oversight of the process through subclause (1)(a). Any rules created under this subclause must be consistent with the Bill, including the permitted and precluded purposes (refer clause 15).
184. Subclause (2) clarifies the point at which an output exits the data sharing scheme, and ceases to be regulated by the Bill. To ensure consistency, the conditions under which exit can occur are set in the Bill or rules, rather than data sharing agreements.
185. Under subclause (2)(a) outputs that exit under subclause (1)(b)(i) or (ii) cease to be regulated by this scheme at the point the individual or business corrects or validates their data. Data cannot exit the scheme under subclause (1)(b)(i) or (ii) in the absence of a positive act of validation or correction.
186. Once the output has exited the Bill's protections, the individual or business may use their validated information as they see fit. The individual or business may choose to provide their data to an entity to collect and use in accordance with other laws. The protections and obligations of those other laws, which may include the *Privacy Act* or social security laws, would then apply.
187. Under subclause (2)(b) outputs that exit under subclause (1)(b)(iii) will exit at the point in time specified in the rules.
188. Subclauses (3) and (4) facilitate release of outputs from the scheme, such as highly aggregated research outputs. While exit is an authorised use of scheme data under clause 13, these subclauses do not create a new authorisation to release data. Instead, as provided by subclause (3), entities must rely on release mechanisms in other legislative and policy frameworks, which are not affected by the operation of this Bill (refer clause 21).
189. Entities' intent to either prohibit release or allow it in circumstances within the scope of clause 20 must be articulated in their data sharing agreement, refer clause 18(1) item 10. This means an

accredited user cannot unilaterally decide to release outputs under this Bill, as custodian agreement is required.

190. In accordance with subclause (4), an output exits the scheme and is no longer scheme data at the time it is released. The released output may be collected and used in accordance with other laws.
191. Providing access to or releasing outputs in a way that is not consistent with clause 20 or any applicable rules may attract penalties for unauthorised sharing or use of data under clause 14.

**Clause 21 – Other authorisations for data custodians not limited**

192. This clause clarifies that the data sharing scheme does not limit other legislative authorities empowering data custodians to share or release public sector data.
193. The authorisation in clause 13 operates as an alternate pathway to share data, for custodians to use at their discretion. Custodians may continue to share and use data, including releasing it, outside of this scheme relying on other legal authorities.
194. Importantly, this scheme does not impact existing authorities to release data in other legislation. If data is shared under clause 13, it may be released by the accredited user if the data custodian indicates agreement in the data sharing agreement and there is legal authority to do so (refer clause 18(1) item 10, and clause 20).

**Clause 22 – Authorisation to share overrides other prohibitions**

195. This Bill provides limited statutory authority to override other Commonwealth, State, and Territory laws that restrict sharing, collection and use of public sector data. Subclauses 22(1) and (2) give effect to the override for each aspect of the sharing process in clause 13: sharing by data custodians under clause 13(1), and collection and use of shared data by accredited entities under clause 13(3).
196. The override is limited in the sense that it only operates where the requirements of clause 13 are met, and operates to the extent necessary to enable sharing authorised by this Bill. This means that sharing that is not, for example, consistent with the data sharing purposes in clause 15 will continue to be subject to existing secrecy and non-disclosure provisions.
197. The override is also limited by clause 17 and the regulations, which prescribe particular entities and legislation that are exempt from this scheme. In the case of prescribed entities, an exemption means they are not authorised to share data through this scheme. In the case of prescribed provisions, an exemption means the provision is not overridden by this clause. For example, the non-disclosure provisions of the *My Health Records Act 2012* are prescribed by the regulations, meaning this Bill does not authorise the sharing of My Health Records data.
198. This clause is only effective against secrecy or non-disclosure provisions, as these provisions present barriers to sharing of public sector data. Separate offence provisions that do not impose secrecy or non-disclosure obligations will continue to apply, as these are necessary for the operation of the Bill's rebound approach (refer clause 14). Provisions relating to data handling and security are also not affected by this clause. For example, requirements relating to the handling and security of personal information under the *Privacy Act's* Australian Privacy Principles will continue to apply to shared data.
199. This clause is effective against laws enacted by the Commonwealth, as well as the States and Territories. The extension to jurisdictional laws is necessary to ensure State and Territory accredited entities can legally collect and use public sector data (i.e. Commonwealth data) to under this scheme. If a State or Territory law ordinarily prevents or restricts collection and/or use of public sector data, the override will remove this barrier to allow the data to be lawfully collected and used by the State or Territory entity. As State and Territory participation in the

scheme is voluntary, the override will only operate on laws in jurisdictions that have chosen to be involved and only to the extent necessary to facilitate collection and use of public sector data.

200. As this clause is an express statutory override, it overcomes secrecy and non-disclosure duties enacted in other legislation, as well as implied statutory duties to keep information confidential, such as in the duty referred to in *Johns v Australian Securities Commission* (1993) 178 CLR 408. While this clause overrides other legislation, clause 17(3)(a)(iii) preserves separate common law duties and obligations relevant to sharing to protect other legitimate interests in the data.
201. The override applies to current as well as future legislation to support longevity of the data sharing scheme, and prevent inadvertent changes to its scope or operation.

### **Clause 23 – No duty to share**

202. This clause emphasises that this Chapter does not require data custodians to share public sector data, or authorise a person to require a custodian to share data. Data custodians are best placed to assess the risks and public interest of sharing data they are responsible for, and so maintain discretion to decide when to share or not share public sector data.
203. While data custodians have no obligation to share public sector data, they should consider reasonable requests for access to their data through this scheme. This clause ensures that custodians follow due process to consider requests that appear appropriate and made in good faith, before accepting or rejecting those requests, without committing custodians to waste resources on frivolous or vexatious requests.
204. This clause interacts with other clauses in this Bill to ensure the National Data Commissioner has oversight of how the data sharing scheme operates. In particular, custodians' decisions to accept or reject sharing requests (and reasoning behind them) will form part of the Commissioner's annual report (refer clause 124). This information may also form the basis for advice to entities or the Minister to improve understanding or operation of the scheme, such as how safeguards may be applied to manage risks of sharing. This approach supports the objects of the Bill to promote availability of public sector data, and to enhance integrity and transparency in sharing public sector data (refer clause 3).

## **Chapter 3 – Responsibilities of data scheme entities**

### **Part 3.1 – Introduction**

205. This part sets out key responsibilities for data scheme entities, including in relation to data breaches, instruments (refer part 6.4), and requirements for review of the decisions made under the Commissioner's regulatory function.
206. Data scheme entities will continue to have responsibilities under other applicable frameworks for information management, in particular the *Privacy Act* and the *Archives Act 1983*, as well as the Protective Security Policy Framework. This Bill operates alongside these schemes.

### **Clause 24 – Simplified outline of this Chapter**

207. This clause provides a simplified outline of Chapter 3 of the Bill, which establishes key data scheme entity responsibilities and instruments, and merits review processes. This simplified outline is included to assist readers to understand the substantive provisions of Chapter 3. As this outline is not intended to be comprehensive, readers should rely on the substantive provisions of Chapter 3.



## Part 3.2 – Responsibilities of data scheme entities

208. This part sets out some key responsibilities for data scheme entities. Civil penalties apply in some cases if these responsibilities are not met. Note that other important responsibilities are set out elsewhere in the Bill – see especially Chapter 2 (Authorisation to share data) clauses 14 and 19.

### Clause 25 – Comply with rules and data codes

209. This clause requires all data scheme entities to comply with the rules and data codes that are made under this Bill (refer part 6.4). Data codes and rules are binding legislative instruments.
210. The Bill and the rules set the parameters and core requirements of the data sharing scheme; data codes shape how entities implement and comply with those requirements. For instance, the rules may flesh out particular elements of the Bill, such as specific criteria for accreditation that address the matters required by clause 74, and a code could set particular considerations to be made when applying particular Data Sharing Principles in clause 16.
211. The Commissioner’s power to make data codes is found in clause 112; the Minister’s power to make rules is in clause 119.

### Clause 26 – Have regard to guidelines

212. Under this clause, data scheme entities must have regard to guidelines issued by the Commissioner under clause 113 when engaging with the data sharing scheme.
213. The Commissioner’s guidelines will explain expectations and best practice for how the data sharing scheme should operate. Requiring entities to have regard to these guidelines is important to build data management capacity and enhance voluntary compliance with this scheme.

### Clause 27 – Privacy coverage

214. Clause 27 ensures personal information shared under this scheme is handled in accordance with privacy obligations to the standard set in the Commonwealth *Privacy Act*. This privacy coverage ensures personal information shared under this Bill is handled properly, and works with part 3.3 to ensure accountability through oversight and redress.
215. All data scheme entities must be subject to the *Privacy Act* or comparable privacy protections. Commonwealth bodies and non-government entities that are APP entities under the *Privacy Act* must comply with their obligations under the *Privacy Act* for their acts and practices relating to personal information under the Bill. Non-government entities and State and Territory government authorities that are not covered by the *Privacy Act* must either become covered by the *Privacy Act* or be covered by their own jurisdiction’s privacy laws (where these exist and are comparable to the *Privacy Act*).
216. Subclause (1) applies to entities that are not already covered by the *Privacy Act* as agencies or organisations (as defined by that Act). It provides two mechanisms for these entities to achieve privacy coverage for acts and practices involving personal information under the data sharing scheme.
217. For the purposes of subclause (1)(a), these entities could use the relevant mechanism of the *Privacy Act* (sections 6E(2), 6EA, and 6F) to become subject to the *Privacy Act*. This clause may apply to non-government entities that are not already organisations under the *Privacy Act* (e.g. many small business operators), and to government authorities based in States and Territories without their own privacy laws (South and Western Australia at the time of drafting).
218. Alternatively, subclause (1)(b) allows State or Territory authorities in jurisdictions with privacy laws to be covered by those laws, where that coverage is equivalent to the *Privacy Act*. To be deemed equivalent, a jurisdictional law must provide for protection of personal information comparable to the Australian Privacy Principles, monitoring of compliance with the law, and a

means of recourse for individuals if their information is handled contrary to the law. This approach is intended to preserve the remit and autonomy of the States and Territories, and their privacy regulators, without diminishing the privacy standards set for personal information by the *Privacy Act*.

- 219. At the time of drafting, New South Wales, Victoria, Queensland, Tasmania, the Australian Capital Territory, and the Northern Territory have privacy laws that may satisfy subclause (1)(b). A State or Territory authority in these jurisdictions may choose to achieve its coverage obligations under subclause (1)(a) or (1)(b).
- 220. Subclause (2) is relevant for accredited entities that are small business operator with obligations as contracted service providers under the *Privacy Act*, by virtue of having a Commonwealth contract outside of this scheme. Without subclause (2), section 7B(2) of the *Privacy Act* would mean the entity is only covered by that Act for its conduct under the Commonwealth contract, but not for other conduct such as participating in the data sharing scheme. Subclause (2) allows those entities to be subject to the *Privacy Act* for their contractual acts and practices as well as for their conduct under this scheme. They may need to achieve privacy coverage under subclause (1).
- 221. Subclause (3) clarifies this Bill does not affect the operation of the *Privacy Act* with respect to data scheme entities that are APP entities (as defined by that Act), except as provided for in subclause (2) and part 3.3. Where such an entity shares personal information covered by the *Privacy Act* through the data sharing scheme, it must continue to comply with its obligations under that Act. This subclause is most relevant to Commonwealth bodies and businesses that are defined by the *Privacy Act* as APP entities, as well as entities that have opted into the operation of that Act.
- 222. Breach notification and mitigation responsibilities are an important element of privacy coverage. These responsibilities are set out in a dedicated part (refer part 3.3).

#### **Clause 28 – Engage ADSP for prescribed data services**

- 223. Clause 28 provides scope for the making of rules that require data custodians to engage an ADSP to perform data services in certain circumstances. For example, such rules may be appropriate where sharing involves complex processes or data, to ensure best practice is followed and robust safeguards are in place.
- 224. This clause builds on the requirement in clause 16(1) for data custodians to consider using ADSPs when assessing the appropriateness of a proposed data sharing project.
- 225. These requirements reinforce the role of ADSPs in filling gaps in resourcing and capability, and the objectives of this Bill to promote better data availability and use.

#### **Clause 29 – Comply with conditions of accreditation**

- 226. The accreditation framework established by the rules (refer clause 74) will set conditions that accredited entities must comply with to maintain their accreditation. Under this clause, an accredited entity may be liable for a civil penalty if it fails to comply with these conditions.
- 227. This is necessary to ensure the data sharing scheme operates as intended, as accreditation is the threshold requirement to ensure an entity is suitable to handle public sector data shared through this scheme.
- 228. The maximum penalty for breach of this clause (300 penalty units) aligns with other civil penalties in this Bill, and is comparable to those in other laws such as the *Privacy Act*. Consistent with the Guide to Framing Commonwealth Offences, the Bill sets maximum penalties and a court will determine what is appropriate in each particular case.

**Clause 30 – Report events and changes in circumstances affecting accreditation to Commissioner**

229. This clause requires accredited entities to report events or changes in their circumstances which affect their accreditation and are prescribed by the rules or a data code. Reports must be made to the National Data Commissioner.
230. As accreditation provides an entry into the scheme, and the information the Commissioner holds can be made available to data custodians (to support consideration of the data sharing principles in clause 16), it is essential that this information is up-to-date.
231. Events or changes that trigger this responsibility would typically relate to the entities' ability to meet ongoing conditions of accreditation, or to perform activities it has been accredited to do under this scheme. For instance if an accredited entity's IT security network is compromised it could impact on its capacity to securely receive and access data through this scheme, and it must notify the Commissioner under this clause.
232. Core accreditation requirements will be established in the accreditation framework (refer clause 74). Other matters relevant to this clause may be established in data codes by the Commissioner, to improve operation of the accreditation framework.

**Clause 31 – Not provide false or misleading information**

233. This clause provides that data scheme entities must not provide false or misleading information to the Commissioner or another data scheme entity when operating in the data sharing scheme.
234. Subclause (1) provides that data scheme entities must not provide false or misleading information to the Commissioner, including where the document or information is false or misleading because of an omission. This is crucial as the Commissioner must have correct information in order to effectively regulate the data sharing scheme, and ensure its safe and effective operation. For example, the Commissioner will need accurate information to assess whether or not an entity is eligible for re-accreditation.
235. Subclause (2) similarly requires that data scheme entities not provide false or misleading information to other data scheme entities for the purposes of entering into or executing data sharing agreements. Accurate information is necessary for data custodians to assess whether data should be shared under the data sharing scheme. Inaccurate information may, for example, lead to inappropriate application of the data sharing principles, leading to data breaches of shared data, or use of data or outputs for precluded purposes.
236. A civil penalty of up to 300 penalty units may apply for breach of this clause. This penalty is specific to this Bill, and does not involve a rebound element like clause 14. Penalties and offences under other legislation may also apply, however, for instance under division 136 or 137 of the *Criminal Code*.
237. The maximum penalty for breach of this clause aligns with other civil penalties in this Bill, and is comparable to those in other laws such as the *Privacy Act*. Consistent with the *Guide to Framing Commonwealth Offences*, the Bill sets maximum penalties and a court will determine what is appropriate in each case.

