2019 – 2020 – 2021 – 2022

THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

SENATE

DATA AVAILABILITY AND TRANSPARENCY BILL 2022

REVISED EXPLANATORY MEMORANDUM

(Circulated by authority of the Minister for Employment, Workforce, Skills, Small and Family Business, the Hon Stuart Robert MP)

THIS MEMORANDUM TAKES ACCOUNT OF AMENDMENTS MADE BY THE HOUSE OF REPRESENTATIVES TO THE BILL AS INTRODUCED

Contents

Data Availability and Transparency Bill 2022

Outline and financial impact

The Data Availability and Transparency Bill 2022 (the **Bill**) establishes a new scheme for sharing Australian Government data (the **Scheme**). The Bill authorises Australian Government bodies to share (provide controlled access to) government data with accredited users for specific purposes in the public interest. Safeguards are embedded in the Bill to ensure data is managed securely, including privacy protections, frameworks for risk management and transparency, and accreditation of data users and data service providers. The Bill establishes the National Data Commissioner (the **Commissioner**) to regulate the Scheme and educate data custodians on best practice data sharing. The Scheme will promote better availability and use of Australian Government data, empower the Government to deliver better services, policies and programs, and support research and development.

Proposal announced: The Bill and the *Data Availability and Transparency (Consequential Amendments) Bill 2022* form part of the 2018-19 Budget measure 'Delivering Australia's Digital Future – data sharing and release arrangements', and the 2020-21 Budget measure 'Department of the Prime Minister and Cabinet — additional resourcing'.

Financial impact: $20.5 million from 2018-19 to 2021-22, $11.1 million from 2020-21 over 4 years, and $0.7 million ongoing from 2024-25.

Compliance cost impact: The measure will increase average regulatory costs by $0.11 million over two years, comprising a cost to business of $0.2 million per year, to community organisations of $0.06 million, and to individuals of $0.02 million per year.

The Productivity Commission's *Inquiry Report into Data Availability and Use (2017)* has been certified as being informed by a process and analysis equivalent to a Regulation Impact Statement (**RIS**) for the purposes of the Government decision to implement this legislation. The Productivity Commission's report can be found at this link: www.pc.gov.au/inquiries/completed/data-access/report.

Human rights implications: The Bill is compatible with human rights, and to the extent that it may limit human rights, those limitations are reasonable, necessary and proportionate. Refer to the Statement of Compatibility with Human Rights in Part 3 below.

Data Availability and Transparency Bill 2022 – Overview

1. The Bill establishes the Scheme for sharing public sector data for specific purposes in the public interest, underpinned by safeguards to manage risks, and transparent processes to foster trust and confidence. The Bill establishes the Commissioner as an independent regulator to oversee the Scheme.

2. Public sector data encompasses all data lawfully collected, created, or held by a Commonwealth body, or on its behalf. The concept of data includes facts, statistics, and other information capable of being communicated, analysed or processed via physical or electronic means.

3. The Productivity Commission's *Inquiry Report into Data Availability and Use (2017)* identified a number of benefits of greater data availability and use, including supporting economic and research opportunities, and the Government's vision for streamlined and efficient service delivery. Reforms were necessary to realise these benefits. In 2018, the Australian Government committed to reform the way it shares public sector data in response to this report.

4. The Bill is central to these reforms. It will help maximise the value of public sector data by providing a mechanism to overcome existing barriers through an authorisation to override other laws with appropriate safeguards in place. Overall, the Bill will establish the Scheme to support a modern data-based society, driving innovation and stimulating economic growth.

5. The Bill takes a principles-based approach to data sharing, providing data scheme entities (**Scheme entities**) with a framework to tailor sharing arrangements, and ensures the Scheme can respond to evolving technologies and community expectations. Modernising the approach to sharing data will empower the Government to deliver effective services and better-informed policy and programs, and support research and development.

6. 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.

7. In developing the Bill, PM&C has taken a privacy-by-design approach to identify, minimise and mitigate privacy impacts wherever possible. Three independent Privacy Impact Assessments were undertaken to inform policy positions, the legislative framework, and the draft Bill. Privacy safeguards were also strengthened in response to guidance and advice received from the National Data Advisory Council and privacy experts, including the Office of the Australian Information Commissioner (**OAIC**). Further consultation was undertaken on an exposure draft of the Bill with a number of key stakeholders. This involved bilateral and multilateral virtual engagements.

8. The Bill is underpinned by four key safeguards to ensure safe sharing of data under the Scheme.

Key safeguard: 1. Accreditation framework

9. Only Scheme entities (data custodians and accredited entities) can participate in the Scheme. Commonwealth bodies that are data custodians are participants in the Scheme by default.

Other entities can apply for accreditation to become an accredited user or an Accredited Data Service Provider (**ADSP**).

10. Foreign entities are not able to become accredited, which means that data cannot be shared with a foreign entity under the Scheme.

11. Private entities (bodies corporate), individuals and unincorporated bodies (such as partnerships and trusts) are precluded from participating in the Scheme. These preclusions are intended to provide an opportunity for the Scheme to establish and mature.

12. An excluded entity cannot share, collect or use data under the Scheme. Australian Government law enforcement and intelligence entities, such as the Office of National Intelligence and the Australian Federal Police, are excluded from the Scheme to ensure independence and integrity of such entities.

13. Entities applying for accreditation will be assessed under the Bill's accreditation framework by the relevant accreditation authority (the Minister or the Commissioner). The accreditation authority is responsible for assessing the entity's capability to handle data safely and manage risks against the accreditation criteria, and grant accreditation if the entity meets the criteria. To become accredited, an entity is required to have: appropriate data management and governance policies and practices; an appropriately qualified individual in a position that has responsibility for data management and data governance; ability to minimise the risk of unauthorised access, sharing or loss of data; the necessary skills and capability to ensure the privacy, protection and appropriate use of data; and any additional criteria prescribed by Rules. The Scheme's accreditation framework ensures accreditation can keep up to date with technology, adhere to robust data security and privacy safeguards, and provide for confidence in the integrity of the Scheme. The Minister will be responsible for accrediting the Commonwealth, State and Territory bodies politic, Commonwealth bodies, and State and Territory bodies as accredited users. The Commissioner will be responsible for accrediting ADSPs and Australian universities. ADSPs must renew their accreditation every five years.

14. The relevant accreditation authority may take administrative measures to impose conditions of accreditation on an entity, and suspend or cancel an entity's accreditation under certain circumstances. This allows the accreditation authority to manage risks associated with the accredited entities and safeguard the integrity of the Scheme.

Key safeguard: 2. Authorisations and penalties

15. The authorisations under the Bill set out requirements for each stage of a data sharing project to ensure the sharing, collection and use of data is safe and fit-for-purpose. The constitutional requirements to support data sharing are built into the authorisation requirements and must be met to authorise the sharing, collection and use of data under the Scheme.

16. Scheme entities must meet the requirements relevant to their entity type in order to obtain authorisation to share, collect or use data. For example, a data custodian must meet the requirements under clause 13 in order for the sharing of data to be authorised.

17. To reflect and add to data management nomenclature, the different roles a Scheme entity may have are also described in plain words in the Bill. A data custodian is also referred to as the sharer of the data, an accredited user is also referred to as the user and an ADSP, being an entity through which the data is shared with a user, is also referred to as the intermediary.

18. Scheme entities may only share, collect or use data for a project that is for a data sharing purpose, consistent with the data sharing principles and covered by a registered data sharing agreement. A project must not be for a precluded purpose, such as an enforcement related

purpose. The three data sharing purposes are: delivery of government services, informing government policy and programs, and research and development.

19. Scheme entities must enter into a data sharing agreement, setting out the details of the data sharing project. A data sharing agreement must contain certain details, including a description of how Scheme entities will give effect to the data sharing principles and how the project serves the public interest. These details will be recorded on a register, kept and maintained by the Commissioner. Part of such details, including the description of the data to be shared and whether personal information is to be shared, are required to be kept on the part of the register that is publicly accessible. Data must not be shared until the data sharing agreement has been registered.

20. Penalty provisions under the Bill will apply where the sharing, collection or use of public sector data are unauthorised. A Scheme entity who fails to meet the authorisation requirements will be subject to both civil and criminal penalty, and designated individuals for an entity, such as a staff or contractor, may also be subject to such penalties. These provisions will operate regardless of other laws of the Commonwealth or a State or Territory.

Key safeguard: 3. Privacy protections

21. Robust privacy protection provisions are embedded in the Bill to safeguard privacy and manage risks of privacy interference. These provisions were developed in consultation with the Attorney-General's Department and the OAIC to ensure alignment with the requirements under the *Privacy Act 1988* (Cth) (the **Privacy Act**). In particular, the Bill provides for general privacy requirements applicable to all data sharing under the Scheme, as well as privacy requirements for specific data sharing purposes. Key privacy protections and privacy enhancing measures include:

- a starting position that data shared under the Scheme must not include personal information unless an exception applies;
- data minimisation requirements, that is personal information can only be shared where necessary;
- a requirement for express consent for the sharing of biometric data;
- a prohibition on the re-identification of de-identified data;
- a prohibition on the storing or accessing of personal information outside of Australia;
- a requirement that the Commissioner must make a data code about how Scheme entities obtain consent from individuals, and principles data custodians must apply in determining if it is necessary, or in the public interest, to share personal information in certain circumstances; and
- a requirement to review the Scheme if changes are implemented following the current review of the *Privacy Act*.

Key safeguard: 4. The National Data Commissioner

22. The Bill establishes the Commissioner as an independent statutory office holder responsible for overseeing the Scheme as its regulator, holding participants accountable to robust standards of privacy, security and transparency.

23. The Commissioner has responsibility for accrediting eligible Australian entities as ADSPs and accredited users, and maintaining registers of accredited entities and data sharing agreements. The accreditation and authorisation frameworks are key safeguards to promoting the integrity of the Scheme.

24. The Commissioner is a member, and may designate themselves as Chair of the National Data Advisory Council (**the Council**). The Council will provide advice to the Commissioner on matters relating to operation of the Scheme and the controlled access and use of public sector data. The Council will advise on ethics, balancing data availability with privacy protection, trust and transparency, technical best practice, and industry and international developments.

25. To promote transparency of the Scheme, and enhance integrity and transparency of sharing public sector data, the Commissioner is required to prepare and give an annual report to the Minister, for presentation to the Parliament, on the Commissioner's activities.

26. The Commissioner will also be responsible for dealing with complaints from Scheme entities about other Scheme entities (scheme complaints), as well as complaints from any person or entity (including members of the public) about the administration and operation of the Scheme (general complaints). The Bill confers a range of regulatory and investigative powers to the Commissioner to support their function to deal with complaints as well as general monitoring and assessment of the Scheme. In the case of a privacy complaint, the Commissioner may share information with and where appropriate, refer the complaint to the OAIC.

27. The Commissioner has education and support related functions to assist data custodians and other Commonwealth bodies participating in the Scheme, and support the overall operation of the Scheme. The Commissioner's education related function is intended to foster best practice safe data handling by Commonwealth bodies in relation to any data sharing.

28. Australian Public Service staff and contractors with appropriate skills, experience and qualifications may assist the Commissioner to perform their functions or exercise powers to the extent that doing so will not give rise to potential conflict of interest.

Implementation

29. The Data Availability and Transparency (Consequential Amendments) Bill 2022 (the **Consequential Bill**) staggers the commencement of the Scheme to allow eligible entities to prepare and seek accreditation. This includes transitional arrangements for eligible Accredited Integrating Authorities to participate in the Scheme as ADSPs while applying for ADSP accreditation.