**Clause 32 – Notify Commissioner in relation to data sharing agreements**

238. Subclause (1) requires a data custodian to provide the National Data Commissioner with a copy of any data sharing agreement (including varied agreements) it enters into. The copy must be provided in an electronic form approved by the Commissioner (to ensure machine readability) within 30 days of making the agreement or variation.
239. This clause provides the Commissioner with oversight of sharing activities necessary for its regulatory function, and promotes transparency as data sharing agreements will be published on

a publicly available register (refer clause 116). The 30-day timeframe provides reasonable time for the custodian to process its agreement while ensuring public accountability.

240. Under subclause (2), a data custodian has 30 days to provide the Commissioner with written notice of the termination of any data sharing agreements to which it was party. This responsibility also supports transparency by allowing the Commissioner to maintain an accurate register of active data sharing agreements.

**Clause 33 – Assist Commissioner as required in preparation of annual report**

241. This clause requires data scheme entities to support the Commissioner to prepare an annual report on the operation of the data sharing scheme.
242. Entities must provide the information and assistance requested by the Commissioner to compile an accurate and comprehensive report, which will address the matters described in clause 124.

**Part 3.3 – Data breach responsibilities**

243. This part sets out data scheme entities' responsibilities with respect to data breaches, building on the requirement for privacy coverage in clause 27.
244. The clauses preserve the Australian Information Commissioner's oversight of breaches involving personal information through a mechanism that engages the notifiable data breach scheme under Part IIIC of the *Privacy Act*.
245. A separate mechanism for reporting serious breaches of non-personal information to the National Data Commissioner is also established, recognising the variety of public sector data that may be shared under the scheme.
246. These responsibilities operate while a data scheme entity holds scheme data.

**Clause 34 – Definition of data breach**

247. This clause defines 'data breach' for the purposes of this Bill. This definition adapts the concept of an 'eligible data breach' in section 26WE of the *Privacy Act* for the purposes and terminology of this scheme, to promote consistency between the frameworks.
248. For the purposes of this Bill, a data breach will have occurred where there is unauthorised sharing, access, or release of scheme data held by a data scheme entity. This definition extends to a loss of data that is likely to result in unauthorised sharing, access, or release; as well as to events prescribed by any applicable data codes.
249. As provided by subclause (a), this clause applies to all data scheme entities that hold scheme data, although it is more likely to apply to accredited entities that have received and created scheme data (i.e. the shared data and outputs derived from it). Data custodians collect and hold their data outside of this scheme; a breach involving such data is not covered by this clause. This clause may, however, apply where a data custodian holds scheme data that was returned to it by an accredited entity pursuant to a direction from the Commissioner (refer clause 98(1)(a)).
250. Intent is that scheme data can only be used as agreed and authorised under Chapter 2, irrespective of permissions in other legislation. To give effect to this intent, subclause (b) provides that a data breach of the entity will have occurred if there is access to, or sharing or release of, the data that is not authorised by this Bill.
251. *Unauthorised access* means access to scheme data by a person who does not have express or delegated authority to do so. This includes access by an employee or contractor of the accredited entity who is not an accredited individual, as well as unauthorised access by a third party such as a hacker.

252. *Unauthorised sharing* describes any sharing that is inconsistent with the authorisation in Chapter 2. For example, deliberate or accidental sharing by an ADSP with an unaccredited user, or an accredited user not specified in the data sharing agreement. This concept would also capture an accredited entity using shared data (scheme data) for a precluded purpose.
253. *Unauthorised release* of scheme data could occur where a user releases an output without agreement from the data custodian in the data sharing agreement (refer clause 18(1) item 10, and clause 20) and there is no legal basis for the user to release that data.
254. Loss of scheme data by a current or former accredited entity will also qualify as a data breach for the purposes of this clause if the loss is likely to result in any unauthorised access to, or sharing or release of, the data. For example, “loss” would cover circumstances in which an employee of an entity accidentally leaves scheme data (including hard copy documents, unsecured computer equipment, or portable storage devices containing the data) on public transport.
255. The concepts of ‘unauthorised access’ and ‘loss’ are consistent with guidance on data breaches from the Australian Information Commissioner (July 2019).
256. Subclause (b) also provides scope for a data code to prescribe a specific event that occurs in relation to the data as an event that qualifies as a data breach of the entity. The Commissioner’s ability to issue data codes on this matter will provide flexibility and help to future-proof the data sharing scheme.
257. Once a data scheme entity reasonably suspects or becomes aware a breach has occurred, the entities involved have mitigation and notification obligations under other clauses in this part.
258. An output that has exited the scheme in accordance with clause 20 is no longer regulated by this Bill; redress for a data breach involving such an output may be sought through the *Privacy Act* or other applicable legislation.

### **Clause 35 – Take steps to mitigate data breach**

259. This clause requires data scheme entities to take reasonable steps to mitigate harm arising from an actual or suspected data breach (refer clause 34).
260. Subclause (1) makes data scheme entities accountable for their actions when a data breach occurs. The responsibility to mitigate harm arises when the entity is aware of an actual breach or reasonably suspects a breach may have occurred. This responsibility arises in circumstances where the breach relates to scheme data held by the entity, or where the entity is otherwise responsible for the breach. For example, a data scheme entity may reasonably suspect a breach if it detects unauthorised access to computer servers upon which scheme data is stored.
261. Data custodians have responsibilities under subclause (1) in addition to the obligations under subclause (2).
262. Subclause (2) requires a data custodian to take reasonable action to mitigate harm where the breach involves data of which they are the custodian. This approach reflects data custodians’ ongoing obligations for data they share under this scheme, the outputs created from such data, as well as for data breaches for which they are directly responsible.
263. Steps taken under subclauses (1) and (2) should be reasonable in the circumstances to mitigate harm to entities, groups of entities, or things arising from the breach. ‘Entity’ is defined in clause 9, and may include an individual, business, or political body. A group of entities could therefore include a community, or bodies corporate. The word ‘thing’ should be interpreted broadly, however should only be interpreted to cover ‘things’ that are capable of experiencing harm such as species, ecosystem, or buildings.

- 264. What steps are ‘reasonable’ will depend on surrounding circumstances, including the severity of the breach, and the resources of the data scheme entity. Notifying affected entities (including other parties to the data sharing agreement) and relevant regulators is a reasonable mitigation step but this alone is not sufficient to mitigate a breach. Entities should take rapid action to regain control of the data to prevent further harm as soon as they become aware of, or reasonably suspect, a breach.
- 265. This responsibility also extends to taking a considered approach to prevent such occurrences in future, such as reviewing and improving data handling processes or security systems, and staff training.
- 266. Where a data breach involves personal information, an entity’s remedial action under this clause may affect its notification obligations under clause 36 and the *Privacy Act*.

**Clause 36 – Interaction with Part IIIC of the *Privacy Act* (notification of eligible data breaches)**

- 267. Where there is a data breach involving personal information shared under this scheme, notification will occur under the Notifiable Data Breach Scheme in Part IIIC of the *Privacy Act*. This clause gives effect to this intent, ensuring a consistent, national approach to regulatory oversight.
- 268. Under subclause (1), default responsibility for notification rests with the data custodian. This is effective as all Commonwealth data custodians are covered by the *Privacy Act* as APP entities (refer clause 27). By bringing all notifications under the federal privacy scheme, this clause caters for different approaches to breach reporting within State and Territory privacy legislation and ensures a redress mechanism is always available.
- 269. Where both the custodian and the accredited entity are APP entities, subclause (2) enables the accredited entity to have responsibility for notification under Part IIIC if this is expressed in the data sharing agreement. This arrangement allows parties to an agreement to decide who has responsibility for notifications: it may remain with the custodian under (1) or may shift to the accredited entity under (2). In both cases, notification is made through the federal privacy scheme, ensuring consistent regulatory oversight.
- 270. Subclause (3) requires the entity with notification responsibilities under subclauses (1) or (2) to give the Commissioner a copy of the statement it provided to the Information Commissioner under section 26WK of the *Privacy Act*. This clause works with clause 37 to ensure the Commissioner has a holistic picture of all data breaches involving scheme data (personal information or otherwise).
- 271. Subclause (4) leverages the *Privacy Act* definition of “hold” to ensure alignment and consistency between the two schemes. This means, for the purposes of this clause, an entity will be taken to hold personal information if it has possession or control of a record that contains the personal information.
- 272. In practice, this clause also interacts with clause 34, which defines ‘data breach’ for the purposes of this scheme, and clause 35, which requires entities to mitigate harm caused by a data breach. Where a data breach within the meaning of clause 34 has occurred and personal information is involved, entities must then determine whether it constitutes an ‘eligible data breach’ (as defined in the *Privacy Act*) as this enlivens notification obligations under the *Privacy Act*. Remedial action taken under clause 35 may affect whether the data breach constitutes an ‘eligible data breach’ for the purposes of the *Privacy Act*.

**Clause 37 – Notify Commissioner of serious non-personal data breach**

273. This clause provides a notification mechanism for data breaches that do not involve personal information within the meaning of the *Privacy Act* (refer clause 37(1)(b)). Intent is to provide the Commissioner with a mechanism to monitor the operation and integrity of the data sharing scheme and the effectiveness of its safeguards.
274. Subclause (1) sets out the criteria that must be satisfied before the obligation to notify the Commissioner is triggered. The intention is that only breaches that are sufficiently serious (refer subclause (2)) should be notified to the Commissioner. The subclause makes provision for an approved form (refer clause 118) to allow streamlining of the notification process in the future.
275. Essentially, an entity must be aware or suspect a breach of scheme data has occurred, the data involved is not personal information (as those breaches are handled under clause 36), and the breach is likely to result in serious harm to entities or things to which the data relates.
276. In terms of ‘serious harm’, subclause (1)(c) requires the data scheme entity to apply a reasonable person test to assess if the breach would likely result in serious harm to an entity, group of entities, or thing. These terms have the same meaning as in clause 35. This paragraph should be read with subclause (2), which adapts section 26WG of the *Privacy Act* to provide a non-exhaustive list of matters a data scheme entity must have regard to when applying the reasonable person test.
277. Subclause (2) lists factors to assist entities to determine what constitutes ‘serious harm’ for the purposes of subclause (1). These factors draw upon the *Privacy Act* (with some modifications to meet the needs of this scheme) to promote the alignment of reporting thresholds for breaches involving personal and non-personal data. Factors include the kind and sensitivity of data involved in the breach, the nature of safeguards protecting the data which were overcome, who has accessed or could access the data, the nature of harm resulting from the breach (such as but not limited to reputational damage, financial loss, or identity theft), as well as other relevant matters in the circumstances.
278. Breaches involving personal information are addressed separately (refer clause 36) to preserve the operation of the notifiable data breaches scheme in Part IIIC of the *Privacy Act*.

**Chapter 4 – National Data Commissioner etc.**

**Part 4.1 – Introduction**

279. This part introduces Chapter 4, summarising its contents and noting that the Commissioner must have regard to the objects of this Bill (refer clause 3).

**Clause 38 – Simplified outline of this Chapter**

280. This clause provides a simplified outline of Chapter 4 of the Bill, which establishes the Commissioner and the National Data Advisory Council.
281. This simplified outline is included to assist readers. As the outline is not intended to be comprehensive, readers should rely on the substantive provisions of Chapter 4.

**Clause 39 – Commissioner to have regard to objects of Act**

282. This clause ensures that the National Data Commissioner upholds the objects of this Bill (refer clause 3) in carrying out their functions under clause 41.

**Part 4.2 – National Data Commissioner**

283. This part establishes the statutory role and functions of the National Data Commissioner, and sets out related administrative arrangements to support this role.

## **Division 1 – Establishment, functions and powers**

### **Clause 40 – National Data Commissioner**

284. This clause provides for the role of a National Data Commissioner. The Commissioner is a statutory office holder, as recommended by the Productivity Commission Inquiry into Data Availability and Use. As a statutory office holder, the Commissioner is bound by the Australian Public Service Code of Conduct, subject to regulations made under section 14(2A) of the *Public Service Act 1999*.
285. This clause works in conjunction with clause 45, which establishes the Commissioner as an official of the Department for the purposes of finance law, as defined by the *PGPA Act*. The Commissioner has obligations under that Act as such an official of the Department.

### **Clause 41 – Functions**

286. This clause sets out the functions of the National Data Commissioner.
287. The National Data Commissioner is the regulator and champion of the data sharing scheme established by this Bill. The Commissioner will provide oversight and guidance to ensure the scheme operates as intended, driving cultural change and supporting capability building among data scheme entities to promote better sharing and release of public sector data.
288. The Commissioner's primary functions relate to advice, advocacy, guidance and regulation (including accreditation) (refer subclause (1)). Subclause (1)(f) clarifies that the Commissioner has the ability to do anything incidental or necessary to support these primary functions. The Commissioner may also have other functions arising under this Bill, the rules or another Commonwealth law.
289. Subclause (2) provides that the Commissioner may perform their advocacy function by undertaking, developing, or supporting educational programs. Such programs enable the Commissioner to support best practice and promote new or emerging ways of managing and sharing data. These programs could be undertaken by the Commissioner, or the Commissioner may expend money to engage contractors to design or run the programs on the Commissioner's behalf. It is not intended for the Commissioner to grant funding to other bodies or organisations to run educational programs.

### **Clause 42 – Advice related functions**

290. This clause outlines the Commissioner's advice functions. The Commissioner will advise the Minister and relevant entities on the operation of the data sharing scheme. The Commissioner may also be required to provide advice to government agencies and Ministers under other pieces of legislation.
291. The Commissioner will be able to provide advice on their own initiative, or at the request of the Minister. For instance, the Commissioner could provide advice to inform legislative proposals and frameworks that interact with, or improve, the data sharing scheme. This may include providing comments on draft legislation, appearing before Senate Committee Inquiries, and engaging in consultations with government agencies.

### **Clause 43 – Guidance related functions**

292. This clause outlines the Commissioner's guidance functions, which are to make data codes and guidelines. These functions enable the Commissioner to support best practice data sharing, release and use, and facilitate compliance with the data sharing scheme.
293. As data codes are legislative instruments, all data scheme entities must comply with their requirements (refer clause 25). For example, data codes may set out how to comply with



requirements for sharing public sector data under this scheme, and other relevant matters, such as data management and curation (refer clause 112).

294. Guidelines are non-legislative instruments that data scheme entities must have regard to when operating under this scheme (refer clause 26). Guidelines may set out principles and processes related to any aspect of the data sharing scheme, and any matters incidental to the scheme (refer clause 113).

#### **Clause 44 – Regulatory functions**

295. This clause sets out the Commissioner's regulatory functions. The Commissioner's regulatory functions are an important element of their role, enabling effective oversight and ensuring integrity of the data sharing scheme.
296. The Commissioner's regulatory functions include handling complaints, conducting assessments and investigations, issuing directions, and performing functions and exercising powers with respect to the accreditation framework. Powers associated with these functions are set out in Chapter 5.
297. The Commissioner's regulatory functions and powers are designed to enable a graduated and proportional enforcement approach that deters, identifies, and proportionally penalises non-compliance (refer part 5.5).

#### **Clause 45 – Application of finance law**

298. This clause establishes the Commissioner as an official of the Department for the purposes of the *PGPA Act*. Officials are generally people who are employed by, or otherwise form part of, a Commonwealth entity. The Commissioner will form part of the Department that has responsibility for this Bill under an Administrative Arrangements Order.
299. As an official, the Commissioner will have duties, and be subject to rules and requirements under the *PGPA Act* and finance law as defined by that Act.

#### **Clause 46 – Staff**

300. This clause provides that the Secretary of the Department responsible for this Bill must make Australian Public Service staff of the Department available to the Commissioner.
301. Staff will assist the Commissioner in the performance of the Commissioner's functions under this Bill and other relevant legislation such as the *PGPA Act* (refer clause 41), and may be delegated functions or powers in order to do so (refer clause 49).
302. The Secretary must make adequate staff available to meet the Commissioner's needs, in terms of both numbers and abilities. The Commissioner will determine the necessary skills, experience and/or qualifications that staff must have.
303. Subclause (2) ensures the Commissioner directs the staff in relation to the Commissioner's functions. The Secretary may continue to direct staff in the performance of other functions outside of the data sharing scheme, so there is no overlap.

#### **Clause 47 – Contractors**

304. This clause allows the Commissioner to engage contractors on behalf of the Commonwealth to assist the Commissioner in the performance of their functions and powers.
305. Contractors may assist the Commissioner, but will not be delegated the Commissioner's functions or powers, or exercise those powers themselves. For instance, contractors may assist the Commissioner to accredit entities by assessing applications, but the decision to accredit an entity ultimately rests with the Commissioner. Similarly, contractors may assist by drafting a data code, which is officially made by the Commissioner.

306. Contractors will be engaged subject to the requirements of the *PGPA Act*.

**Clause 48 – Consultants**

307. This clause allows the Commissioner to engage consultants to advise the Commissioner. For example, consultants may provide expert or technical advice as relevant to support the Commissioner in the performance of their functions or powers.

308. Consultants will be engaged subject to the requirements of the *PGPA Act*. They may assist the Commissioner, but will not be delegated functions or powers under clause 49.

**Clause 49 – Delegation by the Commissioner**

309. This clause enables the Commissioner to delegate functions and powers conferred by this Bill – with some exceptions – to Departmental staff made available to them (refer clause 46). Delegation is at the discretion of the Commissioner; the Commissioner may continue to personally perform their functions and exercise their powers.

310. Delegation is a standard regulatory practice that promotes efficient administration. Delegating powers and functions will allow the Commissioner to focus on high priority matters, supporting timely and effective management of workflows for routine functions and processes as the data sharing scheme matures.

311. This Bill restricts the functions and powers that can be delegated, rather than people or roles within the Department who can become delegates. This approach gives the Commissioner discretion to ensure staff with appropriate skills have access to powers appropriate for their role. This aligns with the approach taken by contemporary regulators, including the Australian Information Commissioner, Australian Competition and Consumer Commission, and Australian Prudential Regulation Authority.

312. Subclause (2)(a) provides that the Commissioner's powers to make data codes, guidelines, and directions (refer clauses 112, 113, and 98 respectively) cannot be delegated. These powers are unsuitable for delegation, due to the importance of these instruments to the operation of the scheme, and the consequences for entities who do not comply. While these powers can only be exercised by the Commissioner, staff and contractors may assist in the preparation of instruments and documents – for instance staff may draft a data code which is formally made by the Commissioner.

313. Subclause (2)(b) provides the Commissioner cannot delegate their functions and powers with respect to regulating the Department or its portfolio agencies. It would be a conflict of interest for Departmental staff to regulate their employer, for instance by making accreditation decisions that affect the Department. Such decisions and powers rest with the Commissioner, as an independent statutory office-holder who is not employed by the Department. The Commissioner's independence is further supported by clause 50, and clause 47, which allows the Commissioner to engage contractors (instead of Departmental staff) to assist with regulating the Department and its portfolio agencies.

314. Subclause (3) requires delegates to comply with any written directions or conditions the Commissioner places on the exercise of delegated functions and powers. This provision ensures that the Commissioner can establish appropriate bounds on the exercise of delegated powers and functions.

315. Where the Commissioner has delegated functions or powers, subclause (4) requires them to make information publicly available about the (classes of) delegates to ensure transparency in the operation and administration of the data sharing scheme.

**Clause 50 – Independence of the Commissioner**

316. This clause establishes the Commissioner's independence.

317. The Commissioner is established as an independent statutory office holder, responsible for integrity of the data sharing scheme. It would not be appropriate for officials or other entities that are involved or interested in the scheme to influence how the Commissioner performs and exercises their powers under this scheme.
318. This clause does not limit the Commissioner's accountability under this Bill or other laws, or limit the capacity of the Minister or data sharing entities to seek advice on the operation of the data sharing scheme (refer clause 42).

**Clause 51 – Commissioner not to be sued**

319. This clause provides that the Commissioner and people acting under their direction or authority are not liable for any actions or omissions done in good faith under the data sharing scheme. This aligns with standard protections for regulators and their staff acting within the limits of their legal authority.
320. Subclause (2) clarifies that this clause does not limit contractual liability. This means that the Commissioner and staff made available to them may be liable for failures to comply with the terms of contractual agreements.

**Division 2 – Terms and conditions etc.**

**Clause 52 – Appointment**

321. This clause enables the Governor-General to appoint a person to be the Commissioner where they have the appropriate qualifications, skills or experience to perform the functions of the Commissioner. The Governor-General would form a view about what qualifications, skills or experience are appropriate considering the functions of the Commissioner under this legislation and the needs of the times.
322. Appointment by the Governor-General supports the independence of the Commissioner.
323. This clause does not prevent a person from being reappointed as the Commissioner, consistent with section 33AA of the *Acts Interpretation Act 1901*.

**Clause 53 – General terms and conditions of appointment**

324. This clause sets out the general terms and conditions of the Commissioner's appointment. In particular, the Commissioner holds office on a full-time basis, for a period that does not exceed five years. Other terms and conditions of appointment may be determined by the Governor-General.

**Clause 54 – Other paid work**

325. The Commissioner is a full-time office holder (refer clause 53(2)). As such, this clause provides that the Commissioner may only engage in paid work outside the duties of the office with the Minister's approval.

**Clause 55 – Remuneration**

326. This clause provides that the Commissioner is to be paid at a rate determined by the Remuneration Tribunal. The Remuneration Tribunal is an independent tribunal established under the *Remuneration Tribunal Act 1973* to determine and advise on entitlements of Commonwealth and other public offices.
327. In line with convention for the remuneration of statutory office holders, subclause (2) enables the Minister to set allowances for the Commissioner in rules. If no determination is made by the Remuneration Tribunal, the Commissioner is to be paid the amount prescribed by the rules.

**Clause 56 – Leave of absence**

328. Aligning with convention, this clause provides that the Commissioner’s recreational leave entitlements determined by the Remuneration Tribunal.
329. Other non-recreational forms of leave, such as personal or carers leave, may be granted by the Minister, on conditions determined by the Minister.

**Clause 57 – Resignation**

330. This clause provides that Commissioner may resign their office by providing a written resignation to the Governor-General. The Commissioner is not required to provide a period of notice; their resignation takes effect on the day the Governor-General receives it, or on a later date specified in the resignation.

**Clause 58 – Termination of appointment**

331. The Governor General may terminate the appointment of the Commissioner on grounds listed in this clause.
332. Consistent with existing legislation establishing statutory office holders, listed grounds include misbehaviour, bankruptcy, extended unapproved absences, and physical or mental incapacity.
333. The Commissioner’s appointment may also be terminated for contraventions of the general duties of an accountable authority under section 29 of the *PGPA Act*.

**Clause 59 – Acting appointments**

334. This clause allows the Minister to appoint someone to act as the Commissioner for a specified period, or periods, when the office of the Commissioner is vacant, or the Commissioner is absent or otherwise unable to perform their duties.
335. A person appointed to act as the Commissioner must have appropriate qualifications, skills or experience to fulfil the role (refer clause 52). The Minister may consult with the Governor-General to confirm appropriate qualifications, skills or experience.
336. Providing for acting appointments is a standard feature of legislation establishing statutory roles to ensure continuity of office in the absence, expected or otherwise, of the office-holder. Appointment by the Minister, rather than the Governor-General, is appropriate as the appointment is on a temporary basis and may need to expeditiously cater for unexpected leave.
337. Terms and powers of acting appointments are subject to the rules within sections 33AB and 33A of the *Acts Interpretation Act 1901*.

**Part 4.3 – National Data Advisory Council**

338. This part establishes the National Data Advisory Council (the Council), establishing its functions, members, and various other administrative matters.

**Clause 60 – Establishment and function of Council**

339. This clause establishes the Council, and its function to provide advice to the Commissioner on matters relating to the operation of the data sharing scheme. The Council’s terms of reference may provide further detail on its remit or areas of focus, within the parameters established by this clause. The Council may, for example, advise on operation of the scheme in relation to best practice data management, ethical processes, privacy, or how emerging technologies and related standards might affect the data sharing scheme.

**Clause 61 – Membership of Council**

340. This clause establishes the membership of the Council.

341. The Council will include four ex-officio members (the Commissioner, Australian Statistician, Information Commissioner, and Chief Scientist), as well as between five and eight appointed members.
342. The Council's ex-officio members have been chosen by virtue of their position and depth of experience in matters relevant to the data sharing scheme. In particular, the Australian Information Commissioner was selected as an ex-officio member due to their role and functions under the Commonwealth's privacy, information, and freedom of information regimes. Other public office-holders with relevant expertise may be engaged as appointed members.
343. Appointment of the Australian Statistician and the Information Commissioner is subject to the requirements of the *Australian Bureau of Statistics Act 1975* and *Australian Information Commissioner Act 2010* respectively. The Chief Scientist is appointed by the Prime Minister.
344. The Commissioner may designate themselves as the Chair of the Council. The Chair may alternatively be an appointed member, designated by the Commissioner or Council for a period of up to three years.

**Clause 62 – Appointment of members**

345. This clause provides that the Commissioner must appoint persons with qualifications, skills or experience that will support the Council's function, on a part-time basis, by written instrument.

**Clause 63 – Term of appointment**

346. This clause provides that appointed members may be appointed for a period up to but not exceeding three years. This arrangement allows the Commissioner to review the make-up of the Council to ensure the qualifications, skills and experience of appointed members remain relevant over time.
347. This provision does not prevent a person being re-appointed, refer to section 33AA of the *Acts Interpretation Act 1901*.
348. Ex-officio members will remain on the Council for as long as they hold their respective offices.

**Clause 64 – Remuneration and allowances**

349. This clause sets out the remuneration arrangements for appointed members, subject to the requirements of the *Remuneration Tribunal Act 1973*.
350. Subclause (1) provides that appointed members are to be paid at a rate determined by the Remuneration Tribunal. The Remuneration Tribunal is an independent tribunal established under the *Remuneration Tribunal Act 1973* to determine and advise on entitlements of Commonwealth and other public offices. If no determination is made by the Remuneration Tribunal, appointed members are to be paid the amount prescribed in the rules.
351. In line with convention for the remuneration of statutory office holders, appointed members will be paid the allowances prescribed by rules.
352. This clause does not impact remuneration of ex-officio members. Entitlements of ex-officio members are established elsewhere – the Australian Statistician, for example, is appointed and remunerated under the *Australian Bureau of Statistics Act 1975*.

**Clause 65 – Leave of absence**

353. This clause enables the Commissioner to grant leave of absence to an appointed member, subject to any terms and conditions determined by the Commissioner. Repeated absence from Council meetings without leave of absence may be grounds for termination (refer clause 69).

**Clause 66 – Disclosure of interests to Minister or Commissioner**

354. This clause requires that the Commissioner and other members of the Council provide written notice of pecuniary and other interests that conflict or may conflict with the proper performance of their role on the Council.
355. The Commissioner must report conflicts of interest to the Minister, while other members must report conflicts of interest to the Commissioner.
356. The requirement to disclose conflicts of interest aligns with this Bill's underlying philosophy of accountability and transparency. It will also help to ensure that the Council provides objective advice on the operation and administration of this scheme.

**Clause 67 – Disclosure of interests to Council**

357. Under this clause, a member with pecuniary or other interests in a matter before the Council must disclose that interest to the Council. This will help to manage and reduce bias in the Council's advice.

**Clause 68 – Resignation of members**

358. This clause provides that appointed members may resign their office by submitting a written resignation to the Commissioner. Resignations will take effect on the day the Commissioner receives it, or a later day specified in the resignation.
359. Ex-officio members cannot resign from their duties on the Council – they remain members for as long as they hold their offices. Individuals who hold the offices of the Australian Statistician, Australian Information Commissioner or Chief Scientist may resign subject to the terms of their appointment – the Australian Statistician, for example, may resign their office subject to requirements of the *Australian Bureau of Statistics Act 1975*.

**Clause 69 – Termination of appointment of members**

360. This clause provides a list of circumstances in which the Commissioner may terminate the employment of appointed members of the Council. The grounds for termination reflect existing laws establishing councils, and include misbehaviour, extended unapproved absences, and physical or mental incapacity.
361. Membership may also be terminated if the member's expertise is no longer relevant or they cease to hold a professional role that was relevant to their membership of the Council. This enables the Council to remove members who have changed profession, and ensures membership can evolve with any changes in focus of the Council.

**Clause 70 – Other terms and conditions of members**

362. This clause allows the Commissioner to determine other terms and conditions on which appointed members hold office, with respect to matters not covered by this Bill.

**Clause 71 – Procedures**

363. This clause sets out core administrative procedures for the Council. In particular, Council meetings must occur at least twice per calendar year and may be convened by the Commissioner or the Chair. Otherwise, this clause empowers the Council to determine its own procedures, allowing them to be adapted as necessary over time.

## **Chapter 5 – Regulation and enforcement**

### **Part 5.1 – Introduction**

#### **Clause 72 – Simplified outline of this Chapter**

364. This clause provides a simplified outline of Chapter 5 to assist readers to understand the substantive provisions on the regulation and enforcement of the data sharing scheme. The outline is not intended to be comprehensive; readers should rely on the substantive provisions of Chapter 5.