30. The Scheme provides accredited users with a pathway to access data in a safe and controlled way. Under the Scheme data custodians are not under an obligation to share data, but are required to provide reasons to accredited users when they refuse to share requested data. The Scheme allows for all existing pathways and mechanisms for data sharing and redress to continue to operate unaffected.

31. Existing legal obligations and policies for handling Australian Government data continue to apply, including the Australian Privacy Principles in the *Privacy Act*, records management requirements under the *Archives Act 1983* (Cth), and the Protective Security Policy Framework.

32. To ensure the Scheme remains relevant and adaptable to evolving technology and public expectations, the Bill provides for an independent review three years after the Scheme's commencement. This is in addition to a review three months after the commencement of any amendments to the *Privacy Act* that would have a material impact on the Scheme. A review must be completed within 12 months, or a longer period agreed by the Minister.

33. The Bill sunsets and ceases to have effect at the end of the day that is the fifth anniversary from the day the Scheme commences. This ensures the operation of the Scheme is reconsidered by the Parliament following the three year review. This means the Scheme must

demonstrate its value to the Australian public to continue into the future. The review and sunset provisions serve as an additional accountability mechanism to ensure the Scheme operates as intended.

ABBREVIATIONS

The following abbreviations are used throughout this revised explanatory memorandum:

Acts Interpretation Act	*Acts Interpretation Act 1901* (Cth)
ADSP	Accredited data service provider
APP	Australian Privacy Principles, as set out under the *Privacy Act*
APS	Australian Public Service
APP entity	An agency or organisation, as defined under the *Privacy Act*
Archives Act	*Archives Act 1983* (Cth)
ARC Guidance	Administrative Review Council, 'What decisions should be subject to merit review?*'* (1999)
ASIO Act	*Australian Security Intelligence Organisation Act 1979* (Cth)
Bill	Data Availability and Transparency Bill 2022
Commissioner	National Data Commissioner
Council	National Data Advisory Council
Criminal Code	Schedule to the *Criminal Code Act 1995* (Cth)
FOI Act	*Freedom of Information 1982* (Cth)
Guide to Framing Commonwealth Offences	Attorney-General's Department, 'Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers' (Sept, 2011)
Information Commissioner	Australian Information Commissioner

Legislation Act	*Legislation Act 2003* (Cth)
PGPA Act	*Public Governance, Performance and Accountability Act 2013* (Cth)
Privacy Act	*Privacy Act 1988* (Cth)
Regulatory Powers Act	*Regulatory Powers (Standard Provisions) Act 2014* (Cth)
Scheme	Data sharing scheme, that is the Bill and its framework of instruments and operational process
Scheme entity	Data scheme entity as defined under the Bill
User	Accredited user

2 – Notes on Clauses

Chapter 1 – Preliminary

Part 1.1 – Introduction

2. 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

3. Once enacted, the short title of the Act will be the *Data Availability and Transparency Act 2022*.

Clause 2 – Commencement

4. Clause 2 provides that the entire Bill will commence the day after Royal Assent is received, as set out in the table.
5. This approach establishes the Commissioner and empowers them to implement the Scheme created by the Bill.
6. In practice, the Scheme will be operational once the Commissioner is appointed, and the instruments and systems underpinning the Scheme have been implemented, in particular the accreditation framework under Part 5.2.

Clause 3 – Objects

7. Clause 3 sets out the objects of this Bill, which are to:
   - serve the public interest by promoting better availability of public sector data;
   - enable the sharing of public sector data consistently with the *Privacy Act* and appropriate security safeguards;
   - enhance integrity and transparency in sharing public sector data;
   - build confidence in the use of public sector data; and
   - establish institutional arrangements for sharing public sector data.
8. This clause sets out specific objectives of the legislation to achieve the Australian Government's intent, addressing priorities identified in the Productivity Commission's *Inquiry Report into Data Availability and Use (2017)* for establishing a scheme to enable and regulate sharing of public sector data.
9. 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 Commissioner to administer and regulate the Scheme is crucial to achieving these objectives.
10. Paragraph 3(c) makes it clear that the Scheme is to operate consistently and harmoniously with the protections to personal information set out in the *Privacy Act*.
11. Substantive provisions elsewhere in the Bill should be read in light of these objectives.

Clause 4 – Simplified outline of this Act

12. Clause 4 sets out a simplified outline of the Bill.

13. The outline is included to assist readers to understand the substantive provisions of this Bill, but it is not intended to be comprehensive. Readers should rely on the substantive provisions of the Bill.

Clause 5 – Act binds the Crown

14. Clause 5 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.

15. 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

16. Clause 6 operates with clause 7 to ensure the authorisations, safeguards, and regulatory aspects of the Scheme (including relevant parts of the *Regulatory Powers Act*) apply consistently throughout Australia and its external territories, as well as extraterritorially.

17. 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

18. Clause 7 extends the application of this Bill and relevant parts of the *Regulatory Powers Act* to conduct, matters, and things outside of Australia, subject to the obligations of Australia under international law, including obligations under any international agreement binding on Australia and any Commonwealth laws giving effect to the agreement.

19. The clause applies to both civil contraventions and criminal offences. Geographical jurisdiction for civil penalty provisions and offences is dealt with in clause 136.

Part 1.2 – Definitions

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

Clause 9 – Definitions

21. Clause 9 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.

22. Where possible, existing definitions have been used or adapted to ensure the Bill operates consistently alongside other legislative schemes. For example, the term personal information has the same meaning as in the *Privacy Act*.

23. Where a word is not defined, readers should rely on its ordinary meaning, when read in the context of the provision in which it appears, as well as the Bill more broadly.

24. Key definitions from this clause, other than signpost definitions, are explained below in alphabetical order.

25. ‘Accreditation authority’ is a person who has the power to accredit Australian entities under Part 5.2. The accreditation authority may be the Minister or the Commissioner depending on the type of entity seeking accreditation and the type of accreditation sought under the Scheme. The Minister is responsible for the accreditation of Commonwealth, State or Territory bodies politic or Commonwealth, State or Territory bodies (within the meaning of this Bill) applying for accreditation as an accredited user. The Commissioner is responsible for accrediting all

other types of Australian entities as accredited users, and all ADSPs (including Commonwealth, State or Territory bodies politic and Commonwealth, State or Territory bodies) under the Bill.

26. 'Australian entity' is a type of entity entitled to apply for accreditation under the Scheme. Australian entities are: a Commonwealth, State or Territory body; the Commonwealth, a State or a Territory; and Australian universities.

27. 'Australian university' is a type of Australian entity that can apply for accreditation under the Scheme. An Australian university must be registered in the Australian University provider category, under the *Tertiary Education Quality and Standards Agency Act 2011* (Cth) and be established by or under a law of the Commonwealth, a State or a Territory.

28. 'Biometric data' means any data that is personal information, and that is about any measurable biological or behavioural characteristic of an individual that could be used to identify, or verify the identity of the individual. Biometric data includes facial features, fingerprints or a person's gait and voice, as well as biometric templates. This definition supports the privacy protection clauses, under which sharing of biometric data is only permitted with the express consent of the individual to whom the biometric data relates.

29. 'Commonwealth body' 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, but does not include bodies that fall within the definition of an Australian university.

30. 'Public sector data' means data lawfully collected, created or held by or on behalf of a Commonwealth body, including ADSP-enhanced data. This definition is intended to be broad, to capture all lawfully held Commonwealth government data. The definition captures 'personal information' and 'sensitive information', as defined by the *Privacy Act*, as well as other types of data, and establishes the scope of data that can be shared under the Scheme (subject to authorisations under clause 13 and other exclusions and protections).

31. 'Scheme data' means any copy of data that has been created for the purpose of being shared under the Scheme (whether or not the data has yet been shared), ADSP-enhanced data of a project, and outputs of a project. However, outputs of a project which have exited the Scheme under clause 20E are no longer scheme data. The sharing, access and use of scheme data is protected and controlled under Chapter 2.

32. 'State body' includes a department of a State, a body established for a public purpose by or under a law of a State (other than as prescribed by the rules), or the holder of statutory office appointed under a law of a State (other than as prescribed by the rules), but does not include bodies that fall within the definition of an Australian university. This definition allows the rules to prescribe bodies that will not be considered to be a State body for the purposes of accreditation.

33. 'Territory body' includes a department of a Territory, a body established for a public purpose by or under a law of a Territory (other than as prescribed by the rules), or the holder of statutory office appointed under a law of a Territory (other than as prescribed by the rules), but does not include bodies that fall within the definition of an Australian university. This definition allows the rules to prescribe bodies that will not be considered to be a Territory body for the purposes of accreditation.

34. 'Use' includes handling, storing, and providing access to data. This definition also intends to encompass the concept of 'use' under the *Privacy Act*.

Clause 10 – References to access to data

35. Clause 10 defines how references to access to data in the Bill should be interpreted. The concept is especially relevant to the penalty provisions set out in clauses 14 and 14A.

36. Subclause 10(1) outlines that a reference to an entity providing access to data includes where an entity provides another entity with data access, and where the entity releases the data by providing open access; for example, where the entity publishes the data on a website. The concept of providing access to data is intended to be interpreted broadly.

37. Subclause 10(2) introduces the expression of 'share' which refers to circumstances where data custodians provide accredited entities with controlled access to data under the Scheme.

38. Subclause 10(3) clarifies that the entity which provides access to data is taken to retain a copy of the data, and the entity to which access is provided is taken to collect a copy of the data. This means that for the purposes of the Scheme, having access to data is the equivalent of collecting data notwithstanding that the data may not be physically received or stored by an entity (for example, in circumstances where a user accesses data through an ADSP intermediary providing a secure access service).

Clause 11 – Entity definitions

39. Clause 11 identifies and defines the key roles entities have in the Scheme.

40. Subclause 11(1) defines the term 'data scheme entities' to mean data custodians of public sector data and accredited entities, defined respectively in subclauses (2) and (4).

41. Subclause 11(2) defines which entities are considered 'data custodians' for the purpose of the Scheme. Data custodians are Commonwealth bodies (refer clause 9 definition) that are not excluded entities under subclause 11(3), that control public sector data (whether alone or jointly with another entity), including by having the right to deal with that data, or have become a data custodian of output of a project in accordance with clause 20F.

42. For the purposes of subparagraph 11(2)(c)(i), control by way of 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.

43. A right to deal with data described in subparagraph 11(2)(c)(i) 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 or letters of exchange.

44. Subparagraph 11(2)(c)(ii) works with subclause 19(4) and clause 20F to allow a data sharing agreement to designate one of the Commonwealth parties as data custodian of each type of scheme data (such as any outputs, shared data, or ADSP-enhanced data) generated under the agreement. This approach is consistent with how custodian rights may arise outside of the Scheme, and provides flexibility so parties can set and streamline their sharing arrangements in a manner that does not compromise the original data custodian's control of the data. In most cases, the entity that collects output of a project to fulfil its legislative functions or purposes (typically a Commonwealth department or agency) will be the custodian of that data.

45. Subclause 11(2A) provides that if a data custodian shares the data with an intermediary under clause 13 as part of a project, the data custodian is taken also to be the data custodian of any ADSP-enhanced data of the project, such as a de-identified dataset created by an ADSP (refer clause 11A). This subclause ensures that the sharing of any ADSP-enhanced data must be done in accordance with clause 13 in order to be authorised.

46. The definition of data custodian must be read with paragraph 13(2)(b), which qualifies custodians' capacity to share data under the Scheme where there are multiple data custodians of the data. In particular, where there are multiple data custodians of data for the purposes of the Scheme, such as where different departments use the same data for different functions, they must each give authority to share the data for the sharing to be authorised under clause 13.

47. Certain Commonwealth bodies are excluded from being data custodians for the purposes of the Scheme, as provided by paragraph 11(2)(b) and listed in subclause 11(3).