### **Part 5.2 – Accreditation**

#### **Clause 73 – Accreditation**

365. This clause sets out the Commissioner's powers in relation to accreditation of entities, which form part of the Commissioner's regulatory functions (refer clauses 41 and 44). Accreditation is an essential precondition to entities' participation in the data sharing scheme, and provides assurance that participants are capable of handling public sector data safely. It works with the purpose test (clause 15), Data Sharing Principles (clause 16) and data sharing agreements (clause 18) to provide a robust approach to requesting and sharing public sector data.
366. Subclause (1) empowers the Commissioner to accredit entities as ASDPs and/or accredited users, and to suspend or cancel an entity's accreditation once granted. Subclause (1)(a) is clear that excluded entities (refer clause 11(3)) cannot be accredited, and works in conjunction with subclause 11(2)(c) to prevent excluded entities from participating in the scheme as any form of data scheme entity.
367. The Commissioner's accreditation powers must be exercised in a manner consistent with the accreditation framework established in Ministerial rules under clause 74. In particular, the criteria for accreditation decisions set in the accreditation framework pursuant to clause 74(2)(a) inform all decisions made under clause 73(1).
368. Subclause (2) gives the Commissioner discretion to impose conditions on an entity's accreditation, or to vary any existing conditions, provided this is done in accordance with the accreditation framework. Varying a condition could involve modifying the terms of the condition, or removing or replacing the condition. Failure to comply with these conditions may attract a civil penalty under clause 29 (comply with conditions of accreditation).
369. Subclause (2) does not limit the Minister's ability to specify conditions of accreditation that apply to accredited entities (refer clause 74(3)(a)(iv)).
370. Subclause (3) gives the Commissioner discretion to make certain accreditation decisions on security grounds, including on the basis of an adverse or qualified security assessment. Such decisions include to refuse accreditation, to place or vary conditions on accreditation, and to suspend or cancel accreditation. Under clause 104, such accreditation decisions with respect to foreign entities (defined clause 9) are not subject to merits review.
371. Subclauses (4) and (5) work together to ensure that accredited entities remain accountable and are subject to obligations and oversight under Chapters 2, 3, and 5 of this Bill – until the point their accreditation is cancelled.
372. Subclause (4) provides that a decision to cancel an entity's accreditation will not be effective if the entity has failed to comply with a direction from the Commissioner under clause 98(1)(a), unless the Commissioner determines otherwise. This means if an accredited entity fails to comply with directions to return or dispose of scheme data, their status as an accredited entity will continue, ensuring they remain subject to relevant responsibilities and liabilities. In practice, this

may involve the Commissioner issuing a direction and taking steps to verify or enforce compliance before making a decision to cancel accreditation.

- 373. Subclause (5) clarifies that an accredited entity has the status of an accredited entity at all times until its accreditation is cancelled. This means the entity continues to be subject to the responsibilities and requirements of the scheme while its accreditation is suspended, but is not authorised to collect and use data (refer clause 13(3)(b)).
- 374. This approach ensures accredited entities remain within the regulatory remit of the Commissioner and can be held accountable for their conduct with respect to scheme data, whether actively sharing or not. For example, sharing by or with an entity with suspended accreditation may attract penalties for unauthorised sharing, collection, and/or use (refer clauses 13(3)(b) and 14).
- 375. Subclause (6) clarifies that accreditation and related interests are not property for the purposes of section 51(xxxi) of the Constitution, which allows Parliament to make laws for the acquisition of property on just terms. Accredited entities are therefore not entitled to just terms compensation if the Commissioner alters their accreditation status. For example, no compensation would be payable if the Commissioner were to accredit an ADSP but later impose conditions limiting the types of data services it may perform.
- 376. Subclause (6) is modelled on section 56CA(3) of the *Competition and Consumer Act 2010* which relates to accreditation of data recipients for the Consumer Data Right, an analogous scheme for private sector data.

#### **Clause 74 – Accreditation framework**

- 377. This clause facilitates establishment of the accreditation framework, an important safeguard that provides a gateway for entities to participate in the data sharing scheme.
- 378. Subclause (1) provides the accreditation framework will be established in Ministerial rules. This approach enables creation of a self-contained system in rules, which are subject to Parliamentary oversight and better suited than a Bill to contain detailed technical requirements which may need to be updated in future.
- 379. The core components of the accreditation framework are set in subclauses (2) and (3).
- 380. Subclause (2) requires the accreditation framework to contain certain provisions relating to accreditation criteria. High-level matters that accreditation criteria must cover to ensure entities have appropriate expertise in data protection and management are set in subclause (2)(a). Subclause (2)(a)(iii) interacts with clauses 73(3) and 94 to ensure the Commissioner considers security (as defined in the *Australian Security Intelligence Organisation Act 1979*) when making accreditation decisions, for instance by considering adverse security assessments, and may engage with relevant agencies as appropriate. To provide certainty, the accreditation framework will also identify the circumstances in which accreditation may or must be cancelled or suspended by the Commissioner (refer clause 73(1)(b)).
- 381. Subclause (3) describes administrative and other matters the accreditation framework may also address. These matters include (but are not limited to) processes for granting or restricting accreditation, and other conditions or requirements to maintain accreditation. While this Bill defines entities broadly (refer clause 9), the scheme may specify the kinds of entities that may be accredited. This includes legal and non-legal entities (subject to part 6.3), and foreign entities. The scope of this provision is intended to facilitate domestic and international cooperation and innovation, particularly for research and development. The Minister may also prescribe other criteria as needed in the rules, consistent with the objects and parameters of this Bill.
- 382. The accreditation framework works with safeguards in Chapters 2 and 3 to ensure accredited entities have both capability and responsibilities to handle government data appropriately. In



addition to those safeguards, Chapter 5 provides for regulatory oversight by the Commissioner within Australia and extra-territorially, where consistent with clauses 7 and 122.

## **Part 5.3 – Complaints**

383. This part establishes a complaints mechanism to manage disputes between data scheme entities. The complaints mechanism is one of several redress mechanisms in the scheme, and a means for the Commissioner to identify potential cases of non-compliance and areas to improve or support implementation of the scheme.

### **Division 1 – Complaints**

#### **Clause 75 – Making complaints**

384. This clause establishes a complaints mechanism for the data sharing scheme. Complaints provide a means for data scheme entities to resolve disputes with each other and to notify the Commissioner about suspected non-compliance. This mechanism supports the Commissioner to monitor and enforce the data sharing scheme, as well as identify areas where additional guidance may be needed to support voluntary compliance.
385. Subclause (1) enables data scheme entities (complainants) that reasonably believe another data scheme entity (respondent) has breached this Act to make a complaint to the Commissioner.
386. Complaints must relate to reasonably suspected breaches of the data sharing scheme, including failure to abide by requirements in the rules and applicable data codes (refer clause 25). Breaches are taken to mean acts, practices, and omissions, both present and past. A reasonable belief is taken to mean actual knowledge or a subjective belief that a prudent person would hold when given the same information.
387. Complaints may be made about former data scheme entities, where the suspected breach occurred while the entity was a data scheme entity. This aligns with the Commissioner's ability to exercise regulatory powers in relation to the activities of former data scheme entities that occurred when the entity had data scheme entity status. This regulatory scope is necessary as breaches may not come to light immediately when they occur.
388. Data scheme entities cannot complain about decisions made by data custodians not to share data under the scheme, as this does not constitute a breach of the legislation. Data custodians are best placed to assess data sharing requests due to their understanding of the data, and the corresponding risks of and public interest in sharing it.
389. Complaints may be made about sharing decisions, for example when data has been shared for a precluded purpose or if agreed safeguards under the data sharing principles were improperly applied. This enlivens the Commissioner's regulatory functions and powers (refer clause 44) to ensure the legislation is applied appropriately, and their role to oversee the operation of the data sharing scheme as a whole.
390. Subclause (2) clarifies that former data scheme entities may make complaints within 12 months of losing their data scheme entity status. This period provides an appropriate window for former data scheme entities to seek to resolve any latent or ongoing issues with their participation in the data sharing scheme. The 12 month window mirrors the Commissioner's ability to dismiss complaints if they are made more than 12 months after the complainant first reasonably believed the respondent breached or was breaching the Act (refer clause 79(1)(d)).
391. Subclause (3) requires complaints to specify the respondent, be made in the approved form (if any), and meet any requirements prescribed by an applicable data code. These requirements will standardise processes and ensure the Commissioner has crucial information to progress complaints.

392. While this mechanism is for data scheme entities, it does not prevent other entities contacting the Commissioner through administrative channels or complaining about data scheme entities' activities through existing legal mechanisms. For instance, a person may complain to the Australian Information Commissioner about mishandling of their personal information, under the *Privacy Act*.
393. This mechanism focusses on situations unique to the data sharing scheme to avoid duplicating existing, understood redress mechanisms under the remit of other regulators, and is supported by the Commissioner's ability to collaborate with other regulators (refer clauses 93 and 94).

#### **Clause 76 – Respondents**

394. This clause clarifies who the respondent to a complaint is, depending on the nature of the entity.
395. Note that not all data scheme entities will be legal persons – part 6.3 outlines the legal treatment of partnerships, unincorporated associations, and trusts respectively.

#### **Clause 77 – Communicating with complainant**

396. This clause ensures the complainant receives notice of how the Commissioner is responding to their complaint within 30 calendar days of receiving it. This provision is intended to provide transparency and assurance to complainants that due process is observed. The 30 day period provides a reasonable timeframe for the Commissioner to begin any preliminary enquiries of the complaint, and set out steps to resolve it.
397. The Commissioner may, but is not required to, notify respondents about complaints. In most cases complainants should have first raised their complaint with the respondent directly. This minimises the burden on the Commissioner and respondents when dealing with vexatious or unsubstantiated complaints. If the Commissioner decides to proceed with an investigation of the complaint they must notify the respondent of this fact (refer clauses 88 and 90).
398. Subclause (2) provides that the Commissioner may, by written notice, request that complainants provide further information in connection with the complaint, within the period specified in the notice. Such requests will allow the Commissioner to collect information needed for preliminary inquiries of complaints when initial requests are incomplete or insubstantial.
399. If the Commissioner makes a request under subclause (2), they need not take further action in relation to the complaint until the complainant complies with that request. The Commissioner has 30 days from the day requested information is provided to notify the complainant how they are responding to their complaint.
400. Subclause (4) states that the Commissioner need not provide notice under subclause (1) if the Commissioner has given the complainant notice that they will not deal with the complaint (refer clause 79) on or before the day the written notice under subclause (1) was due.

#### **Clause 78 – Dealing with complaints**

401. This clause provides the essential steps, at a high level, the Commissioner must follow in order to determine how best to deal with a complaint. In particular, the Commissioner must make preliminary inquiries as needed, and consider and arrange for conciliation if appropriate.
402. Conciliation is encouraged as it maximises the autonomy of parties to the complaint. If the Commissioner is satisfied that conciliation is not appropriate to deal with the complaint or if the complaint is not resolved through conciliation, the Commissioner must start an investigation under clause 88.
403. The Commissioner need not proceed with handling a complaint if the Commissioner is satisfied that there are grounds to do so under clause 79.

**Clause 79 – Grounds for not dealing with complaints**

404. This clause lists circumstances in which the Commissioner may decide to cease dealing with a complaint or not deal with a complaint. The Commissioner may rely on one or more circumstance. Listed circumstances are intended to prevent regulatory duplication and limit unnecessary use of time and resources.
405. To ensure transparency, if the Commissioner decides to cease dealing with a complaint, they must notify the complainant of their decision and the reasons for it. If the Commissioner has notified the respondent of the complaint, the respondent must also be notified.

**Clause 80 – Admissibility of things said or done in conciliation**

406. This clause provides that anything said or done in the course of conciliation is not admissible in relevant legal proceedings, unless otherwise agreed to by the parties or when the thing itself constitutes an offence or civil contravention.
407. This clause allows data scheme entities to fully commit to conciliation and aligns with standard protections for matters and parties involved in conciliation. This should increase satisfactory resolution of complaints via conciliation, and reduce the resourcing and time burden of managing disputes through the courts.

**Division 2 – Representative complaints**

408. This division establishes a scheme for representative complaints. All provisions are modelled off equivalent provisions from the *Privacy Act*.

**Clause 81 – Conditions for making a representative complaint**

409. This clause sets out when representative complaints can be made under clause 75. A complainant may submit a representative complaint when there is a group of data scheme entities who all have complaints against the same data scheme entity, and those complaints all come from similar or related circumstances giving rise to a substantial and shared issue of law or fact. Representative complaints will allow the Commissioner to deal with multiple related complaints in a single, unified process, with all the relevant information. Representative complaints will be particularly useful when seeking to resolve matters related to multi-party Data Sharing Agreements.
410. Representative complaints must describe or identify class members, and specify the nature of the complaint, relief sought, and common questions of law or fact to be address. Complainants need not specify the number of class members, or name them. Similarly, complainants need not seek the consent of class members before submitting a representative. This is because complainants may not know or be able to find out the details of all data scheme entities affected by the subject of the complaint.

**Clause 82 – Commissioner may determine that a complaint is not to continue as a representative complaint**

411. This clause sets out when the Commissioner may determine that a representative complaint will not continue. The parameters for determinations align with precedent for management of representative complaints, such as those in the *Privacy Act*.
412. Subclause (1) provides the Commissioner may determine a complaint should not continue as a representative complaint on their initiative or upon application by the relevant respondent.
413. The Commissioner may make such a determination if they are satisfied it is in the interests of justice to do so for any of the listed reasons in subclause (2). These reasons include where the representative complaint is likely to be more costly than the costs of class members making separate complaints, or will not be an efficient means of dealing with members' complaints. Other

reasons include where the complainant did not submit the complaint in good faith, or it is otherwise inappropriate to pursue the matter as a representative complaint.

414. If such a determination is made, subclause (3) provides that the complaint may be continued as a separate complaint by the complainant or another class member, on their own behalf. Allowing representative complaints to continue as separate complaints ensures that the complainant and class members do not lose access to appropriate recourse avenues.

**Clause 83 – Additional rules applying to the determination of representative complaints**

415. Subclause (1) allows the Commissioner to replace the complainant with another class member to improve the efficient and effective management and outcomes of representative complaints.
416. Subclause (2) allows a class member to withdraw from a representative complaint if was made without their consent, or otherwise before the Commissioner begins their preliminary investigations (refer clause 78 (1)) into the matter.
417. Where a person withdraws from a representative complaint under clause 83(2), they may still lodge a complaint about the same matter under clause 75.
418. Subclause (3) enables the Commissioner to direct that notice of any matter be given to a class member or class members by the representative complainant or another person. This power could be used to manage situations where information needs to be provided to particular (but not all) class members, and the representative complainant has not identified which to the Commissioner. It could also be used to notify class members of matters relating to the representative complaint, especially where it is uncertain whether all have consented to participating in the matter, to ensure they are made aware of their involvement.

**Clause 84 – Amendment of representative complaints**

419. This clause allows the Commissioner to alter the class membership of a representative complaint (so it continues as a representative complaint), or to unify related individual complaints into a representative complaint.
420. ‘Altered’ includes addition and removal of members, and other changes to composition of the class of members – for instance in response to the scope of the matter being refined or clarified. Where this involves removal of class members whose complaints are not shared with the rest of the class, so are not part of the class action, such complaints brought separately.

**Clause 85 – Class member for representative complaint not entitled to lodge individual complaint**

421. This clause provides that a class member of a representative complaint cannot lodge a separate complaint about the same matter. This reduces unnecessary administrative burden and duplication.

**Part 5.4 – Assessments and investigations**

422. This part establishes mechanisms for the Commissioner to monitor and gather information about the operation of the data sharing scheme and data scheme entities within it.

**Clause 86 – Assessments**

423. This clause empowers the Commissioner to assess whether data scheme entities’ activities are consistent with the requirements of the data sharing scheme. Assessments may target compliance with specific aspects of this Bill, in line with the Commissioner’s annual regulatory priorities, such as application of a particular data sharing principle.
424. Assessments will be constructive, regular processes that support voluntary compliance and provide assurance to the Commissioner that the scheme is operating as intended. The

Commissioner may undertake assessments in any manner they consider appropriate. This may include inviting submissions, and exercising their information-gathering and monitoring powers (refer clauses 91 and 95). This non-prescriptive approach will allow the Commissioner to adapt assessments to different circumstances and data scheme entities, and update and improve how they are undertaken over time.

425. The Commissioner may assess the conduct of former data scheme entities, provided that the conduct being assessed occurred while the entity was a data scheme entity. This supports scheme integrity and ensures former data scheme entities are accountable for any conduct engaged in while participating in the data sharing scheme.