48. Subclause 11(3) lists entities that are excluded from the Scheme. Excluded entities cannot be data custodians, and are unable to seek accreditation (refer Part 5.2). As excluded entities are not Scheme entities, they are not able to use the authorisations and are not subject to the responsibilities and regulatory provisions of this Bill. Commonwealth intelligence and law enforcement entities such as the Australian Federal Police, the Australian Secret Intelligence Service, the Australian Security Intelligence Organisation, and the Australian Signals Directorate 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. The Commissioner and any APS employee made available to the Commissioner under clause 47 is also excluded as they have oversight of the Scheme. Data originating with, held by or received from excluded entities may not be shared under the Bill (refer paragraph 17(2)(a)).

49. Subclause 11(4) defines accredited entities. The term accredited entity refers to two kinds of Scheme entities: accredited users and accredited data service providers that are accredited under the accreditation framework (refer Part 5.2).

50. Accredited entities are authorised by clauses 13A and 13B to collect and use data shared with them under clause 13, within the parameters set by their data sharing agreement (refer clause 18 and Chapter 2).

51. Accredited users are entities that are capable of securely and appropriately handling data shared with them under the Scheme in a way that minimises risk of unauthorised access or use and satisfy the relevant accreditation criteria under Part 5.2.

52. ADSPs are expert intermediaries in the sharing process that provide data services (such as complex integration, secure access, and de-identification) which support sharing by data custodians with accredited users. ADSPs play a crucial role in the Scheme to fill gaps in resourcing and capability that would otherwise inhibit data availability and secure use.

53. Only Australian entities, other than excluded entities (refer clause 11(3)), within the definition in clause 9 may apply for accreditation under clause 74. This means that only Commonwealth, State, and Territory bodies politic, Commonwealth, State and Territory bodies, and Australian universities can participate in the Scheme.

54. To become accredited, applicant entities are assessed by the relevant accreditation authority to ensure they have appropriate capabilities and governance structures to participate safely in the Scheme (refer clauses 74 and 77). The accreditation authority may be the Minister or the Commissioner depending on the type of entity seeking accreditation and the type of accreditation sought under the Scheme. The Minister is responsible for the accreditation of entities who are Commonwealth, State or Territory bodies politic or Commonwealth, State or Territory bodies (within the meaning of this Bill). The Commissioner is responsible for accrediting all other types of entities, and all ADSP accreditation (including Commonwealth, State or Territory bodies) under the Bill.

55. Subclause 11(5) recognises that a Scheme entity (a data custodian, an ADSP, or an accredited user) may have different roles in a data sharing arrangement between different entities, or in a data sharing agreement with itself. In each of those capacities, the entity is taken to be a different Scheme entity and must comply with the requirements under the Bill relevant to each capacity they are participating for their actions to be authorised. This also means that a Scheme entity may enter into a data sharing agreement to which it is a party in more than one capacity in different transactions pursuant to the data sharing agreement. This subclause ensures the Scheme can accommodate different types of data flows including various exchanges of data that may be required for complex projects. 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 clauses 18 and 19).

56. The note to this subclause provides an example. The same entity may be party to the agreement in its capacity as data custodian of data to be shared and in its capacity as the accredited entity with which the data is shared.

Clause 11A – The data sharing project

57. Clause 11A relates to concepts and terms used that form a 'data sharing project'. The data sharing project is a key concept, as the sharing, collection and use of data must be part of a data sharing project that is for one or more of the defined data sharing purposes in order to be authorised under the Scheme.

58. Subclause 11A(1) describes the mandatory elements of a 'project', which involves a 'sharer' (a data custodian) sharing data with a 'user' (an accredited user), either directly or through an 'intermediary' (an ADSP). The user then collects and uses the 'output' of the project. This subclause also defines the output of a project, which is the copy of the data collected by the user or any resulting product of the user's use of the data.

59. Note 1 to subclause 11A(1) provides guidance that the sharer's authorisation to share is under clause 13, the user's authorisation to collect and use the data is under clause 13A. Note 2 to this subclause explains that a project may involve multiple sharers if multiple entities are data custodians.

60. Subclause 11A(2) expands the concept of a 'project' to include circumstances where data is being created or data services are performed in relation to the data on behalf of the sharer.

61. Subclause 11A(3) extends the definition of a project to include circumstances where the sharer shares data through an intermediary, and the intermediary collects and uses the data, which results in 'ADSP-enhanced data'. The note to this subclause provides guidance that the relevant authorisations for the sharer and intermediary to share data are under clauses 13 and 13B. The concept of ADSP-enhanced data captures, for example, data that has been de-identified by an ADSP under clause 16C.

62. Subclause 11A(4) expands the concept of a project to include the sharer's collection and use of the output or ADSP-enhanced data, which is authorised under clause 13C.

63. Subclause 11A(5) provides that multiple projects may be combined and treated as a single project in a data sharing agreement, as long as they have the same purpose(s), and the same sharer(s) and user(s).

64. Subclause 11A(6) provides for when a user subsequently shares the output of the project, as part of a later project. In such a situation, the copy retained by the user is considered to be output of the earlier project, the copy subsequently made or collected in the later project is considered output of the later project. Similarly, if an intermediary is used, the copy collected by the intermediary in the later project is considered ADSP-enhanced data of the later project.

In effect, each successive project is treated separately for the purposes of the Scheme. The note to this subclause clarifies that a data sharing agreement may allow the user to share output under clause 13 as part of a later project in accordance with clause 20D.

Chapter 2 – Authorisations

65. Chapter 2 of the Bill authorises data custodians to share public sector data with accredited users as part of a data sharing project in permitted circumstances, either directly or through an intermediary ADSP. Chapter 2 also authorises accredited users and ADSPs to collect and use public sector data in permitted circumstances. Authorisations to share, collect and use data is subject to the controls set out in this Chapter.

66. Key requirements to share, collect and use data are specified in clauses 13 to 13C, and expanded upon in subsequent clauses. Where these requirements are met, and sharing is not otherwise barred under clause 17, this Bill overrides other laws to the extent that they restrict sharing (refer clause 23).

67. As Data custodians retain discretion regarding whether to use this authorisation to share public sector data, there is no duty to share and other pathways for sharing data outside of the Scheme continue to operate.

68. Scheme entities must comply with legislative instruments (refer clause 26), and have regard to the Commissioner's guidelines (refer clause 27) when engaging with the Scheme.

Part 2.1 – Introduction

Clause 12 – Simplified outline of this Chapter

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

Part 2.2 – Authorisations

Clause 13 – Authorisation for data custodian to share public sector data

70. Clause 13 outlines the authorisation for a sharer (a data custodian) to share public sector data. Public sector data may be shared directly with an accredited user, or with the accredited user through an intermediary (an ADSP).

71. Subclause 13(1) specifies the requirements that must be met before a sharer is authorised to share data. Paragraph 13(1)(a) refers to the constitutional requirements in subclause 13(4) and paragraph 13(1)(b) refers to the data custodian requirements in subclause 13(2). Thus, a Commonwealth body has no authorisation to share data under the Scheme unless all of the requirements in subclauses 13(1) and 13(2) are satisfied, and the constitutional requirements in subclause 13(4) are met. Subclause 13(1) requires all sharing to be covered by a registered data sharing agreement that complies with all of the requirements for data sharing agreements in the Bill, and is registered by the Commissioner in accordance with the Bill. The sharing must be in accordance with that agreement. The sharing can only occur if the sharer is satisfied that the sharing will be consistent with the data sharing principles (what is required in order to be satisfied about this matter is explained in subclause 16(11)). Data may only be shared with an accredited user whose accreditation is not suspended. If personal information is shared, the accredited user must have privacy coverage in relation to the personal information (refer clause 16E). Where data is shared through an intermediary, the intermediary must be an ADSP

whose accreditation is not suspended, and if personal information is being shared, the ADSP must meet the privacy coverage condition in clause 16E.

72. Subclause 13(2) sets out further requirements that must be satisfied in relation to the sharing of data. The sharer has to be the data custodian of the data to be shared and the data must be public sector data. The term 'data custodian' is defined in clause 11. The term 'public sector data' is defined in clause 9 to mean data lawfully collected, created or held by or on behalf of a Commonwealth body, and includes ADSP-enhanced data. Paragraph 13(2)(b) requires authority to be given by all data custodians if the sharer is not the only data custodian of the data. Where an ADSP develops an integrated dataset as part of a project and two or more Commonwealth bodies are the data custodians of the integrated dataset, all of these data custodians need to provide authority to share the integrated dataset with an accredited user (this is explained in the note below subclause 13(2)).

73. Data cannot be shared if the sharing of that data is barred by clause 17.

74. The privacy requirements in clauses 16A and 16B must be met, and the requirements in clauses 16C and 16D about data services also need to be met. Where personal information is to be shared, clause 16B requires that only the minimum amount of personal information necessary for the project is shared. Paragraph 13(2)(e) imposes a similar requirement to minimise the sharing of data in relation to data that is not personal information.

75. Subclause 13(3) supplements paragraph 13(2)(b) by clarifying the manner in which authority must be given where there are multiple data custodians of shared data. Only an authorised officer of a data custodian may provide authority on behalf of the data custodian, unless one data custodian of a dataset has authorised another data custodian of that dataset to provide authority on its behalf as its agent – in which case an authorised officer of the agent data custodian may provide authority to share on behalf of the principal data custodian.

76. Data may only be shared under the Scheme if one or more of the paragraphs in subclause 13(4) apply to the sharing. Where one or more paragraphs apply, the sharing will be supported by the Commonwealth's powers to make laws under the Constitution. Normally, where data is to be shared under the Scheme, the data will be shared by electronic means (for example, secure system to system communications) and so paragraph 13(4)(e) will apply.

Clause 13A – Authorisation for accredited user to collect and use data

77. Clause 13A provides the authorisation for an accredited user to collect and use data shared with it by a data custodian under clause 13 (including in some cases where data was purportedly shared with it under clause 13, but one or more of the requirements in clause 13 were not met). The accredited user is authorised to collect and use output in accordance with a registered data sharing agreement that is in effect and that meets all of the requirements of the Bill if:

- the user is satisfied that the project is consistent with the data sharing principles (what is required in order to be satisfied about this matter is explained in subclause 16(11));
- the user is an accredited user, and the user's accreditation is not suspended; and
- if the shared data includes personal information, the accredited user has privacy coverage in relation to the personal information (as required by clause 16E).

78. In some cases, if a data custodian shares data purportedly under clause 13, but all the requirements of clause 13 are not fully met and so the sharing is not authorised, the accredited user could not be expected to know that. For example, an accredited user would not normally be expected to know that sharing is barred under subclause 17(3) because the sharing contravenes an agreement to which the data custodian is a party. Where an accredited user does

not actually know, and could not be reasonably expected to know, that a purported sharing under clause 13 was invalid, the accredited user is still authorised to collect and use data under clause 13A if the requirements in clause 13A are otherwise met. However, if the accredited user becomes aware that not all of the requirements in clause 13 relating to the sharing were met, or becomes aware of circumstances that mean it would be reasonable for the accredited user to know that, the accredited user has no further authorisation under clause 13A to use output. The term 'output' is defined in clause 11A. The data collected by the accredited user, and any data that is the result or product of the accredited user's use of the data, is 'output'.

Clause 13B – Authorisation for ADSP to act as intermediary

79. Clause 13B provides the authorisation for an ADSP to collect and use data shared with it by a data custodian under clause 13 (including in some cases where data was purportedly shared with it under clause 13, but one or more of the requirements in clause 13 were not met). The ADSP is authorised to collect and use ADSP-enhanced data in accordance with a registered data sharing agreement that is in effect and that meets all of the requirements of the Bill if:

    - the ADSP is satisfied that the project is consistent with the data sharing principles (what is required in order to be satisfied about this matter is explained in subclause 16(11));
    - the ADSP's accreditation is not suspended; and
    - if the shared data includes personal information, the ADSP has privacy coverage in relation to the personal information (as required by clause 16E).

80. In some cases, if a data custodian shares data purportedly under clause 13, but all the requirements of clause 13 are not fully met and so the sharing is not authorised, the ADSP could not be expected to know that. For example, an ADSP would not normally be expected to know that sharing is barred under subclause 17(3) because the sharing contravenes an agreement to which the data custodian is a party. Where an ADSP does not actually know, and could not be reasonably expected to know, that a purported sharing under clause 13 was invalid, the ADSP is still authorised to collect and use data under clause 13B if the requirements in clause 13B are met. However, if the ADSP becomes aware that not all of the requirements in clause 13 relating to the sharing were met, or becomes aware of circumstances that mean it would be reasonable for the ADSP to know that, the ADSP has no further authorisation under clause 13B to use ADSP-enhanced data. The term 'ADSP-enhanced data' is defined in clause 11A. The data collected by the ADSP, and any data that is the result or product of the ADSP's use of the data, is 'ADSP-enhanced data'.

Clause 13C – Authorisation for data custodian to collect and use submitted data

81. Clause 20A permits a data sharing agreement for a project to allow (or require) an ADSP to provide ADSP-enhanced data, or for an accredited user to provide output, to the data custodian to enable the data custodian to confirm that requirements in the data sharing agreement have been met. The provision of ADSP-enhanced data or output to the data custodian as permitted by clause 20A is referred to as the 'submission' of data (refer subclause 20A(3)).

82. Where ADSP-enhanced data, or output, is submitted to the data custodian, the ADSP-enhanced data or output remains scheme data and may only be collected or used by the data custodian as authorised by clause 13C. Clause 13C provides the data custodian with an authorisation to collect and use submitted data if the collection and use is in accordance with a registered data sharing agreement that is current and that meets the requirements of the Bill.

83. Clause 20A only permits a data sharing agreement to allow ADSP-enhanced data to be submitted to the data custodian for the purpose of ensuring the ADSP-enhanced data is as

agreed in the data sharing agreement, and for output to be submitted to the data custodian for the purpose of ensuring the output is as agreed in the data sharing agreement. This limitation on the purpose for which data custodians may use submitted data must be reflected in the data sharing agreement, and this limitation will therefore affect the breadth of the authorisation provided to data custodians by clause 13C in relation to submitted data.

84. Where ADSP-enhanced data is submitted to the data custodian, it remains scheme data and the collection and use of the data by the data custodian is controlled by the Scheme (refer clause 20A).

Clause 14 – Penalties for unauthorised sharing

85. Subclause 14(1) provides for a civil penalty to apply if an entity provides access to data to another entity purportedly under clause 13, but the sharing is not authorised under clause 13 (for example, because one of the requirements in subclause 13(1) was not satisfied). Subclause 14(3) creates an offence for this conduct if it can be proved that the entity was reckless as to whether the provision of access to the data was authorised by clause 13. In some cases, where the data purportedly shared under clause 13 is protected by secrecy provisions in other Commonwealth legislation, the purported sharing may contravene the other legislation because clause 23 will not apply.

86. The circumstances where the conduct of an individual or a body corporate may be attributed to an entity for the purposes of clause 14 are set out in clause 125A (in relation to a civil penalty) and clause 125B (in relation to an offence). Subclause 125A(2) establishes a due diligence defence for government entities (as defined in subclause 125A(4)) in relation to civil penalty provisions under the Bill, including the civil penalty in subclause 14(1).

87. Individuals and bodies corporate involved in the provision of access to data under, or purportedly under, clause 13 may also contravene a civil penalty provision or commit an offence.

88. Subclause 14(2) provides for a civil penalty to apply if:

- an individual in a designated relationship with entity A (see clause 123), or a body corporate with an approved contract with entity A (see clause 123) uses data by providing access to the data to entity B;
- the provision of access is purportedly sharing by entity A to entity B under clause 13; and
- the use of the data by the individual was not authorised (either because clause 124 does not extend entity A's authorisation to the individual or the body corporate, or because the purported sharing by entity A is not authorised under clause 13).

89. Subclause 14(4) creates an offence for this conduct if it can be proved that the individual or the body corporate (as the case requires) was reckless whether the use of the data was authorised by the Bill.

90. An individual may contravene the civil penalty provision in subclause 14(2), or commit the offence in subclause 14(4), irrespective of whether they were acting within the scope of their designation (actual or apparent).

91. A body corporate may contravene the civil penalty provision in subclause 14(2), or commit the offence in subclause 14(4), irrespective of whether it was acting within the scope of their contract (actual or apparent).

92. Where a designated individual of a 'government entity' (as defined in subclause 125A(4)) is acting within the scope of their designation and their conduct is attributed to the government

entity, subclause 125A(3) provides that the individual is not personally liable for a contravention of a civil penalty provision.

93. Subclauses 14(1) and 14(2) provide for civil penalties of 300 penalty units. The offences in subclauses 14(3) and 14(4) provide for a penalty of imprisonment for five years, 300 penalty units, or both.

Clause 14A – Penalties for unauthorised collection or use

94. Subclause 14A(1) provides for a civil penalty to apply if an entity collects and uses data, the data is ADSP-enhanced data or output of a project involving the sharing of the data with the entity under (or purportedly under) clause 13 and the collection and use is not authorised by the Bill.

95. Subclause 14A(4) creates an offence for this conduct if it can be proved that the entity was reckless whether the collection or use of the ADSP-enhanced data or output (as the case requires) was authorised by the Bill. In some cases, where the data collected and used by the entity is protected by secrecy provisions in other Commonwealth legislation, the collection and use may contravene the other legislation, because clause 23 will not apply.

96. Individuals and bodies corporate who use ADSP-enhanced data, or output, may also contravene a civil penalty provision or commit an offence.

97. Subclause 14A(3) provides for a civil penalty to apply if:

- an individual in a designated relationship with an entity (see clause 123), or body corporate with an approved contract with the entity (see clause 123) uses data that is ADSP-enhanced data or output of a project that involves the sharing of data with the entity under (or purportedly under) clause 13; and
- the use of the ADSP-enhanced data or output by the individual was not authorised by the Bill (either because clause 124 does not extend the entity's authorisation to the individual or the body corporate, or because the use did not fall within the authorisation to the entity provided by the Bill).

98. Subclause 14A(5) creates an offence for this conduct if it can be proved that the individual or the body corporate (as the case requires) was reckless as to whether the use of the data was authorised by the Bill.

99. Subclause 14A(6) creates a defence for entities, individuals and bodies corporate if it can be established that the data collected and used was a copy of ADSP-enhanced data or output that has exited the Scheme (refer clause 20E), or data derived from such a copy. The defendant bears an evidential burden of proof to establish that subclause 14A(6) applies. An example of how subclause 14A(6) may apply is as follows. A data sharing agreement may permit an accredited user to release specified output in certain circumstances (refer clause 20C). If an accredited user releases a copy of specified output by putting a copy on the internet, that copy would 'exit' the Scheme, but the copy of the specified output retained by the accredited user would remain scheme data. In proceedings against the accredited user seeking an order for a civil penalty for unauthorised use of a copy of the specified output, subclause 14A(6) would apply if the accredited user could bring forward evidence that the relevant conduct was use of a copy of the specified output that had exited the Scheme (for example, that it used a copy of the specified output downloaded from the internet).

100. Where a copy of ADSP-enhanced data, or output, is submitted to the data custodian under a data sharing agreement for a project (refer clause 20A), the data custodian is only authorised to collect and use the submitted data as permitted by clause 13C.

101. Subclause 14A(7) provides for a civil penalty to apply if a data custodian collects and uses submitted data and the collection and use is not authorised by the Bill.

102. Subclause 14A(9) creates an offence for this conduct if it can be proved that the data custodian was reckless as to whether the collection or use of the submitted data was authorised by the Bill.

103. Individuals and bodies corporate who use submitted data may also contravene a civil penalty provision or commit an offence.

104. Subclause 14A(8) provides for a civil penalty to apply if:

- an individual in a designated relationship with an entity (see clause 123), or body corporate with an approved contract with the entity (see clause 123) uses submitted data; and
- the use of the submitted data by the individual was not authorised by the Bill (either because clause 124 does not extend the entity's authorisation to the individual or the body corporate, or because the use did not fall within the authorisation to the entity provided by the Bill).

105. Subclause 14A(10) creates an offence for this conduct if it can be proved that the individual or the body corporate (as the case requires) was reckless as to whether the use of the submitted data was authorised by the Bill.

106. The circumstances where the conduct of an individual or a body corporate may be attributed to an entity for the purposes of clause 14A are set out in clause 125A (in relation to a civil penalty) and clause 125B (in relation to an offence). Subclause 125A(2) establishes a due diligence defence for government entities (as defined in subclause 125A(4)) in relation to civil penalty provisions under the Bill, including the civil penalties in clause 14A.

107. Where a designated individual of a government entity (as defined in subclause 125A(4)) is acting within the scope of their designation and their conduct is attributed to the government entity, subclause 125A(3) provides that the individual is not personally liable for a contravention of a civil penalty provision.

108. An individual may contravene a civil penalty provision in clause 14A, or commit an offence in clause 14A, irrespective of whether they were acting within the scope of their designation (actual or apparent).

109. A body corporate may contravene a civil penalty provision in clause 14A, or commit an offence in clause 14A, irrespective of whether it was acting within the scope of their contract (actual or apparent).

110. The civil penalty provisions in clause 14A generally provide for civil penalties of 300 penalty units. However, a penalty of 600 penalty units applies to a contravention of subclause 14A(1) if subclause 14A(2) applies. Subclause 14A(2) will apply if a court considers that a contravention of subclause 14A(1) is serious, taking account of the sensitivity of the data collected or used (for example, if the data is personal information), the consequences of the contravention (for example, whether the security of the personal information of individuals has been compromised) and the level of care taken by the entity (for example, whether it provided training to its employees about its obligations under the Scheme).

111. The offences in clause 14A provide for a penalty of imprisonment for five years, 300 penalty units, or both.

112. Clause 14A(11) confirms that the civil penalties and offences in clause 14A apply notwithstanding any other legislation, including legislation relating to certain data that may be passed under this Bill. The civil penalties and offences in clause 14 also apply notwithstanding

any other legislation, including legislation relating to certain data that may be passed under this Bill.

113. Clause 14A(12) confirms that the civil penalties and offences in clause 14A apply, notwithstanding that a permitted situation or a permitted health situation exists for the purposes of the *Privacy Act*. That is, the fact that a particular use of data may be authorised in some circumstances under the *Privacy Act* does not affect whether use of the data is authorised, or not authorised, under this Bill. The same position applies in relation to civil penalties and offences in clause 14.

Part 2.3 – Data sharing purposes and principles

Clause 15 – Data sharing purposes

114. A data sharing agreement must specify the data sharing purpose or purposes of a project and (except as allowed in accordance with clause 20D) prohibit the accredited user from using output for any other purpose or a precluded purpose (refer subclause 19(6)). The authorisations in clauses 13, 13A, 13B and 13C only have effect in relation to the sharing, collection and use of data that is in accordance with a registered data sharing agreement that is in effect and that meets the requirements in the Bill.

115. Subclause 15(1) defines the term 'data sharing purposes'. There are three data sharing purposes: the delivery of government services; informing government policy and programs; and research and development. The reference to 'government policy and programs' are the policies and programs of the Australian Government and the governments of the States and Territories.