#### **Clause 87 – Notices of assessment**

426. To ensure procedural fairness, this clause requires the Commissioner to give data scheme entities notice before starting, and on the completion of, an assessment of the operations of that entity.
427. Assessments are intended to be collaborative processes between the entity and Commissioner, so notices given before starting assessments must specify their intended scope. This will allow data scheme entities to make any preparations necessary to facilitate the assessment and request that the assessment cover other matters, if desired.

#### **Clause 88 – Investigations**

428. Investigations provide a means for the Commissioner to determine whether an entity is breaching or has breached requirements of the data sharing scheme. Under this clause, investigations occur in response to a complaint (refer clause 75), or on the Commissioner's own initiative.
429. Subclause (1) requires that the Commissioner investigate the subject of a complaint when satisfied that it is not appropriate to deal with the complaint by conciliation, or conciliation failed to resolve the complaint (refer clause 78).
430. Subclause (2) allows the Commissioner to investigate an entity when they reasonably suspect that entity has breached or is breaching the requirements of the data sharing scheme. Reasonable grounds may derive from advice from other regulators, information gathered during an assessment, or a pattern of breaches across the scheme that provides a realistic likelihood of non-compliance.
431. Subclause (3) provides that the Commissioner may investigate former data scheme entities if the conduct being investigated occurred at a time when the entity was still a data scheme entity. This supports scheme integrity as breaches may not come to light immediately after they occur.
432. Subclauses (4) to (7) contain procedural matters for how the Commissioner undertakes investigations, including when investigations may cease. Further details on when investigations may cease are established in clause 79.
433. Note that this clause applies to entities, rather than data scheme entities, so the Commissioner may investigate non-compliance with their notice to produce information power in clause 91 (which applies to data scheme entities as well as other persons). Clauses 89 and 90 flow from investigations under clause 88, as do certain consequences of a determination of breach set out in later clauses, so take the same approach.

#### **Clause 89 – Determination on completion of investigation**

434. This clause requires the Commissioner to make a written determination setting out findings of an investigation completed under clause 88.
435. Subclause (1) prescribes the content of determinations. To ensure due process, each determination must be in writing, and set out the Commissioner's opinion and reasoning of whether the investigated entity breached the requirements of this legislation. If the Commissioner

finds a breach has occurred or is occurring, the determination will also describe what regulatory or enforcement action the Commissioner intends to take to address the situation.

- 436. Certain enforcement actions, such as issuing infringement notices and seeking injunctions or judicial remedies, rely on a determination of breach being made by the Commissioner.
- 437. Determinations will be provided to relevant entities under clause 90, providing a clear outcome from investigations. Subclause (2) provides that the Commissioner may also to publish determinations, for example when they relate to a breach which may impact other data scheme entities.
- 438. Subclause (3) provides that if at any time the Commissioner has reason to vary or revoke a breach determination, they may do so. This could include when a data scheme entity provides evidence that changes the Commissioner's opinion as to whether the breach has occurred.
- 439. Subclause (4) is included to assist readers, as determinations are not legislative instruments within the meaning of subclause 8(1) of the *Legislation Act 2003*.

#### **Clause 90 – Notices relating to investigation**

- 440. To ensure procedural fairness, the Commissioner must give entities notice providing the intended scope of an investigation before commencing it. The Commissioner must also give determinations made under clause 89 to the entity that was investigated upon completion of that investigation. This will provide a clear outcome from each investigation, and clarify next steps, if any.
- 441. The Commissioner may, but is not required to, notify complainants about determinations related to their complaint. It may not always be appropriate for complainants to be given full details of the outcomes of investigations, particularly if they would tend to disclose sensitive details about the data or processes under investigation.
- 442. If the Commissioner varies or revokes a determination, the Commissioner must give the variation or revocation to the persons who were given the original determination. This will ensure relevant people are kept up-to-date on any changes to the outcomes of the investigation.

### **Part 5.5 – Regulatory powers and enforcement**

- 443. This part provides the Commissioner's regulatory powers to monitor and enforce the requirements of the data sharing scheme. These powers are designed to enable a graduated enforcement approach that identifies and responds proportionally to address non-compliance. Voluntary compliance will be supported through capacity building measures, such as regular assessments (refer clause 86) and paired recommendations (refer clause 97), and activities under the Commissioner's other functions.

#### **Clause 91 – Power to require information and documents**

- 444. This clause empowers the Commissioner to compel the production of information and documents relevant to the exercise of their regulatory functions (refer clause 44) from any person. This is known as a 'notice to produce' power, or an information gathering power.
- 445. The Commissioner's information gathering power supplements their monitoring and investigation powers derived from the *Regulatory Powers Act*, which only allow for the collection of information and documents when physically inspecting a premises (refer clauses 95 and 96). Being able to collect information and documents remotely is less invasive and often more practical than gathering information on-site. This supports a graduated and proportional approach to managing non-compliance and enforcing the data sharing scheme.

446. Subclause (1) enables the Commissioner to make requests to any person, so long as they reasonably believe the person has relevant information. This coverage mirrors that of the *Regulatory Powers Act* monitoring and investigation powers. Inclusion of non-data scheme entities is necessary given the scope of civil penalty provisions and criminal offences in the Bill which cover, for example, sharing data with entities that are not accredited.
447. The information requested must be relevant to the exercise of the Commissioner's regulatory functions. These functions include monitoring and investigating compliance with the scheme, accrediting entities, and handling complaints. Information requested may also inform the Commissioner's enforcement approach. Note that the Commissioner may not require the provision of information from the Inspector General of Intelligence and Security or intelligence agencies, or documents specified in a certificate under clause 92.
448. Information and document requests made under this clause must be reasonable. Information requested must be relevant to the exercise of a regulatory function, and the Commissioner must have reasonable grounds to believe the person holds it. People should also be given a reasonable amount of time to comply with requests made under this clause. For example, if a request relates to a high-risk situation, a short response period may be permissible. If the request relates to a low-risk process, however, longer periods may be appropriate.
449. Subclauses (2) and (3) introduce penalties for failure to comply with subclause (1). Having penalties available for failure to comply with requests relating to investigations is appropriate given delays in identifying and rectifying non-compliance may have serious implications for people or things to which shared data relates.
450. The consequences for breach of the penalty or offence provisions established by this clause – up to 300 penalty units or up to two years imprisonment, respectively – align with analogous laws and the *Guide to Framing Commonwealth Offences*. Consistent with the *Guide*, the Bill sets maximum penalties; a court will determine what is appropriate on a case-by-case basis. The maximums set balance the penalties of older frameworks, such as the *Privacy Act*, with more contemporary offences for mishandling government and consumer data. This approach is in keeping with intent for this scheme to align with other applicable frameworks, without duplicating them, as well as with community expectations.
451. Subclause (4) explains the scope of the Commissioner's power to deal with documents obtained under this clause.
452. Subclause (5) expressly provides that legal professional privilege is not a basis to refuse to provide information requested under this clause. Providing information requested under this clause does not abrogate legal professional privilege outside of the context of the request, for example, legal advice obtained for the purpose of proceedings that follow an investigation.
453. Subclause (5) promotes effective oversight and regulation of the scheme by preventing legal professional privilege being used to deny access to materials relevant to an investigation. Abrogation of this privilege will allow the Commissioner to effectively hold data scheme entities to account for their handling of government information, an outcome in which there is a strong public interest. This approach is also informed by other regulators' experience, whose investigatory activities have been delayed or hampered by an inability to access relevant information, and the difficulty establishing the bounds of the privilege (see Australian Law Reform Commission, *Client Legal Privilege and Federal Investigatory Bodies*, Discussion Paper 73 (September 2007) chapter 6).
454. Consistent with standard practice, requests for information that is otherwise subject to legal professional privilege would only be made where the information is central to the issues

considered by the investigation, and where there are no alternatives to accessing the information (that do not involve abrogating the privilege) in a timely and complete way.

- 455. The abrogation of legal professional privilege is necessary, as data scheme entities are likely to obtain legal advice before entering into data sharing agreements that may be material to investigations under this clause. This information is likely to be central to the issues being considered by the Commissioner's investigations but unlikely to be available from an alternate source.
- 456. Subclause (5) is modelled on similar provisions for other government regulators, including the *Ombudsman Act 1976*, *Crimes Act 1914*, *Law Enforcement Integrity Commissioner Act 2006* and the *Inspector-General of Intelligence and Security Act 1986*.
- 457. Subclause (6) clarifies that subclause (5) does not affect any claims to legal professional privilege another person may have over the information or document requested under this clause. The application of subclause (5) is also constrained by subclause (1) and clause 92, which place limits on the Commissioner's power to require information and documents.
- 458. This clause does not displace the common law privilege against self-incrimination or affect Parliamentary privilege (refer clause 92(4)).

#### **Clause 92 – Limits on power to require information and documents**

- 459. This clause limits the Commissioner's information gathering power in clause 91. A notice to produce information cannot be given to excluded entities or their employees, or in relation to information that is subject to a public interest certificate issued by the Attorney-General.
- 460. Subclause (1) prevents the Commissioner requesting information from excluded entities (refer clause 9). The information that these entities hold may have particular national security sensitivities so should not be provided except when the relevant entity agrees. Subclause (1) does not prevent these entities providing information to the Commissioner if they choose to.
- 461. Subclause (2) prevents the Commissioner requesting information that is subject to a certificate issued by the Attorney-General under subclause (3), stating that provision of that information would be contrary to the public interest. If the Commissioner receives a certificate under subclause (3), any existing requests under clause 91 relating to the relevant information or documents are void.
- 462. This clause preserves protections that are available for information held by excluded entities, as well as for certain information under section 70 of the *Privacy Act*. It is not appropriate for the Commissioner to be provided information that could prejudice any of the following: Australia's security or international relations; the deliberations of Government; the conduct of an enquiry or trial; effectiveness of an investigation and enforcement of criminal law; or public safety.
- 463. As the Cabinet minister responsible for these matters, the Attorney-General issues certificates under this clause.
- 464. Subclause (4) clarifies that the information gathering power in clause 91 does not affect Parliamentary immunities or privileges, within the meaning of the *Parliamentary Privileges Act 1987*.

#### **Clause 93– Transfer of matters to appropriate authority**

- 465. This clause allows the Commissioner to request certain regulatory bodies (refer clause 94) to take carriage of matters when they are better placed to manage and/or resolve it.
- 466. Enabling transfer of matters to appropriate regulators will reduce inefficiency and unnecessary duplication. For example, if the Commissioner formed the view that the primary subject of a



complaint was potential non-compliance with the *Privacy Act*, the Commissioner could request the Australian Privacy Commissioner deal with the matter instead under this clause.

**Clause 94 – Authorisation for Commissioner to disclose and receive information**

467. This clause authorises the Commissioner to exchange information with other regulatory bodies in pursuit of regulatory or enforcement functions. This clause facilitates ongoing cooperation among regulators to resolve issues and enable activities under other functions, such as the development of joint guidelines (refer clause 113). It does not impact or override secrecy provisions which may prevent listed entities disclosing their information.
468. The Commissioner's powers to transfer matters (refer clause 93) and information (this clause) are crucial to allow the Commissioner and other regulators to perform their roles effectively. For instance, in order to assess whether an applicant for accreditation has capability to handle Commonwealth data securely the Commissioner may need information from other bodies (refer clause 74). Similarly, the Commissioner may identify matters that fall within the remit of another regulatory body (e.g. fraud, or the mishandling of personal, protected or consumer information) while monitoring and enforcing compliance with the data sharing scheme.
469. This power is a regulatory mechanism, distinct from the authorisation in clause 13 which enables data custodians to share public sector data under the data sharing scheme. It aligns with powers of other regulators such as the e-Safety Commissioner.
470. Subclause (2)(1) allows the Minister to prescribe additional agencies and bodies with whom the Commissioner may share information in the rules. This will enable the Commissioner to continue effectively overseeing and regulating the data sharing scheme in the event of machinery of government changes, and introduction of other relevant bodies.
471. Note that the Commissioner has the power to do anything necessary or incidental to their legislated functions (refer clause 41), so may communicate with data scheme entities in the course of administering the data sharing scheme without needing to rely on this clause.

**Clause 95 – Monitoring powers**

472. This clause grants the Commissioner standard monitoring powers under Part 2 of the *Regulatory Powers Act* in relation to certain provisions of this Bill.
473. Part 2 of the *Regulatory Powers Act* establishes a framework for monitoring compliance with legislative requirements. Under this framework, authorised people may enter premises for the purposes of monitoring, either with the voluntary consent of the occupier or under a monitoring warrant. The authorised person may be assisted by other persons if reasonable and necessary.
474. Subclause (1) grants the Commissioner standard regulatory monitoring powers in relation to all civil penalty and criminal offence provisions in this Bill, as well as the responsibilities of data scheme entities under Chapter 3 of this Bill.
475. Subclause (2) clarifies the Commissioner's monitoring powers extend to verifying the accuracy and completeness of any information given in compliance or purported compliance with the requirements of the data sharing scheme. This includes information provided under the accreditation framework, and information provided for the purpose of preparing the Commissioner's annual report.
476. Subclause (3) identifies particular roles and bodies for the purpose of the *Regulatory Powers Act*, for instance specifying the Commissioner is an authorised applicant and person, and relevant courts.
477. Subclause (4) provides that as an authorised person for the purpose of the *Regulatory Powers Act*, the Commissioner may be assisted by other persons in carrying out their monitoring powers

and functions. This is a standard approach to ensure regulatory efficiency, supported by provisions relating to staff, contractors and consultants in Chapter 3.

**Clause 96 – Investigation powers**

478. This clause grants the Commissioner standard regulatory powers under Part 3 of the *Regulatory Powers Act* to investigate potential contraventions of the civil and criminal penalty provisions in this Bill, as well as possible failures to comply with the responsibilities of data scheme entities in Chapter 3. Investigation powers may only be exercised in relation to an investigation under clause 88, by people identified in this clause (or their delegates).
479. The *Regulatory Powers Act* creates a framework for investigating suspected breaches of penalty and offence provisions. Part 3 of that Act allows authorised people to enter premises for the purposes of investigation, either pursuant to the voluntary consent of the occupier or under a monitoring warrant. The authorised person may be assisted by other persons if reasonable and necessary.
480. Subclause (1) specifies the matters in relation to which the Commissioner may exercise investigatory powers. Consistent with subclause (1)(b), these powers extend to investigating third parties who assist a data scheme entity to contravene the legislation, or who are accessories to an offence after the fact (refer clause 9, definition of “offence against this Act”).
481. Subclause (2) identifies particular roles and bodies for the purpose of the *Regulatory Powers Act*, for instance specifying the Commissioner is an authorised applicant and person, and relevant courts.
482. Subclause (3) provides that as an authorised person for the purpose of the *Regulatory Powers Act*, the Commissioner may be assisted by other persons in carrying out their investigatory powers and functions. This is a standard approach to ensure regulatory efficiency, supported by provisions relating to staff, contractors and consultants in Chapter 3.

**Clause 97 – Recommendations**

483. This clause enables the Commissioner to give data scheme entities recommendations reflecting outcomes from assessments or investigations (refer part 5.3).
484. Recommendations may be used to suggest how data scheme entities could improve compliance with the data sharing scheme and achieve best-practice. The Commissioner may also use recommendations to encourage data scheme entities to reconsider certain decisions, for example decisions to use a particular methodology for data management.