116. The term 'delivery of government services' is defined in subclause 15(1A) to mean the provision of the following services by the Australian Government, or by a government of a State or a Territory:

- the provision of information (such as advice that an individual may be eligible to receive a benefit, or a reminder that action on the part of an individual is required);
- the provision of a service that not a service relating to a payment, entitlement or benefit (for example, a service to provide assistance to a person to help restore their property after a flood, or to provide counselling);
- determining eligibility for a payment, entitlement or benefit (this includes a benefit payable under legislation, and a grant payment); and
- paying a payment, entitlement or benefit.

117. The note under subclause 15(1A) makes it clear that using data to make a decision whether a person is eligible for a government benefit and, if so, paying that benefit, are examples of the delivery of government services. Determining eligibility for a payment before the payment is made is not a precluded purpose.

118. Subclauses 15(2), 15(3) and 15(4) define 'precluded purposes' and an 'enforcement related purpose'. Subclause 15(2) provides that an enforcement related purpose, a purpose that relates to, or prejudices national security or a purpose prescribed by the rules are all precluded purposes. Rules are disallowable legislative instruments made by the Minister under clause 133. Rules may expand what categories are precluded purposes (and hence limit the circumstances where data may be shared under the Scheme).

119. Enforcement related purposes are defined in subclause 15(3) to include the detection, investigation and response to offences, contravention of laws punishable by pecuniary penalties and acts or practices detrimental to the public revenue (such as claiming benefits for which

there is no entitlement). The note under subclause 15(3) confirms that the use of data to verify that a payment made previously was correctly made is an enforcement related purpose. Using data to identify individuals for compliance review or compliance activity is also an enforcement related purpose.

120. Subclause 15(4) confirms that a data sharing project for a data sharing purpose (such as informing government policy and programs, or research and development) is not for a precluded purpose where it deals with conduct punishable by criminal or civil penalties, or with acts or practices detrimental to the public revenue, in a general way. For example, a project to research trends in criminal behaviour in relation to Australian Government programs, where the research does not relate to any particular individuals, would not be for a precluded purpose.

121. In some cases an accredited user that is also a Commonwealth body may wish to develop a data asset that can subsequently be shared under the Scheme. At the time the accredited user is developing the data asset, the accredited used may not have specific future projects in mind that may utilise the data asset. Subclauses 15(5) and 15(6) provide that a project to prepare data for a later project, that will be for one or more of the data sharing purposes is taken to be for that, or those data sharing purposes.

Clause 16 – Data sharing principles

122. Clause 16 defines five risk management principles as the 'data sharing principles'. These are otherwise known as the 'five safes'.

123. Subclauses 16(1) and 16(2) define the 'project principle'. This principle is that the project is an appropriate project or program. This principle includes that the project can reasonably be expected to serve the public interest, and the entities involved in the project observe appropriate ethics processes.

124. Subclauses 16(3) and 16(4) define the 'people principle'. This principle is that data is only made available to appropriate persons. This is considered at the accredited entity level (that is, for the accredited user and the ADSP, if any) and at the level of designated individuals (refer clause 123), and bodies corporate who may be contracted to, the accredited entity or entities.

125. Subclauses 16(5) and 16(6) define the 'setting principle. This principle is that data is only shared, collected and used in an appropriately controlled environment. This principle considers the means by which data is to be shared and the security standards to apply in relation to the collection and use of data.

126. Subclauses 16(7) and 16(8) define the 'data principle'. This principle is that appropriate protections are applied to shared data. The principle includes a requirement that only data reasonably necessary to achieve the data sharing purpose or purposes is shared. Clause 13(2) and clause 16B also limit the amount of data that may be shared as part of a project.

127. Subclauses 16(9) and 16(10) define the 'output principle'. This principle is that the only output of a project is the final output (as agreed by the parties involved in the project) and output reasonably necessary or incidental to the creation of this output. The final output must only contain the data reasonably necessary to achieve the applicable data sharing purpose or purposes.

128. Subclause 126(2A) requires the Commissioner to make a data sharing code about the data sharing principles. The data code is a disallowable legislative instrument binding on Scheme entities.

129. The authorisations in clauses 13, 13A and 13B require the authorised entity to be satisfied that the project is consistent with the data sharing principles. What is required to meet this

requirement is explained in subclause 16(11). To be so satisfied, the entity must be satisfied that it has applied each of the five data sharing principles to the project in such a way that, viewed as a whole, the risks associated with the sharing, collection and use of data under the Scheme as part of the project are appropriately mitigated. This means that if some of the data sharing principles are applied in a way that adequately manages the risks of the project, the remaining data sharing principles may require fewer controls to be put in place.

130. Clause 19(7) requires a data sharing agreement for a project to specify how the project will be consistent with the data sharing principles, and the actions that will be taken by the parties to the agreement to give effect to the principles.

Part 2.4 – Privacy protections

Clause 16A – General privacy protections

131. Clause 16A provides for three privacy protections that apply to all projects, irrespective of the data sharing purpose.

132. Subclause 16A(1) prohibits the sharing of biometric data under the Scheme unless the individual to whom the biometric data relates expressly consents to the sharing. The term 'biometric data' is defined in clause 9. Because information cannot be biometric data unless it is also personal information, all biometric data is information about an identified individual. Consent cannot be inferred for the purpose of subclause 16A(1).

133. Where data shared as part of a project includes personal information, subclause 16A(2) requires the data sharing agreement covering the project to prohibit the accredited user from storing or accessing, or providing access to output outside of Australia, and to prohibit the ADSP (if there is an ADSP involved as part of the project) from storing or accessing, or providing access to ADSP-enhanced data outside of Australia. Any use of output (including the handling or storage of output) by the accredited user contrary to this prohibition would not be authorised by clause 13A and could lead to penalties under clause 14A. Any use of ADSP-enhanced data (including the handling or storage of ADSP-enhanced data) by the ADSP contrary to this prohibition would not be authorised by clause 13B and could lead to penalties under clause 14A. Permitting an individual in a foreign country to log into a system operating on a server in Australia, to access personal information stored in Australia, would be prohibited by the data sharing agreement provision required by subclause 16A(2).

134. For projects where the data sharing purpose is informing government policy and programs, or research and development, de-identified data rather than personal information will be shared whenever possible. Where de-identified data is shared as part of a project, subclause 16A(3) requires that the data sharing agreement covering the project must prohibit the accredited user from taking any action that may have the result that the data ceases to be de-identified. Any use of output by the accredited user contrary to this prohibition would not be authorised by clause 13A and could lead to penalties under clause 14A. An action by the accredited user that may have the result that the data ceases to be de-identified would be prohibited by the data sharing agreement provision required by subclause 16A(3), even if the action was not done with the intention of producing data that is no longer de-identified, and even if the action did not in fact produce data that was no longer de-identified.

Clause 16B – Purpose-specific privacy protections

135. Clause 16B imposes different restrictions on the sharing of personal information as part of a project, depending on the data sharing purpose of the project.

Delivery of government services

136. Subclauses 16B(1) and 16B(2) relate to projects for the data sharing purpose of delivery of government services.

137. Generally, personal information may only be shared under such projects with the consent of the individuals to whom the personal information relates (paragraph 16B(1)(a)(ii)). However, personal information may be shared without the consent of the individual to whom the information relates in two circumstances:

- in order to deliver a service to the individual that is the provision of information, or a service other than determining eligibility for a payment, entitlement or benefit, or the making of a payment (subparagraph 16B(1)(a)(i)); and
- where the sharing would be a disclosure authorised under Part VIA of the *Privacy Act* (dealing with personal information in emergencies and disasters, refer subparagraph16B(1)(a)(iii)).

138. Thus, subject to other restrictions in subclauses 16B(1) and 16B(2) (see below), the personal information of an individual could be shared with an accredited user to enable the accredited user to provide the individual with information about a benefit they may be entitled to, or to provide a counselling service. It would not be possible for the accredited user to use the shared personal information to determine that the individual was entitled to a statutory benefit unless the individual had consented to the sharing of their personal information.

139. Declarations under section 80J of the *Privacy Act* may be made if an emergency or disaster of national significance has occurred.

140. Paragraph 16B(1)(b) prevents the sharing of personal information for a project for the government service delivery data sharing purpose unless the data sharing agreement for the project identifies the service or services to be delivered by the accredited user. This identification would need to cover both the program to which the delivery of services relates, and the nature of the services to be provided (by reference to the definition of 'delivery of government services' in subclause 15(1A)).

141. Paragraph 16B(1)(c) prevents the sharing of personal information for a project for the government service delivery data sharing purpose unless only the minimum amount of personal information necessary to properly deliver the service is shared. Paragraph 126(2C)(b) requires the Commissioner to make a data code on the principles to be applied by data custodians when determining whether it is necessary to share personal information to properly deliver a government service. Data codes are disallowable legislative instruments that are binding on data custodians.

142. Clause 20E, dealing with the exit of personal information from the Scheme, permits an individual to expressly consent to both the sharing of their personal information with an accredited user, and the accredited user's use of that personal information without the use constraints imposed by the Scheme. Where a project permits personal information to exit the Scheme under subclause 20E(4), subclause 16B(2) requires that the data sharing agreement for the project specify this.

Informing government policy and programs, and research and development

143. Subclause 16B(3) provides that, where the data sharing purpose of a project is informing government policy and programs, or research and development, generally the shared data cannot include an individual's personal information unless both the individual consents to the sharing and only the minimum amount of information necessary for the project to proceed is shared.

144. However, subclause 16B(3) also permits the sharing of personal information about an individual without the individual's consent if:

- the project cannot proceed without the personal information;
- the public interest to be served by the project justifies the sharing of the personal information without consent;
- only the minimum amount of personal information necessary for the project to proceed is shared; and
- at least one of the 'permitted circumstances' in subclause 16B(4) (where the project is for the purpose of informing government policy and programs) or subclause 16B(5) (where the project is for the purpose of research and development) applies.

145. While it is a matter for the judgment of the data custodian whether the public interest to be served by the project justifies the sharing of the personal information without consent, paragraph 126(2C)(b) requires the Commissioner to make a data code on the principles to be applied by data custodians when determining the circumstances, or categories of circumstances, where the public interest to be served by a project justifies the sharing of personal information without consent. Data codes are disallowable legislative instruments that are binding on data custodians.

146. Subclauses 16B(4) and 16B(5) provide that the following are 'permitted circumstances' for projects for the purpose of informing government policy and programs, and projects for the purpose of research and development:

- it is unreasonable or impractical to seek the individual's consent;
- the data is to be collected and used in the course of medical research and in accordance with guidelines made under subsection 95(1) of the *Privacy Act;*
- the sharing is with an ADSP to enable the ADSP to prepare data for sharing with the accredited user that does not include personal information (for example, the ADSP is performing a de-identification data service in relation to the data shared by the data custodian);
- the sharing is authorised under Part VIA of the *Privacy Act* (dealing with personal information in emergencies and disasters);
- the sharing is ADSP-controlled access.

147. A note below subclause 16B(4) confirms that it is not unreasonable or impractical to seek the consent of individuals to the sharing of their personal information merely because a very large number of individuals would need to contacted. Paragraph 126(2C)(a) requires the Commissioner to make a data code on the circumstances in which it is unreasonable or impracticable to seek the consent of individuals. Data codes are disallowable legislative instruments that are binding on data custodians. Where, as part of a project the personal information of individuals is shared without their consent on the basis that it is unreasonable or impractical to seek the consent of the individuals, subclause 16B(7) requires the data sharing agreement for the project to include a statement about this circumstance that includes an explanation as to why the data custodian thinks it would be unreasonable or impractical to seek consent. Subclause 130(2) requires this statement to be included on the publicly accessible part of the register of data sharing agreements.

148. Subclause 16B(6) defines the term 'ADSP-controlled access', which is a service within the secure access data service. ADSP-controlled access occurs where, rather than sharing data with an accredited user so that the accredited user stores the shared data in its systems, the data is

stored on the ADSP's systems and particular designated individuals with appropriate training are provided with access to the ADSP's systems to use the shared data (which is output). The ADSP is able to put a number of controls in place in this environment to significantly reduce the risk that the accredited user is able to identify any individual.

149. Where a project is for the purpose of informing government policies and programs, paragraphs 16B(4)(e) and 16B(4)(f) provide for additional 'permitted circumstances' that permit the sharing of personal information without consent, if the other requirements in subclause 16B(3) are satisfied. Paragraph 16B(4)(e) permits the sharing of personal information without consent with another Commonwealth body (other than a Commonwealth body excluded from this paragraph by the rules) but only if the final output of the project only includes de-identified data. For example, Commonwealth department A could share personal information without consent to enable Commonwealth department B to match the shared data with its own data, so long as the final output was a report that did not include any personal information about individuals. The report could be used to inform government policy. In this example, department B would not be able to use the shared data for any other purpose, other than the creation of the report.

150. Paragraph 16B(4)(f) permits the sharing of personal information without consent if the disclosure of the personal information would be authorised under Part VIA of the *Privacy Act*. Declarations under section 80J of the *Privacy Act* may be made if an emergency or disaster of national significance has occurred.

151. Subclause 16B(8) applies if, as part of a project where the data sharing purpose is informing government policy and programs, or research and development, personal information is shared without consent. In these circumstances, the data sharing agreement for the project must include a statement setting out why the sharing of the personal information is consistent with clause 16B. Subclause 130(2) requires this statement to be included on the publicly accessible part of the register of data sharing agreements.

Clause 16C – Project involving use of de-identification or secure access data services

152. Clause 16C sets out requirements for projects that involve the use of a 'de-identification data service' or a 'secure access data service'. The clause also includes definitions for these two data services (refer subclauses 16C(3) and 16C(4)). These data services are two of the three types of services that an ADSP can provide under the Scheme. The third data service an ADSP can provide is the 'complex data integration service' (refer clause 16D).

153. Under subclauses 16C(1) and 16C(2), if the data sharing purpose of the project is informing government policy and programs, or research and development, and the project involves performing a de-identification data service or a secure access data service, there is a requirement that either a data custodian for the data to be shared under the project, or an ADSP, must perform the service. These requirements are set out in subclause 16C(2).

154. Subclause 16C(2) requires, if the facts in subclause 16C(1) are met, that the data sharing agreement covering the project must require the de-identification data service or the secure access data service to be performed by the data custodian of the data to be shared under the project, or an ADSP that is able to perform the data service. If the data custodian of the data is not an ADSP, under paragraph 16C(2)(a), the data custodian may only perform the relevant data service if the data custodian is satisfied that it has the appropriate skills and experience to perform the service. If the data custodian of the data is an ADSP, under paragraph 16C(2)(b) the data custodian may only perform the service consistently with its conditions of accreditation as an ADSP. This means that, if a data custodian who is accredited as an ADSP has a condition imposed that would prevent it from performing the data service as an ADSP, the data custodian

cannot perform the service in its capacity as a data custodian (even if it believes it has the appropriate skills and experience to perform the service). If the data services are not performed by the data custodian of the data, in accordance with paragraph 16C(2)(c), the data sharing agreement must require that an ADSP that is able to perform the service consistently with its conditions of accreditation perform the data service for the project. These requirements are safeguards that protect data shared under the Scheme.

155. Subclause 16C(3) defines 'de-identification data service' as a service to treat data that includes personal information so that the data is de-identified, using techniques that restrict the data being used in a way that would have the result that the data ceases to be de-identified. This definition frames the service as a data treatment. The service can only be performed on data that includes personal information. Once performed, the service has the effect of removing personal information from the data and includes techniques that would prevent re-identification of the data.

156. Subclause 16C(4) defines 'secure access data service' as the service of providing ADSP-controlled access, or any other service that enables an entity to access data under the control of another entity, including controls to prevent or minimise the risk of the data being misused. ADSP-controlled access is defined in subsection 16B(6). This service is about the system on which data is stored and how entities access that system. Under this service, ADSPs provide a secure system to host data and provide certain designated individuals of accredited users with controlled access to that system. This service protects data by controlling the storage of it in a secure system managed by an ADSP, and the way in which the shared data is used by the accredited user.

Clause 16D – Project involving complex data integration services

157. Clause 16D sets out requirements for projects that involve the use of a 'complex data integration service' and includes a definition for this service. Where sensitive datasets are to be integrated, this clause requires an ADSP to perform the complex data integration service, unless an individual (an authorised officer of the data custodian, or an individual authorised under subclause 137(4)) determines otherwise. This requirement is a safeguard designed to ensure data integration work involving sensitive data sets is only undertaken by an ADSP (including an ADSP that is also a data custodian of the data to be integrated as part of the project).

158. Under subclause 16D(1), if the data sharing purpose of the project is informing government policy and programs, or research and development, and the project involves performing a complex data integration service, and a decision under subclause 16D(4) has not been made, the data sharing agreement that covers the project must require the service to be performed by the data custodian of the data (if the data custodian is an ADSP) or an ADSP. This requirement is set out in subclause 16D(2).

159. Subclause 16D(2) requires, if the facts in subclause 16D(1) are met, that the data sharing agreement covering the project must require the service to be performed by either a data custodian of the data to be shared, if the data custodian is an ADSP able to perform such a service consistently with its conditions of accreditation, or an ADSP able to perform the service consistently with its conditions of accreditation. Where there is more than one data custodian of the data to be shared, the requirement in paragraph 16D(2)(a) is satisfied if any of those data custodians who is an ADSP able to perform the service undertakes the complex data integration.

160. Subclause 16D(3) defines 'complex data integration service'. A service to integrate data is a complex data integration service if two or more entities control the data being integrated, the data is at the unit or micro level, any paragraph in subclause 16D(3) applies to any of the data

to be integrated or to the integrated data and, if applicable, the data to be integrated or the integrated data has any of the characteristics prescribed by rules. Subparagraphs 16D(3)(c)(i) to 16D(3)(c)(v) set out data characteristics for consideration in relation to the data to be integrated, or to the integrated data. For example, if the data includes personal information or commercially sensitive information. The definition of 'complex data integration service' is functional and requires entities to methodically assess the data proposed to be integrated, or the hypothetical integrated data.

161. Subclause 16D(4) allows an individual prescribed by subclause 16D(5) to make a decision, so that subclause 16D(2) will not apply to the project. Under subclause 16D(4), if the individual is satisfied, having regard to the matters listed in subparagraphs 16D(4)(a) to 16D(4)(a)(i), that the risk the integration could cause substantial harm is low, subclause 16D(2) will not apply to the project. A decision made under subclause 16D(4) exempts a data custodian from having to use an ADSP, or to be an ADSP that is able to perform the complex data integration service.

162. Subclause 16D(5) provides that an authorised officer of a data custodian of the data being integrated, or an individual authorised under subclause 137(4) for the data custodian, may make a decision under subclause 16D(4).

163. Subclause 16D(6) requires the individual making a decision under subclause 16D(4) to make a written record of the decision and the reasons for the decision. This is a transparency and accountability mechanism for data custodians.

Clause 16E – Privacy coverage condition

164. Clause 13 provides that a data custodian may only share personal information with an accredited user, or through an ADSP, if the privacy coverage condition in clause 16E is met in relation to the accredited user and, if an ADSP is part of the project, the ADSP. Similarly, where a project involves the sharing of personal information, clause 13A provides that the accredited user is only authorised to collect and use output if the privacy coverage condition in clause 16E is met in relation to the accredited user. If the project involves an ADSP, clause 13B provides that the ADSP is only authorised to collect and use output if the privacy coverage condition in clause 16E is met in relation to the ADSP.

165. The privacy coverage condition in subclause 16E(1) may be satisfied in a number of different ways. Many Scheme entities will be agencies or organisations for the purposes of the *Privacy Act* and, if they are, this satisfies the privacy coverage condition. The privacy coverage condition is also met if the *Privacy Act* applies to the entity as if it were an organisation in relation to the collection and use of information as part of the project (because it is prescribed in a Regulation made under the *Privacy Act*) or if the entity is covered by a privacy law of a State or a Territory that has the three characteristics mentioned in paragraph 16E(1)(d), one of which is that the law must provide a means for an individual to seek recourse if their personal information is handled in a way that is inconsistent with the law.

166. The privacy coverage condition is also met in relation to an entity if the data sharing agreement includes an 'APP-equivalence term' that covers the entity. This is defined in clause 16E(2) to mean a provision in a data sharing agreement that prohibits the entity from collecting or using personal information in any way that would be a breach of the Australian Privacy Principles, if the entity was an organisation for the purposes of the *Privacy Act*. The enforcement of APP-equivalence terms is covered by clause 16F.

167. Generally, an act or practice of a small business that is an organisation for the purpose of the *Privacy Act* because they are a contracted service provider for a Commonwealth contract is exempt for the purposes of the *Privacy Act* if the act or practice is not for the purpose of meeting an obligation under a Commonwealth contract. Clause 16F(3) provides that an act or

practice of a small business that involves the collection or use of personal information that is ADSP-enhanced data or output is not exempt for the purposes of the *Privacy Act*, despite section 7B of that Act.

168. The Bill is intended to work with, rather than override or modify the operation of the *Privacy Act*. Clause 16E(4) confirms that, except as provided in clause 16E(3) and Part 3.3 (relating to data breach responsibilities), nothing in the Bill affects the operation of the *Privacy Act*.

Clause 16F – Compliance with APP-equivalence term

169. Where a data sharing agreement includes an APP-equivalence term, a use of ADSP-enhanced data or output that is not consistent with the APP-equivalent term would not be authorised by clause 13A or 13B (as applicable) and penalties in clause 14A may apply. However, the Information Commissioner also has power to investigate a possible breach of an APP-equivalent term and to deal with complaints about interferences with privacy that relate to a breach of an APP-equivalence term. Clause 16F provides that a contravention of an APP-equivalence term is taken to be an interference with the privacy of the individual for the purposes of the *Privacy Act*. Section 13G of the *Privacy Act*, relating to serious and repeated interferences with privacy, applies to acts or practices covered by an APP-equivalence term. The Information Commissioner may conduct assessments and investigations, deal with complaints, accept enforceable undertakings and seek injunctions in relation to conduct that contravenes an APP-equivalence term.

Part 2.5 – When sharing is barred

Clause 17 – When sharing is barred

170. Clause 13 does not authorise the sharing of public sector data if the sharing is 'barred' by clause 17.

171. Subclause 17(1) provides that, for the purposes of clause 13, the sharing of data is barred if it is barred by subclauses 17(2) to 17(6).

172. Paragraph 17(2)(a) provides that the sharing of data of barred if it is held by, originated with or was received from, an excluded entity. The term 'excluded entity' is defined in subclause 11(3).

173. Paragraph 17(2)(b) bars the sharing of operational data from AUSTRAC, the Australian Federal Police and the Department of Home Affairs. The term 'operational data' is defined in clause 9 to include information about information sources, operational activities or methods and particular past, current and future operations.

174. The sharing of data is also barred under paragraph 17(2)(c) if an excluded entity would be one of the data custodians of the data but for paragraph 11(2)(b). The definition of 'data custodian' in subclause 11(2) means that an excluded entity cannot be the data custodian of any data. For example, Agency X, an excluded entity, asks Department Y, a non-excluded entity, to create a public sector dataset from data already held by Department Y for Agency X's policy development purposes. The agreement gives Agency X and Department Y joint rights to deal with the dataset. The dataset is stored only on Department Y's systems. In this example, although Department Y is not an excluded entity and the dataset is not held by and did originated from an excluded entity (and therefore paragraph 17(2)(a) does not apply), sharing of the dataset under the Scheme would be barred under paragraph 17(2)(c), because the Agency X would also be a data custodian of this dataset if paragraph 11(2)(b) were to be disregarded.