**Clause 98 – Directions**

485. This clause empowers the Commissioner to issue written directions to data scheme entities that require them to act or cease acting in a particular manner. Directions will be used to minimise risk and non-compliance in situations of emergency or breach of this Bill. Directions are binding on recipients and are enforced through the courts.
486. Subclause (1) specifies circumstances in which the Commissioner may issue directions.
487. The first circumstance enables the Commissioner to issue directions to accredited entities to deal with scheme data in a certain way to mitigate risks associated with the suspension or pending cancellation of their accreditation. A direction could be to destroy, return, or otherwise handle the scheme data as instructed. For example, the Commissioner may direct the entity to return any scheme data in their possession to the data custodian. A return of data is distinct from sharing authorised by Chapter 2 as the direction to return is a regulatory measure.
488. The second circumstance is when the Commissioner is satisfied a data scheme entity has breached or is breaching the requirements of the data sharing scheme. The Commissioner may detect a

breach in the course of an assessment or investigation, or be otherwise satisfied of the entity's breach. An example of the latter is where a data sharing entity is clearly acting inconsistently with its data sharing agreement, like an ADSP sharing to the wrong accredited user or in a manner that is different to safeguards agreed under the data sharing principles. In these circumstances, directions would be issued to correct non-compliant or contributory behaviours, and mitigate associated risks or harm.

489. The third circumstance is an emergency or high-risk situation. Such a situation exists when the Commissioner reasonably believes a threat has arisen that poses serious risks to activities or participants in the data sharing scheme if not promptly addressed. An example of a high-risk situation is where the Commissioner becomes aware of a systemic weakness in IT systems used to share data that could result in unauthorised sharing or release of sensitive data, that is likely to compromise the integrity or wellbeing of entities to which the data relates.
490. Directions will allow the Commissioner to act quickly to protect the integrity of the data sharing scheme, and to limit and manage the impact of legislative and data breaches. This approach allows the Commissioner to flexibly manage non-compliance, mitigating serious consequences that are less able to be addressed through slower court processes. The directions power also allows for a graduated enforcement approach and aligns with existing regulatory norms. This includes seeking court injunctions (refer clause 102) when the Commissioner seeks to correct non-compliance that is serious, systemic and ongoing, deliberate or reckless.
491. The Commissioner's directions power is not intended to impinge upon, or overlap with, judicial injunction powers. Instead, the Commissioner's directions power will be subject to judicial oversight. Directions must be enforced through the courts, and the courts may review the legality of an exercise of the directions power through established channels for judicial review. Directions may also be reviewed on their merits, and the Administrative Appeals Tribunal may make an order to stay directions while under review.
492. The consequences for breach of a direction – up to 300 penalty units – align with analogous laws and the *Guide to Framing Commonwealth Offences*. Consistent with the *Guide*, the Bill sets maximum penalties; a court will determine what is appropriate on a case-by-case basis. The maximums balance the penalties of older frameworks, such as the *Privacy Act*, with more contemporary offences for mishandling government and consumer data. This approach is in keeping with intent for this scheme to align with other applicable frameworks, without duplicating them, as well as with community expectations.
493. Subclause (4) is included to assist readers, as the instrument is not a legislative instrument within the meaning of subsection 8(1) of the *Legislation Act 2003*.

#### **Clause 99 – Civil penalty provisions**

494. This clause allows the Commissioner to seek civil penalties from a court under Part 4 of the *Regulatory Powers Act*, which provides a framework for use of civil penalties. This framework covers how civil penalties may be sought, state of mind factors that must be proved, and applicable defences.
495. Penalties may be sought once the Commissioner has investigated and determined that a civil penalty provision has been breached (refer clauses 88 and 89).
496. This clause also clarifies procedural matters, including the federal, State and Territory courts that may hear matters arising under this Bill.

#### **Clause 100 – Infringement notices**

497. This clause allows the Commissioner to issue infringement notices to current and former data scheme entities under Part 5 of the *Regulatory Powers Act*.

498. The Commissioner may issue an infringement notice if they have determined that a breach has occurred or is occurring (refer clauses 88 and 89). Infringement notices will contain fees to be paid in relation to alleged breaches. If the fee is paid, the matter is resolved, and there will be no need for court enforcement. If the fee is not paid, the Commissioner may bring court proceedings against the entity in relation to the alleged breach.
499. Infringement notices are intended to address minor instances of non-compliance, as an alternative to court proceedings which may be long and expensive. For efficiency purposes, infringement notices may deal with multiple contraventions, but may not charge multiple fees in relation to the same conduct.

#### **Clause 101 – Enforceable undertakings**

500. This clause empowers the Commissioner to accept and enter into enforceable undertakings with data scheme entities under Part 6 of the *Regulatory Powers Act*.
501. Enforceable undertakings are tools to support and enforce compliance with legislative obligations. They will set out actions an entity must take to comply with their requirements under the data sharing scheme. The Commissioner may enter into undertakings in various situations, including when they have assessed a data scheme entity (refer clause 86) and identified ways in which the entity could better comply with requirements.
502. Enforceable undertakings are voluntarily entered into, but once accepted by the Commissioner are enforceable through the judicial system. Parties may withdraw or vary an enforceable undertaking with the Commissioner's agreement.
503. In the interests of transparency, the Commissioner may publish enforceable undertakings made under this clause.

#### **Clause 102 – Injunctions**

504. This clause enables the Commissioner to seek injunctions from specified federal and jurisdictional courts to enforce obligations arising under civil penalty provisions of this legislation. Such injunctions are made under Part 7 of the *Regulatory Powers Act*.
505. Part 7 of the *Regulatory Powers Act* establishes a framework for using injunctions, including interim injunctions, to enforce legislative obligations. Injunctions are court orders directing a person or entity to do or not do a certain thing. They are often sought to resolve legal issues and disputes, but can also be used as temporary remedy while courts hear related matters.
506. The Commissioner must have determined a breach has or is occurring under clause 89 before seeking an injunction.

## **Chapter 6 – Other matters**

### **Part 6.1 – Introduction**

507. This part introduces Chapter 6, providing a simplified outline of its contents.

#### **Clause 103 – Simplified outline of this Chapter**

508. This clause provides a simplified outline of Chapter 6 of the Bill, which provides for various matters relevant to the operation of the data sharing scheme. This simplified outline is intended to assist readers to understand the substantive provisions of Chapter 6, without being comprehensive. Readers should rely on the substantive provisions of Chapter 6.

## Part 6.2 – Review of decisions

509. This Bill provides tailored redress mechanisms for the data sharing scheme, including an avenue for complaints (refer clause 75) and provision for administrative and judicial review. Avenues for redress under other frameworks and bodies continue to be available, such as the *Privacy Act* and the Commonwealth Ombudsman, including where data sharing is involved.
510. This part sets out internal and external merits review available under the data sharing scheme. Note that operation of this part does not affect the availability of judicial review, which may be available for decisions made under the data sharing scheme.

### Clause 104 – Reviewable decisions

511. This clause provides that regulatory decisions (refer clause 44) made by the Commissioner may be reviewed on their merits, aside from the types of decisions listed in subclause (2). Intent is to ensure the Commissioner's regulatory decisions are correct (i.e. made according to law) or preferable (the best on the facts before the decision-maker, when exercising discretion), to promote best practice and fair treatment of entities affected by a decision.
512. Decisions made under the Commissioner's regulatory function are generally appropriate for merits review as they may directly impact the rights and interests of individuals. This would include decisions made under the accreditation framework (refer part 5.2) and decisions under Chapter 5 to conduct assessments and investigations, make determinations, and issue directions (refer clauses 86, 88, 89, and 98 respectively).
513. This approach is consistent with government policy on administrative decision-making, as merits review is available for administrative decisions that will, or are likely to, adversely affect the interests of a person – unless there are factors justifying exclusion of review (see Attorney-General's Department, *Australian Administrative Law Policy Guide* (2011), p. 14).
514. Subclause (2) lists three types of decisions the Commissioner may make which are not subject to merits review, relating to accreditation and exchange of information with other regulators. Judicial review of the legality of such decisions will still be available through existing channels such as the *Administrative Decisions (Judicial Review) Act 1977*.
515. Subclause (2)(a) provides that accreditation decisions relating to foreign entities made by the Commissioner under clause 73(3) on security grounds are not subject to merits review. The exclusion covers decisions made under clause 73(3) with respect to either a foreign entity or an Australian entity connected with a foreign entity. A 'foreign entity' is defined in clause 9 as an entity that is not an Australia entity. Foreign entities include foreign government bodies and individuals who are not Australian citizens or permanent residents.
516. The excluded decisions are not appropriate for merits review as the review process could expose classified or otherwise sensitive details about Australia's national security, and jeopardise ongoing security operations. The exclusion is narrow; it focusses on adverse accreditation decisions relating to foreign entities made on security grounds. Other accreditation decisions will be reviewable on their merits, for instance decisions involving Australian entities not connected to foreign entities, or decisions involving foreign entities or Australian entities connected to foreign entities that are not made on security grounds. The scope of the exclusion draws on similar exclusions in Part IV of the *Australian Security Intelligence Organisation Act 1979*.
517. Subclause (2)(b) and (c) provide that decisions by the Commissioner to transfer a matter (refer clause 93), or to disclose or receive information (refer clause 94) are not subject to merits review. These decisions are preliminary or procedural in nature as they facilitate or lead to the making of a substantive or determinative decision by the body that receives the matter or information. The

procedural or preliminary quality of these decisions makes them unsuitable for merits review, and the availability of review could frustrate or delay administrative decision-making.

518. Certain other decisions made under this Bill are not subject to merits review as a function of the nature of the decision, rather than through an express exclusion in clause 104. Decisions made under the Commissioner's advice, guidance, advocacy, and incidental functions (refer clause 41) are not appropriate for merits review. For instance, decisions made under the advocacy and guidance functions do not relate to the rights or interests of a particular individual, and are legislation-like in character. Delegation decisions are also unsuitable for merits review, as they are preliminary or procedural decisions that precede the making of a substantive decision. Merits review is also unavailable for appointments to the National Data Advisory Council as decisions to appoint persons to undertake specified functions are generally not appropriate for review. This approach is consistent with the Administrative Review Council publication, *What decisions should be subject to merits review?* (1999) paras 3.3-4.48
519. Certain decisions under the Commissioner's incidental function may be challenged through other channels, such as the independent review mechanism for government procurement under the *PGPA Act*. The Commissioner's decisions will also be subject to public and Parliamentary scrutiny through their annual report and various other government accountability processes.

#### **Clause 105 – Applications for reconsideration of decisions made by delegates of the Commissioner**

520. This clause establishes a formal process for internal merits review. A decision that is a reviewable decision under clause 104 may be internally reviewed if the decision was made by a delegate of the Commissioner (refer clause 49).
521. A formal internal review process is consistent with good administrative decision-making practices. Internal review is generally easier for applicants to access, and provides a quicker and less expensive means of re-examining decisions than external review. Formal (statute-based) internal review also provides applicants with greater certainty and clarity as to their review rights, compared with informal review processes. This is consistent with the Attorney-General's Department's *Australian Administrative Law Policy Guide* (2011).
522. If a delegate has made a reviewable decision, subclause (2) allows an affected person to apply to the Commissioner for review. This internal review will be undertaken by the Commissioner personally, or a delegate, in accordance with the process set out in clause 106.
523. Decisions made personally by the Commissioner (i.e. not a delegate) cannot be reviewed internally, and affected persons must seek external review by the Administrative Appeals Tribunal (refer clause 108).
524. Under subclause (3), applications for internal review must provide reasons for the application and be in an approved form (if any) to ensure consistency.
525. In circumstances where the Minister has made rules prescribing fees for the purpose of this clause, subclause (4) provides that an application will only be considered to have been made if the relevant fee has been paid. If such a rule is made, merits review applications made under this clause are deemed not to have been made unless the prescribed fee is paid. This subclause and any rule issued under it does not preclude application fees from being paid otherwise than together with an application.

#### **Clause 106 – Reconsideration by the Commissioner**

526. This clause sets out how the Commissioner or their delegate must deal with applications for internal merits review made under clause 104. The processes established by this provision reflect and formalise standard practice for internal merits review.

527. Subclause (1) provides that reviewable decisions must be reviewed, then either affirmed, varied or revoked by the Commissioner or their delegate.
528. Subclause (2) clarifies that the affirmed, varied, or revoked decision operates as if it were the original decision. This means, for example, if a decision to issue a direction is revoked, relevant data scheme entities are not liable for failing to comply with the direction prior to its revocation.
529. Subclauses (3) and (4) promote procedural fairness by requiring written notice be provided to applicants, advising them of the outcome of the review and the reasons for the decision. The requirement to provide reasons in subclause (4) is separate from the ability to request reasons for a decision under section 28(1) of the *Administrative Appeals Tribunal Act 1975*. Reasons must be provided within 28 days after the Commissioner or their delegate decides to affirm, vary, or revoke the relevant decision.
530. Subclause (5) sets out requirements for delegates when reviewing decisions. Delegates must not have been involved in making the original decision, and must at least hold a position or perform duties at the same level as the original decision maker. This ensures appropriate separation from the original decision-making process, while maintaining the seniority of delegates involved.

#### **Clause 107 – Deadline for reconsideration**

531. This clause establishes a period within which the Commissioner or their delegates must reconsider decisions under clause 106.
532. Subclause (1) provides that the Commissioner or their delegate must reconsider decisions within 90 calendar days of receiving an application under clause 105. This deadline provides assurance to applicants that their case will be considered in a timely manner that does not unduly impede their ability to seek external merits review.
533. Subclause (2) clarifies the original decision is taken to be affirmed if the Commissioner does not notify applicants of the outcome of a review within 90 days.

#### **Clause 108 – Review by the Administrative Appeals Tribunal**

534. This clause enables the Administrative Appeals Tribunal to review the merits of regulatory decisions that are reviewable under clause 104.
535. A person may seek review of a reviewable decision by the Administrative Appeals Tribunal where the decision has been made by the Commissioner personally (that is, not by a delegate), or where the decision has been affirmed or varied by the Commissioner or a delegate. In the latter situation, the Tribunal will review the decision as affirmed or varied by the Commissioner or the delegate (not the original decision).
536. In accordance with section 28 of the *Administrative Tribunal Act 1975*, a person who is entitled to apply to the Tribunal for review of a decision is able to request a statement of the reasons for the reviewable decision from the relevant decision-maker.

### **Part 6.3 – Treatment of certain entities**

537. This part describes the treatment of various entities participating in the data sharing scheme. Clause 109 outlines when and how the conduct of individual employees, officers, agents or members may be attributed to the relevant Commonwealth, State or Territory body. Clauses 110 and 111 take a similar approach with respect to non-legal entities, such as partnerships and trusts.
538. Responsibility of bodies corporate not covered by clause 109 will be determined in accordance with Part 2.5 of the *Criminal Code* and section 97 of the *Regulatory Powers Act*.
539. These clauses and legislation work together to hold all data scheme entities accountable for actions within the scheme, to a consistent standard.