175. Paragraph 17(3)(a) provides that sharing is barred if the sharing would contravene or infringe:

- copyright or other intellectual property rights;

- a contract or agreement to which the data custodian is party (including a memorandum of understanding that is not legally enforceable);
- a common law duty or privilege; or
- a Parliamentary privilege or immunity.

176. Where a data custodian holds data that is commercial information subject to a duty of confidence, and the sharing of that data by the data custodian would found an action by a person (other than the Commonwealth or a Commonwealth body), the sharing of that data is also barred.

177. Regulations may be made under clause 134 for the purpose of subclause 17(4). Subclause 17(4) permits the Regulations to prescribe matters by reference to provisions in other laws, instruments, data custodians, or any other circumstances which then, because of subclause 17(4), will mean that the sharing of particular data is barred. It is necessary to have a power to make Regulations so that, as new Australian Government programs are developed, if appropriate, the sharing of data relating to those programs under the Scheme can be barred quickly, without the need to pass amending legislation. Regulations made for the purpose of subclause 17(4) may only limit the types of data that may be shared under the Scheme. There is no power for Regulations (or any other legislative instruments made under the Bill) to expand the type of data that may be shared under the Scheme. Paragraph 17(4)(a) provides that if a law prescribed in the Regulations prohibits individuals of the data custodian who would be covered by the data custodian's authorisation (refer clause 124) from disclosing data, the sharing of the data by the data custodian is barred.

178. Paragraph 17(5)(a) provides that sharing is barred if the sharing would be inconsistent with Australian's obligations under international law (including under international agreements), or with Commonwealth legislation enacted to give domestic effect to such international agreements. The *Privacy Act*, and instruments made under that Act such as the *Privacy (Tax File Number) Rule 2015*, are Commonwealth legislation giving effect to international agreements. Thus, paragraph 17(5)(a) bars the sharing of any data if the sharing would be inconsistent with the *Privacy Act*.

179. Paragraph 17(5)(b) bars the sharing of any data collected from a foreign government, or an agency of a foreign government, unless the foreign government or foreign government agency agrees to the sharing. Such agreement could be given generally, or in relation to a particular project.

180. Paragraphs 17(6)(a) and 17(6)(b) bar the sharing of the particular copy of data that is being held as evidence before a court, or obtained by a tribunal, authority or other person with the power to compel documents. These paragraphs do not bar the sharing of other copies of the same data held by the data custodian.

181. Paragraph 17(6)(c) bars the sharing of data where a court or tribunal has made an order that restricts or prohibits disclosure of the data. This paragraph applies to bar the sharing of any copies of the relevant data held by the data custodian.

Part 2.6 – Data sharing agreements

Clause 18 – Data sharing agreement

182. Subclause 18(1) sets out four requirements that must be met for an agreement to be a data sharing agreement and includes three explanatory notes. To be a data sharing agreement, the agreement must relate to the sharing of public sector data, parties to the agreement must include at a minimum one data custodian and one accredited user, if there is an approved form for an

agreement, the agreement must be in that form (or in writing if there is no approved form), and any requirements set out in a data code must be met. Note 1 signposts that all data sharing agreements must also meet requirements in clause 19 and, if applicable, other provisions that impose requirements. Clause 19 sets out requirements to be met by all data sharing agreements. Clause 19 sets out details of what a data sharing agreement must include in substance.

183. Subclause 18(2) states a data sharing agreement must not be entered into by an individual on behalf of a Scheme entity unless the individual is an authorised officer of the entity, or is authorised under subclause 137(4) for the entity. Unless authorised in this way, an individual may not enter into a data sharing agreement on behalf of an entity, even if they are otherwise authorised to enter contracts or agreements on behalf of the entity. For example, an individual who is authorised by power of attorney to enter agreements on behalf of an entity would not be able to enter into a data sharing agreement, unless they were an authorised officer of the entity, or authorised under clause 137(4) for the entity. Clause 18(2) is intended to apply notwithstanding any other general provision in Commonwealth, State or Territory legislation authorising individuals, or classes of individuals, to execute agreements on behalf of the entity. Clause 18(2) does not prevent an entity executing an agreement itself. For example, an Australian university may enter into a data sharing agreement by sealing the agreement with its seal, if this is consistent with its enabling legislation.

184. Subclause 18(3) states a variation to a data sharing agreement must not be entered into by an individual on behalf of a Scheme entity unless the individual is an authorised officer of the entity, or is authorised under clause 137(4), for the entity. If an individual that is not authorised in this way purports to enter into a variation of a data sharing agreement on behalf of an entity, that variation would not be a valid variation to a registered data sharing agreement.

185. Under subclause 18(4), a data sharing agreement has no effect until the agreement is registered. Data sharing agreements must be given to the Commissioner for registration under clause 33. The Commissioner must maintain a register of data sharing agreements under clause 130. Once a data sharing agreement is registered, it may take effect in accordance with its terms.

186. Subclause 18(5) clarifies that a variation of a data sharing agreement has no effect until the variation, or the agreement as varied, is registered. Until the variation or agreement as varied is registered by the Commissioner, the original registered agreement continues to be in effect and determines what parties to the data sharing agreement are authorised to do under Part 2.2.

187. Subclause 18(6) clarifies that a data sharing agreement may also deal with matters not required under the Bill, but must not do so in a way that is inconsistent with the Scheme. For example, under clause 20F, an agreement could appoint a Commonwealth body that is not the data custodian or accredited user (that is, a third party) to be the data custodian of output of the project. A data sharing agreement may provide for matters such as funding and intellectual property rights under subclause 18(6), because dealing with these matters is not inconsistent with the requirements for data sharing agreements in the Bill. If provisions of a data sharing agreement alter the operation of other provisions of the agreement in a way that is inconsistent with requirements under the Bill, the data sharing agreement would not meet the requirements of subclause 19(6). This would mean that the agreement would not meet the requirements of the Bill for the purposes of clauses such as clause 13A.

Clause 19 – Requirements to be met by all data sharing agreements

188. Clause 19 sets out a number of requirements that must be met by all data sharing agreements (refer subclause 19A(1A)). If a data sharing agreement for the project does not meet the requirements of clause 19, a data custodian will not be authorised to share data as part of the

project under clause 13, and accredited users, ADSPs and data custodians will not be authorised to collect and use data under clauses 13A, 13B and 13C.

189. A data sharing agreement for a project must:

- identify the parties to the agreement (subclause 19(1)) – entities may be party to a data sharing agreement even if they are not the data custodian of the data to be shared with the accredited user under clause 13, and are not the ADSP for the project or the accredited user;
- describe the project and specify that this Bill applies to the project (refer subclause 19(2));
- specify the data to be shared with the accredited user (including any ADSP-enhanced data) and the agreed final output of the project (refer subclause 19(3));
- specify the data custodian or data custodians of the data to be shared under clause 13 (refer paragraph 19(4)(a));
- where a Commonwealth body that is party to the agreement is appointed as the data custodian of specific output (this Commonwealth body may be the accredited user, or another entity), specify the output and explain the appointment (refer paragraph 19(4)(b));
- specify the title of any law that the sharing of the data under clause 13 would contravene, but for the operation of clause 23 – it is not necessary to specify the particular provision or provisions of that law or those laws (refer subclause 19(5));
- specify the data sharing purpose or data sharing purposes of the project and any incidental purposes (refer paragraph 19(6)(a));
- prohibit the accredited user from using output for any purpose not specified, including any precluded purpose (refer clause 15(2)), other than in relation to sharing permitted under clause 20D (refer paragraph 19(6)(b));
- prohibit the accredited user from creating output other than the agreed final output of the project, and output that is reasonably necessary or incidental to the creation of that final output (refer subclause 19(6A));
- specify how the project will be consistent with the five data sharing principles (see clause 16), including how the parties to the agreement will give effect to the principles (for example, imposing controls on what designated individuals of the accredited user may use output) and describe how the project the will service the public interest (refer subclause 19(7));
- if an ADSP is involved in the project, specify the services to be performed by the ADSP, the circumstances where the ADSP is to share ADSP-enhanced data with the accredited user, and prohibit the ADSP from providing access to, or releasing ADSP-enhanced data in any other circumstances (except for a submission to the data custodian as permitted by clause 20A) (refer subclauses 19(8) and 19(8A);
- describe (in general terms) the use the accredited user may make of output, and prohibit the accredited user from using the output in any other way (refer paragraphs 19(9)(a) and 19(9)(b));
- prohibit the accredited user from providing access to output, or releasing output of the project except under a term of the data sharing agreement (if it includes such a term) permitted by clause 20A, 20B, 20C or 20D (refer paragraph 19(9)(c) and subclause 19(10));
- prevent the accredited entities that are parties to the agreement from doing anything inconsistent with their conditions of accreditation applying to their accreditation as an ADSP or accredited user (as applicable to their role in the project) (refer subclause 19(11));

- where the project involves the sharing of personal information, specify that subclauses 37(2) and 37(3) apply (these clauses relate to responsibility for eligible data breach notifications under the *Privacy Act*; the data sharing agreement can specify that these clauses do not apply – see subclause 37(4)) (refer subclause 19(12));
- if the parties agree that one or more of them have responsibilities in relation to data breaches that are in additional to their obligations under Part 3.3, specify those additional responsibilities (refer subclause 19(12A));
- specify when and how the agreement may be varied or terminated (refer subclause 19(13));
- specify the termination date for the agreement (which may be a calendar date, the end of a specified period or the date an event occurs), the date for regular reviews of the agreement or both (refer subclause 19(14));
- specify how scheme data (refer clause 9) covered by the agreement must be handled when the agreement ends (either by termination or expiry of the term) (refer subclause 19(15));
- meet any other requirements for agreements set out in a data code (a data code is a disallowable legislative instrument made by the Commissioner under clause 126) (refer subclause 19(16)); and
- require the data custodian (or a data custodian of there is more than one data custodian of the data shared under the project) to advise the Commissioner as soon as practical after the agreement ceases to be in effect (for example, as a result of the termination of the agreement) (refer subclause 19(17)).

190. Clause 130 requires the Commissioner to maintain a register of data sharing agreements. Subclause 130(2) sets out a number of details about data sharing agreements that must be in the publicly accessible part of the register.

Part 2.7 – Allowed access to output of project

191. Part 2.7 sets out the circumstances where a data sharing agreement may permit the accredited user to provide access to output to another entity, when a copy of output 'exits' the Scheme (which means the copy is no longer subject to the controls on use imposed by the Scheme) and other matters. Clause 13A only authorises an accredited user to collect and use data shared with it under the Scheme if, amongst other matters, the collection and use is in accordance with the applicable data sharing agreement and the data sharing agreement is registered, in effect and meets the requirements of the Bill. Civil penalties and offences may apply if an accredited user uses data shared with it under the Scheme and that use is not authorised by clause 13A. Clause 9 defines 'use' to include handle, store and provide access.

Clause 20A – Allowed access: providing data custodian of source data with access to ADSP-enhanced data or output

192. In some circumstances where data is shared under the Scheme through an ADSP as intermediary, or an ADSP is engaged as part of a project to perform a data service, such as the de-identification data service, it is appropriate for the data custodian to confirm that the ADSP has complied with its obligations in relation to the data, prior to the ADSP-enhanced data being shared with the accredited user. This type of confirmation enables the data custodian to properly manage the data sharing agreement and ensure that the controls and risk mitigations in the agreement are fully implemented.