**Clause 109 – Treatment of Commonwealth bodies, State bodies and Territory bodies**

540. This clause is important from an accountability perspective, as it clarifies when an individual's conduct will be attributed to a Commonwealth, State or Territory body for the purposes of triggering the entity-level authorisations, responsibilities, and penalties under this Bill.
541. Subclause (1) explains that this Bill applies to a data scheme entity that is a Commonwealth, State or Territory body (refer clause 9) as if the body were a person, but with certain modifications set out in subclauses (2) to (4).
542. Subclause (2) recognises that Commonwealth, State and Territory bodies act through their employees, agents, officers, and members. Where these individuals engage in conduct within the scope of their employment or authority, their act or omission is attributed to the relevant data scheme entity under subclause (3), subject to subclause (4).
543. The term 'officer' is defined in clause 9 as an individual who is involved in decision-making within an entity. 'Employees' and 'agents' have their ordinary meaning, while the term 'member' captures individuals that are not considered employees of their entity, such as members of the Australian Federal Police or Australian Defence Force. The scope of authority for such roles can be determined using resources such as their terms of employment, delegation, or contract.
544. Subclause (3) sets out when and how breaches of this Bill will be attributed to the entity, instead of a person who acts (or omits to act) on its behalf. Clause 9 defines 'breach' to include civil contraventions, criminal offences, and other conduct which is not consistent with the Bill.
545. Subclause (3)(a) attributes the conduct of an employee, agent, officer or member to the relevant entity, if they engaged in the conduct on that body's behalf and within the actual or apparent scope of their employment or authority. For example, if an authorised officer of a data custodian (see clause 123) shares data for an enforcement related purpose such as conducting surveillance, their conduct would be attributed to the data custodian. The data custodian may then be liable for unauthorised sharing (refer clause 14), unless subclause (4) applies.
546. For the purpose of establishing whether an entity has breached this Bill, subclause (3)(b) provides it is sufficient to establish the person in subclause (3)(a) engaged in conduct with the requisite state of mind. The reference to 'state of mind' covers intention, knowledge, and recklessness, as well as beliefs, such as a belief about the purposes of sharing, or reasonable suspicion of a data breach.
547. A person will be liable for their own actions where they act outside the scope of their employment or authority, or not on behalf of an entity. This could mean that the person breaches this Bill, or another law under the rebound approach (refer clause 14).
548. Where subclause (3)(a) attributes a person's conduct to an entity, subclause (4) provides that the entity will not have contravened this Bill if it took reasonable precautions and exercised due diligence to avoid the conduct. This subclause encourages entities to have sound internal governance processes and procedures to support and monitor compliance with this Bill. Examples of due diligence and reasonable precautions include protective security policies, employee codes of conduct, clear delegation instruments, as well as training and review of sharing, privacy and data management practices.
549. Subclause (4) places a legal burden on an entity in proceedings for a breach of this Bill, requiring them to establish it took reasonable precautions and exercised due diligence to avoid the conduct. This burden is justifiable as the evidence required to prove reasonable precautions and due diligence would be peculiarly within the entity's knowledge and means to provide (see *Guide to Framing Commonwealth Offences* at 4.3.1). Consistent with section 13.5 of the *Criminal Code*,



a defendant need only discharge this burden on the balance of probabilities, a lower standard of proof than beyond reasonable doubt.

550. As clarified in the Note under subclause (3), this clause interacts with clause 5(2), as government bodies that do not form part of the Crown may be liable for criminal offences. Note also that Commonwealth bodies are notionally liable to pay a fee under clause 126.
551. This clause does not apply to data scheme entities that are legal persons in the form of bodies corporate. Instead, as clarified by subclause (5), section 97 of the *Regulatory Powers Act* and Part 2.5 of the *Criminal Code* will apply in relation to civil penalties and criminal offences respectively. These sections operate similarly to subclause (3)(a), attributing the conduct of individuals to bodies corporate for the purposes of civil penalties and criminal offences.
552. This clause is based on section 8 of the *Privacy Act*, section 245 of the *Work Health and Safety Act 2011*, and section 250 of the *Life Insurance Act 1995* – adapted for the needs of this Bill.

#### **Clause 110 – Treatment of partnerships and unincorporated associations**

553. This clause establishes how the data sharing scheme applies to partnerships and unincorporated associations, both of which may be accredited entities (refer clause 11). In short, partnerships and unincorporated associations have responsibilities under this scheme themselves, as if they were persons, although these obligations may be imposed upon and discharged by a responsible individual for the entity. Subclause (6) clarifies that a responsible individual is either a partner or a member of the association's committee of management, as relevant.
554. Consistent with legal norms, a responsible individual may be personally liable where their actions or omissions contribute to a civil contravention or criminal offence of the partnership or unincorporated association. Subclauses (3) and (4) provide three situations where such liability arises, namely where the partner or member:
- a. Committed the relevant act or omission; or
  - b. Supported the commission of the act or omission by aiding, abetting, counselling, or affirming it;
  - c. Was otherwise involved in or party to the act or omission, either directly or indirectly.
555. Subclause (5) provides that a change in composition of the partnership or unincorporated association, such as the addition or removal of partners or members of the committee of management, does not impact the continuity of its obligations as a data scheme entity. This maintains consistent standards for and regulation of all entities participating in this scheme, while allowing for changes in particular entities' circumstances.
556. Subclause (7) clarifies that this clause does not apply to a Commonwealth, State or Territory body, as clause 109 covers treatment of these entities.
557. This clause is modelled on sections 98A and 98B of the *Privacy Act*.

#### **Clause 111 – Treatment of trusts**

558. This clause establishes how the data sharing scheme applies to trusts, which may be accredited entities (refer clause 11). In short, a trust has responsibilities under this scheme itself, as if it were a person, although these obligations may be imposed upon and discharged by individual trustees.
559. If a trust has a single trustee, subclause (2) provides that trustee will be personally liable for contraventions or offences of the trust. If a trust has multiple trustees, subclause (3)(a) provides that an obligation imposed on a trust by this Bill is imposed on each trustee, however, any trustee may discharge the obligation.

560. Consistent with legal norms, an individual trustee may be personally liable where their actions or omissions contribute to a civil contravention or criminal offence of the trust. Subclause (3)(b) provides three situations where such liability arises, namely where the trustee:
- a. Committed the relevant act or omission; or
  - b. Supported the commission of the act or omission by aiding, abetting, counselling, or affirming it;
  - c. Was otherwise involved in or party to the act or omission, either directly or indirectly.
561. A change in the composition of a trust may affect its continuity as a data scheme entity. This reflects the legal nature of trusts, as distinct from other non-legal entities in the data sharing scheme (refer clause 110).
562. Subclause (5) clarifies that this clause does not apply to a Commonwealth, State or Territory body, as clause 109 covers treatment of these entities.
563. This clause is modelled on section 98C of the *Privacy Act*.

## **Part 6.4 – Data sharing scheme instruments**

564. This part covers the instruments that the Commissioner will be responsible for under the data sharing scheme.
565. There are three kinds of legislative instruments under the data sharing scheme. Regulations and Ministerial rules set parameters of the scheme and establish key criteria and thresholds for engaging with the scheme. Data codes are primarily intended to clarify how the data sharing scheme operates and how the legislative requirements should be complied with, and may implement administrative improvements. These instruments could also address how using certain technology or methodologies affects entities' obligations under the Bill. This approach allows the Bill itself to remain technology neutral, while enabling the data sharing scheme to adapt to emerging technologies and future needs over time.
566. Non-legislative instruments in the scheme include guidelines and registers made by the Commissioner to support best practice and transparency in the scheme.

### **Clause 112 – Data codes**

567. This clause empowers the Commissioner to make data codes, legislative instruments that serve as binding codes of practice for the data sharing scheme. The purpose and legal nature of data codes are similar to registered privacy codes under the *Privacy Act*. The Commissioner will consult with experts and other bodies on the development of data codes.
568. Subclause (2) provides a non-exhaustive list of what data codes may address.
569. Subclause (2)(a) provides data codes may set out how to comply with requirements for sharing public sector data under Chapter 2. This could include prescribing how to apply the Data Sharing Principles in different situations, such as when sharing via an ADSP, or assess requests against the data sharing purposes. Use of data codes in this manner will clarify core requirements for sharing, and standardise their application by data scheme entities.
570. Data codes may also deal with the management of complaints, including by imposing additional requirements on their submission and management, under subclause (2)(b). These requirements may be used, for example, to minimise the submission of vexatious or frivolous complaints. This provides a means for the Commissioner to effectively and appropriately administer the complaints mechanism to maximise satisfactory outcomes.

571. Subclause (2)(c) enables data codes to deal with any other matters the Commissioner considers relevant, where these matters are not contrary to, or inconsistent with, the requirements of the data sharing scheme.
572. Use of data codes for these matters, rather than regulations, is consistent with the Office of Parliamentary Counsel's Drafting Direction No. 3.8 – Subordinate Legislation. This Drafting Direction states that the contemporary approach is to use legislative instruments other than regulations. This approach has a number of advantages, including rationalising the types, number, and content of legislative instruments, as well as simplifying the structure and language of this Bill.
573. Data codes made under this clause are legislative instruments for the purposes of the *Legislation Act 2003*. Under sections 15G, 38, and 39 of that Act, legislative instruments and their explanatory statements must be registered on the Federal Register of Legislation and tabled in both Houses of the Parliament within six sitting days of registration. Once tabled, instruments are subject to Parliamentary scrutiny and may be disallowed by a notice of motion in either House within 15 sitting days.
574. As legislative instruments, data codes may not create an offence or civil penalty, provide the Commissioner with additional powers, impose a tax, set an amount to be appropriated from the Consolidated Revenue Fund under an appropriation in this Bill, or directly amend the text of this Bill. Matters set out in data codes apply where they do not contradict, or are not inconsistent with, the requirements of this Bill.
575. Subclause (3) clarifies that rules and regulations prevail over data codes in the event of any inconsistency.

#### **Clause 113 – Guidelines**

576. This clause empowers the Commissioner to make guidelines with respect to matters relating to their functions and powers under the data sharing scheme. The Commissioner will use guidelines to support best practice and to provide information about how the data sharing scheme operates. Data scheme entities are required to have regard to guidelines when engaging in conduct under this Bill (refer clause 26).
577. Guidelines may outline principles and processes related to any aspect of the data sharing scheme and matters incidental to it such as data release, management, and curation, technical matters and standards, and emerging technologies. Guidelines will help to build capacity in the data sharing scheme and data system more broadly, contributing to the Commissioner's functions and objects of the Bill.
578. Guidelines will be developed in consultation with specialists and other bodies and agencies, such as the Office of the Australian Information Commissioner and the National Archives of Australia. The National Data Advisory Council may also advise the Commissioner on the development of guidelines, particularly those that relate to the council's functions (refer clause 60).
579. Subclause (3) provides that the Commissioner may publish the guidelines in any manner they consider appropriate. In order to maximise the availability and subsequent impact of guidelines, it is likely the Commissioner will publish them on their website.
580. Subclause (4) is included to assist readers, as a guideline is not a legislative instrument within the meaning of section 8(1) of the *Legislation Act 2003*.

#### **Clause 114 – Register of ADSPs**

581. This clause requires the Commissioner to maintain a public register of ADSPs. The register will support the Commissioner's administration of the accreditation framework, and provide a

transparency mechanism to report and provide information on ADSPs to data scheme entities and the public more broadly.

- 582. Subclause (2) requires the register to contain the name, contact details, and data services that each ADSP is accredited to perform. Subclause (3) provides that this information may be supplemented by any other information the Commissioner considers appropriate. Additional information could, for example, include conditions or restrictions on an entity's accreditation, or whether the entity's accreditation has been suspended.
- 583. Subclauses (4) and (5) work together to allow the Commissioner to maintain the register in any form they consider appropriate, so long as it is publically available. The Commissioner may omit details from the register if they are satisfied it would be appropriate to do so. The Commissioner may, for example, remove the details of an ADSP from the register when their accreditation is suspended because of an investigation into a serious potential breach.
- 584. Subclause (6) is included to assist readers, as a register is not a legislative instrument within the meaning of section 8(1) of the *Legislation Act 2003*.

#### **Clause 115 – Register of accredited users**

- 585. This clause requires the Commissioner to maintain a public register of accredited users. The register will support the Commissioner's administration of the accreditation framework, and provide a transparency mechanism to report and provide information on accredited users to data scheme entities and the public more broadly.
- 586. Subclause (2) requires the register to contain the name and contact details of each accredited user. Subclause (3) provides that this information may be supplemented by any other information the Commissioner considers appropriate. Additional information could, for example, include conditions on an entity's accreditation, or whether the entity's accreditation has been suspended or cancelled.
- 587. Subclauses (4) and (5) work together allow the Commissioner to maintain the register in any form they consider appropriate, so long as it is publically available. The Commissioner may omit details from the register if they are satisfied it would be appropriate to do so. The Commissioner may, for example, not provide complete contact details for an accredited user if those contact details include an individual's personal mobile phone number.
- 588. Subclause (6) is included to assist readers, as a register is not a legislative instrument within the meaning of section 8(1) of the *Legislation Act 2003*.

#### **Clause 116 – Register of data sharing agreements**

- 589. The register of data sharing agreements is a key transparency and accountability mechanism, providing useful insights on the operation of the scheme, and information necessary for the effective use of redress mechanisms.
- 590. This clause requires the Commissioner to maintain a public register of data sharing agreements. The register will support the Commissioner in administering and reporting on the data sharing scheme, and provides transparency about data sharing activities for data scheme entities and the public more broadly.
- 591. Subclause (2) requires that the register must contain mandatory terms and any variations to mandatory terms for each data sharing agreement. Mandatory terms set out key elements of data sharing agreements including the purpose of and parties to the agreement, public sector data involved, and an explanation of how the data sharing principles have been applied. Subclause (3) provides that this information may be supplemented by any other information the Commissioner considers appropriate. This may, for example, include information on terminated or expired data sharing agreements.

592. Subclauses (4) and (5) work together allow the Commissioner to maintain the register in any form they consider appropriate, so long as it is publically available. The Commissioner may omit details from the register if they are satisfied it would be appropriate to do so. For example, the Commissioner may not publish detailed information about data security or privacy controls used by data scheme entities, in order to prevent those controls being compromised.
593. Subclause (6) is included to assist readers, as a register is not a legislative instrument within the meaning of section 8(1) of the *Legislation Act 2003*.

#### **Clause 117 – Recognition of external dispute resolution schemes**

594. This clause empowers the Commissioner to recognise external dispute resolution schemes for the purposes of resolving complaints received under clause 75. The Commissioner may refer a complaint to external dispute resolution when they are satisfied it would effectively resolve the relevant matter (refer clause 79(1)(h)).
595. External dispute resolution is an independent service that generally includes mediation and conciliation. Use of such processes is encouraged as they maximise the autonomy of parties to the complaint (refer clause 78) and can avoid the need for court proceedings. It also reflects precedent from the *Privacy Act* and the *Corporations Act 2001*.
596. Subclause (1) allows the Commissioner to recognise an external dispute resolution scheme for an entity or a class of entities, or for a specified purpose.
597. Subclause (2) sets out matters the Commissioner must take into account before recognising a scheme. The list is modelled on matters that must be considered by the Australian Information Commissioner and the Australian Securities and Investments Commission Chair under their respective schemes.
598. Subclause (3) allows the Commissioner to recognise an external dispute resolution scheme for a set period of time, or subject to particular conditions (which may be varied or revoked).
599. Subclause (4) is included to assist readers, as the instrument of recognition is not a legislative instrument within the meaning of section 8(1) of the *Legislation Act 2003*.

#### **Clause 118 – Approved forms**

600. The Commissioner may approve a form for use in the data sharing scheme.
601. Approved forms may be used to standardise the content, format, and means of distribution of information to the Commissioner and among data scheme entities. This approach supports the consistent practice and streamlining of the administrative and operational systems underpinning the data sharing scheme. The Commissioner will also be able to update approved forms over time to cater for future needs, such as changes to machine readable technologies.
602. Approved forms may be made to standardise the form of data sharing agreements (refer clause 18), non-personal data breach notifications (refer clause 37), applications for internal merits review (refer clause 105), and complaints (refer clause 75). Rules and data codes may prescribe other situations where an approved form may or must be used.

#### **Clause 119 – Rules**

603. This clause empowers the Minister to issue rules for the data sharing scheme. The rules may prescribe matters required or permitted by the Bill, such as establishing the accreditation framework (refer clause 74) and prescribing additional precluded purposes for sharing (refer clause 15). The Minister may also prescribe other matters necessary or convenient for giving effect to the data sharing scheme, to cater for future needs as the scheme evolves over time. The rules will reflect the scope of the data sharing scheme established by this Bill, and may not contradict or be inconsistent with its clauses.

604. Dealing with the matters outlined above in rules rather than regulations accords with the Office of Parliamentary Counsel's Drafting Direction 3.8 – Subordinate Legislation. Drafting Direction 3.8 outlines the contemporary approach to legislative instruments: namely, subordinate instruments should be made in the form of legislative instruments (as distinct from regulations) unless there is good reason not to do so. This approach has a number of advantages, including rationalising the types, number, and content of legislative instruments, as well as shortening the Bill and simplifying the structure and language of its provisions.
605. Covering matters in the rules will also allow the Bill to be technology agnostic, and give flexibility for the data sharing scheme to adapt to changing technology and needs over time. The capacity for rules to prescribe additional requirements on precluded purposes (refer clause 15), data sharing agreements (refer clause 18), and use of ADSPs (refer clause 28) are particularly important to ensure that the data sharing scheme is appropriately safeguarded against new and emerging risks.
606. As legislative instruments, rules made under this clause are legislative instruments for the purposes of the *Legislation Act 2003*. Under sections 15G, 38, and 39 of that Act, legislative instruments and their explanatory statements must be registered on the Federal Register of Legislation and tabled in both Houses of the Parliament within six sitting days of registration. Once tabled, instruments are subject to Parliamentary scrutiny and may be disallowed by a notice of motion in either House within 15 sitting days.
607. To avoid any doubt, subclause (2) clarifies that, as legislative instruments, rules may not create an offence or civil penalty, provide the Commissioner with additional powers, impose a tax, set an amount to be appropriated from the Consolidated Revenue Fund under an appropriation in this Bill, or directly amend the text of this Bill.
608. There are three kinds of legislative instruments under the data sharing scheme. The rules and regulations set parameters for the scheme, including criteria and thresholds for engaging with the scheme. Data codes focus on how the scheme operates, and how entities should implement and comply with legislative requirements.
609. Subclause (3) clarifies that the regulations prevail over rules, and rules prevail over data codes in the event of inconsistency.

#### **Clause 120 – Regulations**

610. This clause empowers the Governor-General to issue regulations which may prescribe matters required or permitted by the Bill, or necessary or convenient for giving effect to the data sharing scheme.
611. Primarily, regulations will list bodies and legislation that are exempt from the scheme (refer clause 17). Establishing these matters in regulations allows exemptions to be adapted over time, while maintaining Parliamentary oversight. As exemptions set thresholds for access to the sharing scheme, it is more appropriate to create them through the Bill itself or in regulations made by the Governor-General, rather than in subordinate instruments made by the Minister or the National Data Commissioner.
612. Regulations prevail over both rules and data codes in the event of any inconsistency.

#### **Part 6.5 – Other matters**

613. This part sets out administrative and other matters that are necessary to ensure the data sharing scheme operates in an effective and accountable manner. This includes provisions relating to fees, the treatment of non-legal persons participating in this scheme, the Commissioner's annual report, and reviews of the operation of the data sharing scheme.

**Clause 121 – Disclosure of scheme data in relation to information-gathering powers**

614. This clause controls the circumstances in which data shared and created under this scheme may be disclosed to a court or tribunal, or a person that could otherwise compel disclosure of information or documents. This provision is designed to preserve the scope of the Bill, while maintaining a limited, legitimate avenue for scheme data to be accessed for judicial proceedings and regulatory processes that arise under, or with respect to, this Bill.
615. Subclause (1) authorises a data scheme entity to disclose scheme data to a court, tribunal, or certain other persons in limited circumstances relating to this Bill or the data sharing scheme. In this context, disclosure includes verbal communications in response to a question, voluntary statements, as well as the production of documents or other tangible information to the same effect.
616. Subclause (1)(a) permits disclosure to persons who are empowered by the laws in subclause (2) to require disclosure of information, provided that person is exercising their powers in relation to a matter arising under, or with respect to, the data sharing scheme. Subclauses (1)(a) and (2) work together to ensure the Auditor-General, Commonwealth Ombudsman and Information Commissioner are able to perform their respective oversight functions in relation to the scheme. Examples include investigating potential privacy breaches by a data scheme entity, auditing the Commissioner, and responding to complaints about data scheme entities' activities under the scheme.
617. Subclause (1)(b) authorises a data scheme entity to disclose scheme data to persons, in circumstances where the disclosure is required under a Commonwealth, State or Territory law for the purposes of giving effect to this Bill. Similar to subclause (1)(a), the requirement to disclose is limited to purposes connected with this Bill or the data sharing scheme. For example, this subclause would authorise disclosure to a State privacy regulator for the purpose of it investigating a State government authority's handling of personal information under the data sharing scheme (refer clause 27(1)(b)).
618. Subclause (1)(c) authorises disclosure to a court or tribunal in response to an order made in the course of proceedings relating to breaches of this Bill, or breaches of other legislation, where an instance of unauthorised sharing has rebounded to the original penalty framework.
619. This clause functions as a regulatory mechanism. Disclosure authorised by this clause is distinct from sharing data under Chapter 2, so would not qualify as sharing for a (precluded) enforcement related activity, or an instance of unauthorised sharing (refer clause 14(7)).
620. This clause is necessary to provide limited access to data created under this scheme. As this data cannot be accessed via any other channel, preventing such access could frustrate proceedings under, and investigations with respect to, this Bill.
621. Permitting disclosure to persons or authorities with certain powers of compulsion also facilitates regulatory cooperation between the Commissioner and other regulators who can receive matters and information from the Commissioner (refer clauses 93 and 94). For example, this would allow the Australian Information Commissioner to conduct an investigation into a potential interference with privacy involving personal information shared under this Bill.
622. To ensure alignment and consistency, this clause is based on equivalent provisions in other schemes, including the *My Health Records Act 2012*, the *Australian Information Commissioner Act 2010*, the *Child Support (Assessment) Act 1989*, and the *Child Support (Registration and Collection) Act 1988*.
623. This clause does not affect powers of regulatory and judicial bodies to conduct their activities or to access information and data outside of the data sharing scheme. Data collected and held outside

of this scheme will be able to be accessed through existing avenues, such as usual warrants processes.

**Clause 122 – Geographical jurisdiction of civil penalty provisions and offences**

624. This clause builds on clauses 6 and 7, providing the Bill may apply extraterritorially where there is a sufficient link between the matter and Australia to establish the Commissioner's jurisdiction.
625. Subclause (1)(a), (b), and (c) cater for situations where there is a territorial link. These clauses affirm that conduct or a result of conduct that occurs in whole or in part in Australia, including its external territories, or an Australian aircraft or ship may constitute a contravention or offence (primary or ancillary) under this Bill.
626. Subclause (1)(d) establishes jurisdiction where there is a link to Australia founded on nationality of the entities involved in the contravention or offence. This clause provides that even if conduct occurs wholly outside of Australia, the Bill applies to entities formed in Australia or individuals with citizenship or permanent residence which are participating in the data sharing scheme.
627. Subclauses (2) and (3) limit the geographic scope of this Bill by providing defences for foreign entities, modelled on defences in section 15.2(2) and (4) of the *Criminal Code*. This ensures all participants in the data sharing scheme are treated equally and have appropriate access to justice.
628. Under subclause (2), a foreign entity will not be liable under this Bill for contravening a civil penalty or criminal offence provision if there is no Australian connection (territorial or nationality) and the conduct is lawful in the foreign jurisdiction in which it occurred. Subclause (3) provides the same defence for an ancillary contravention or ancillary offence, where it relates to a primary contravention or offence which occurred outside of Australia.
629. Subclauses (4) and (5) explain how the defences in subclauses (2) and (3) interact with the *Criminal Code*, in particular that the responsibility to establish a valid defence under subclause (2) or (3) rests on the entity alleged to have contravened this Bill (i.e. the defendant).
630. Subclause (6) notes that this clause displaces the application of Division 14 of the *Criminal Code* in relation to an offence under this Bill. Division 14 of the *Criminal Code* provides for the geographical jurisdiction applicable to offences under Commonwealth laws. The geographical jurisdiction established in this clause is modelled on the extended geographical jurisdiction, category B, in section 15 of the *Criminal Code*.
631. Subclauses (7) and (8) clarify concepts necessary to establish extraterritorial operation of the Bill. Subclause (7) explains that a 'result of conduct' refers to an element of the contravention or offence at issue. Subclause (8) explains that conduct involving electronic communications will be considered to have occurred partly within Australia if the communication was sent or received within Australia.
632. Subclause (9) provides a definition of the word 'point' as that term is used in this clause.

**Clause 123 – Authorised officers**

633. This clause identifies the authorised officers of data scheme entities for the purposes of clause 18, which requires data sharing agreements be entered into by an authorised officer of the relevant data scheme entity.
634. The table specifies persons who may be authorised to enter data sharing agreements on behalf of a data scheme entity, and covers the range of possible types of entities that may participate in the scheme. Typically, an authorised officer will be the head of the entity, or their delegate who has been authorised in writing for the purposes of this Bill. The ability to specify authorised officers in writing provides data scheme entities with the autonomy to authorise appropriate persons to



enter into data sharing agreements on their behalf, and, in the case of data custodians, retain oversight and control of their data.

635. Subclause (2) allows for Ministerial rules to modify authorised officers listed in the table in subclause (1). If such rules are made, the prescribed individuals (or categories of individuals) are the authorised officers for the relevant kind of data scheme entity, not the individuals listed in the table. Any modification to subclause (1) through rules will not represent a significant change to the substance and operation of this Bill. Rather, this approach recognises the variety of potential participants in the scheme, and ensures the scheme is capable of adapting to future needs, subject to the usual requirements for disallowable instruments.

#### **Clause 124 – Annual report**

636. This clause sets out matters for the Commissioner's annual report. The annual report is a key accountability and transparency mechanism for the data sharing scheme and the Commissioner as its regulator.
637. Subclause (1) requires the Commissioner to prepare and give the Minister, for presentation to Parliament, an annual report on the operation of the data sharing scheme each financial year, in accordance with the standard timing set in subclause (4). These requirements mirrors that for accountable authorities in section 46 of the *PGPA Act*. The Commissioner's annual report will not overlap with the report of the Department, as it only pertains to the data sharing scheme.
638. Subclause (2) sets out key information that the annual report must include about the operation of the data sharing scheme, and the Commissioner and National Data Advisory Council's activities. Such information includes details of any legislative instruments made that financial year, and the scope of data sharing activities and regulatory actions which have occurred. Information on reasons for entering or rejecting data sharing requests will be particularly important as an indicator of whether the data sharing scheme has or is achieving its objectives, and to identify areas for improvement. The report will also cover the staffing and financial resources made available to the Commissioner, and how they were used, for transparency.
639. Other relevant information on operation or implementation of the scheme may be included under subclause (3).
640. The Commissioner may require data scheme entities to give information and assistance for the preparation of the annual report (refer clause 33).

#### **Clause 125 – Charging of fees by Commissioner**

641. The Commissioner may charge fees to recover costs of providing services related to their functions or powers that are not covered by appropriations funding. Subclause (1) provides that Ministerial rules may prescribe such fees.
642. Fees may be charged where the services were provided by the Commissioner on their behalf. For example, the Commissioner could charge fees for coordinating conciliation in relation to a complaint, or processing an application for an entity to become accredited. The Commissioner may also charge fees for the cost of outsourcing certain elements of their functions, for example the cost of hiring a contractor to undertake an assessment of whether entities satisfy accreditation criteria.
643. Subclause (3) provides that fees are payable to the Commonwealth, through the Consolidated Revenue Fund. Under subclause (4), Ministerial rules may specify when and how fees are payable, and any other matters in relation to fees including exemptions, refunds and remissions. Other fee frameworks may also apply, including the Australian Government Cost Recovery Guidelines.

- 644. Subclause (5) provides that the Commissioner need not deliver a service when a fee is payable but remains unpaid in connection to that service. This means, for example, if the rules specified a fee for an entity to be accredited, that entity may not be accredited until that fee is paid. The Minister may provide for the extension of time for providing services in the rules.
- 645. Charging of fees by the Commissioner is established in the rules to enable appropriate and flexible adjustments of fees and related processes overtime, whilst maintaining Parliamentary oversight.
- 646. To avoid doubt, fees prescribed by rules may not impose a tax (refer clause 119). This means that fees must be charged on a cost-recovery basis, unless a relevant exception applies, such as applying a fee for a licence (refer section 53 of the Constitution for further information).

**Clause 126 – Commonwealth not liable to pay a fee**

- 647. While the Commonwealth is not liable to pay a fee imposed by its own legislation, this clause expresses Parliament's intent for the Commonwealth to be notionally liable. This is consistent with the intent behind part 6.3, which ensures that all data scheme entities are held to account for their actions within the scheme, and to a consistent standard. Subclauses (2) and (3) enable the Finance Minister to give such written directions to give effect to this policy.
- 648. In practice, this means that the Commissioner may charge other Commonwealth entities for services under clause 125, and that Commonwealth entities are notionally liable for civil penalties.

**Clause 127 – Periodic reviews of operation of Act**

- 649. This clause ensures the operation of the Act is periodically reviewed. Reviews must be completed within 12 months or a longer period agreed to by the Minister, as is standard to enable more comprehensive reviews.
- 650. Reviews will conclude with a written report submitted to the Minister, and subsequently tabled in each House of Parliament. Review reports must be tabled within 15 sitting days of the Minister receiving the report.
- 651. Reviews will occur every ten years from commencement, except the first review which must start three years after commencement. The first review occurring three years after commencement will allow for swift identification and implementation of improvements to the operation of the data sharing scheme.
- 652. Reviews will help ensure the data sharing scheme operates as intended, and provide an opportunity to consider expansion or refinements. The data sharing scheme could, for instance, be expanded in the future to enable greater State and Territory participation. They also provide a key accountability and Parliamentary oversight mechanism, to ensure the data sharing scheme is operating in-line with public expectations.