193. Subclause 20A(1) permits a data sharing agreement covering a project to allow, or require, an ADSP that is party to the agreement to provide the data custodian with particular ADSP-

enhanced data. Providing access to the ADSP-enhanced data to the data custodian is referred to as 'submitting' the data to the data custodian (refer subclause 20A(3)). Where ADSP-enhanced data is submitted to the data custodian, the submission is taken to be for the data sharing purpose, or data sharing purposes, of the project (refer subclause 20A(4)), because the submission process is intended to help ensure that the controls in the data sharing agreement are full implemented.

194. In some circumstances it is appropriate for the data custodian for a project to confirm that output is as agreed in the data sharing agreement covering the project, before the accredited user in the project makes the output available to another entity, or releases the output, in accordance with the data sharing agreement.

195. Subclause 20A(2) permits a data sharing agreement covering a project to allow, or require, the accredited user to provide the data custodian with particular output. Providing access to the output to the data custodian is referred to as 'submitting' the data to the data custodian (refer subclause 20A(3)). Where output is submitted to the data custodian, the submission is taken to be for the data sharing purpose, or data sharing purposes, of the project (refer subclause 20A(4)), because the submission process is intended to help ensure that the controls in the data sharing agreement are fully implemented.

196. Both subclauses 20A(1) and 20A(2) provide that, where data (ADSP-enhanced data or output) is submitted to the data custodian, the submission is for the purpose of the data custodian ensuring that the data is as agreed in the data sharing agreement. A data sharing agreement that includes a provision permitted by subclause 20A(1) or 20A(2) must limit the purpose for which the data custodian may use submitted data to the purpose mentioned in subclause 20A(1) or 20A(2). Where data is submitted to the data custodian, it remains scheme data and the collection and use of the data by the data custodian is controlled by the Scheme. Clause 13C provides the data custodian with a limited authorisation to collect and use the submitted data. If the data custodian uses submitted data otherwise than as permitted by clause 13C, it may contravene the civil penalty in subclause 14A(7) or commit the offence in subclause 14A(9).

Clause 20B – Allowed access: providing access to output for validation or correction

197. Subclause 20B(1) permits the data sharing agreement for the project to allow the accredited user provide output (which may be the shared data collected from the data custodian, or a processed form of that data) to the individual or organisation to whom it relates for validation or correction. For example, the accredited user may use output to pre-fill application forms for individuals to whom the output relates and provide those forms to the individuals for review. The individuals may then either confirm the pre-filled information or correct the pre-filled information.

198. Subparagraph 20B(1)(a)(iii), when read with clause 133, allows the Minister to make rules to supplement the operation of subclause 20B(1) so that a data sharing agreement may permit access to persons other than entities that carry on a business, or not-for-profit entities (refer paragraph 20B(1)(a)) and individuals (refer paragraph 20B(1)(b)). However, the scope of such rules is intended to be narrow. A rule may only allow a data sharing agreement to permit access to be provided to output to enable the output to be validated or corrected.

199. The term 'not-for-profit entity' in subparagraph 20B(1)(a)(i) is intended to be read broadly and includes entities registered under the *Australian Charities and Non-for-profits Commission Act 2012*.

200. Where a data sharing agreement permits the accredited user to provide a person with access to output as permitted by paragraph 20B(1)(a), the agreement must also require the data custodian to be satisfied that the type of access the accredited user proposes to provide is in accordance

with the data sharing agreement. This is an important control to ensure that the access provided by the accredited user does not exceed what is permitted by the data sharing agreement.

201. Subclause 20B(3) confirms, for avoidance of doubt, that where a data sharing agreement provides for access to be given in accordance with subclause 20B(1), the access is taken to be for the data sharing purpose, or data sharing purposes, of the project.

202. Subclause 20E(2) deals with the exit of data from the Scheme. Where data has exited the Scheme, the Scheme no longer controls how the data is collected or used. Subclause 20E(2) provides that, if a person is provided with access to a copy of data pursuant to a clause of a data sharing agreement permitted by subclause 20B(1), the person's copy is taken to have exited the Scheme (so long as the accredited user complies with other requirements in relation to the provision of access in clause 13A). Subclause 20E(2) does not have the effect that the copy of the data held by the accredited user also exits, and the accredited user must continue to use the data only as permitted by clause 13A.

203. Where a person who has been provided with data for validation or correction under a provision of a data sharing agreement permitted by subclause 20B(1) provides the accredited user with confirmation that the data is correct, or with corrected data, the accredited user is taken to have collected a copy of the data, or the corrected data, from the person (refer subclause 20B(2)). This data that is taken to be collected from the person is not scheme data and the Scheme does not impose restrictions on how such data is used. If the person does not respond to the accredited user when asked to validate or correct data, the accredited user cannot take the absence of a response as constituting the validation of the data.

Clause 20C – Allowed access: providing access to or releasing output in other circumstances

204. Subclause 20C(1) permits a data sharing agreement to include a provision to allow an accredited user to provide access to specified output to another entity, or to release specified output, if three conditions set out in subclause 20C(1) are satisfied. A data custodian is not required to include a provision in a data sharing agreement permitted by clause 20C, and will only do so if the project, including the provision of access to, or release, of data, is consistent with the data sharing principles. The term 'release' is defined in subclause 10(1) to mean the provision of open access to specific data.

205. Paragraph 20C(1)(a) only allows a data sharing agreement to permit the provision of access, or release, or specified output in particular circumstances if the provision of the access, or the release, would not contravene any other law of the Commonwealth or a law of a State or Territory. When considering this, the operation of clause 23 (which provides that the authorisations in clauses 13, 13A, 13B and 13C have effect despite anything in another law of the Commonwealth, or a law of a State or Territory) is disregarded. Thus, for example, if secrecy provisions in another Commonwealth law would prevent output being released (disregarding the operation of clause 23), subclause 20C(1) would not permit a data sharing agreement to provide for release of the output.

206. Paragraph 20C(1)(b) only allows a data sharing agreement to permit the provision of access, or release, or specified output if the agreement prohibits the provision of access or release of output that contains the personal information of an individual without the individual's consent. For example, a data sharing agreement may permit the release of a research report, but if the research report includes any personal information of individuals, the agreement must prohibit the release of the research report unless all of those individuals consent.

207. Paragraph 20C(1)(c) provides that, where a data sharing agreement allows for an accredited user to provide access to output to another entity, or to release output, it must also require the data custodian to be satisfied, before the provision of access or the release, that what the

accredited user proposes to do is in accordance with the data sharing agreement. This is an important control to ensure that an accredited user does not provide access to, or release, output inappropriately.

208. Where an accredited user provides access to, or releases, a copy of specified output under a provision of a data sharing agreement permitted by subclause 20C(1), that copy of the output exits the Scheme under subclause 20E(2).

209. The provision of access to, or release of, specified output under a provision of a data sharing agreement permitted by subclause 20C(1) as part of a project is taken to be for the data sharing purpose, or data sharing purposes, of the project (refer subclause 20C(2)).

Clause 20D – Allowed access: sharing under section 13

210. In circumstances where an accredited entity is a Commonwealth body and the data sharing agreement provides that the accredited user is the data custodian of specified output (as permitted by clause 20F), clause 20D permits the data sharing agreement to also permit the accredited user to share the specified output under clause 13. However, where the sharing of output under clause 13 is permitted, paragraph 20D(b) requires the data sharing agreement to provide for the data custodian of the source data to be satisfied that any sharing of specified output will be authorised.

211. Thus, if entity A and entity B are both Commonwealth bodies, entity A could enter into a data sharing agreement with entity B covering the sharing of certain public sector data. The agreement could provide that entity B is the data custodian of a particular product that is the product of entity B's use of the shared public sector data (the 'specified output'). The data sharing agreement between entity A and entity B could permit entity B to share the specified output under clause 13, if it wishes to do so and the conditions in clause 13 are satisfied. However, the data sharing agreement must require that entity A is satisfied that the sharing of specified output under clause 13 will be authorised under the Scheme, before entity B shares the data. Where entity B then shares the specified output under a data sharing agreement with entity C, the authorisation of entity C to collect and use the data is governed by the data sharing agreement between entity B and entity C (the data sharing agreement between entity A and entity B has no relevance to entity C's authorisation to collect and use data).

Clause 20E – Exit of ADSP-enhanced data or output of project

212. Generally, the Scheme controls how ADSP-enhanced data and output is collected and used. Clauses 13A and 13C provide authorisations to collect and use output. Clause 13B provides an authorisation to collect and use ADSP-enhanced data. Penalties apply under clause 14A if ADSP-enhanced data or output is used in an authorised way.

213. The Scheme provides for a limited number of circumstances where a copy of ADSP-enhanced data, or output, may exit the Scheme, in which case the Scheme controls on collection and use no longer apply to that copy. If a data sharing agreement permits an accredited user to release a copy of specified output in particular circumstances and the accredited user then releases the output in accordance with the agreement (for example, by placing the copy on the internet), the copy of the specified output retained by the accredited user remains scheme data and it may still only be used as authorised by clause 13A. However, if the accredited user obtains a copy of the exited copy of the specified data (for example, by downloading a copy from the internet), it may use the exited copy in a manner not authorised by clause 13A. Subclause 14A(6) provides a defence from the civil penalties and offences in subclauses 14A(1), 14A(2), 14A(4) and 14A(5) if the data collected or used by the defendant is a copy that has exited the Scheme.

214. A direction given by the Commissioner under clause 112 may require a Scheme entity to provide access to output or ADSP-enhanced data to another person. Where a person obtains a copy of output or ADSP-enhanced data pursuant to a direction given by the Commissioner, the copy of the output or the ADSP-enhanced data collected by the person is taken to exit the Scheme.

215. Clause 135 authorises a Scheme entity to provide scheme data to the Auditor-General, the Commonwealth Ombudsman, the Information Commissioner, a Royal Commission or a court or tribunal in certain circumstances. Where a copy of output or ADSP-enhanced data is provided in a manner authorised by clause 135, that copy exits the Scheme.

216. Subclause 20E(1) provides a general overview of the exit of data from the Scheme.

217. Subclause 20E(2) provides for the circumstances where output exits the Scheme. A data sharing agreement can provide for another person to be provided with access to output in the circumstances set out in clauses 20A, 20B, 20C and 20D. Where a data sharing agreement provides for the provision of access to output to another person, generally the copy of the output collected by the other person exits the Scheme. This is not the case, however, if the provision of access is a submission of the output to the data custodian. Where output is submitted to the data custodian, it remains scheme data and may only be collected and used by the data custodian in accordance with clause 13C. Further, where a data sharing agreement for a project (the first project) includes the clause permitted by clause 20D and specified output of the first project is shared under clause 13 as part of a second project, the data shared under section 13 as part of the second project is scheme data and the accredited user may only use output in the second project (including output that was the specified output of the first project) as authorised by clause 13A.

218. Subclause 20E(3) provides for the circumstances where ADSP-enhanced data exits the Scheme. ADSP-enhanced data may only exit the Scheme if the Commissioner gives a direction to provide access to another person under clause 112, or access is provided as authorised by clause 135.

219. In some projects where the data sharing purpose is the delivery of government services, it is important that the accredited user has a copy of shared data that is an individual's personal information that has exited the Scheme. While data is scheme data, it cannot be used for an enforcement related purpose. This includes ensuring that a payment made previously was correctly made, recovering overpayments and identifying people for compliance review (refer subclause 15(3)). In some circumstances, service delivery agencies may not consider it is appropriate to rely upon shared data to deliver a program unless they can also rely upon the same data for later compliance action. Further, service delivery agencies may not have systems in place to be able to use shared data for some aspects of a program but not other aspects.

220. Where an individual's personal information is to be shared as part of a service delivery project, subclause 20E(4) allows for the individual to expressly consent to both the sharing, and the accredited user using the individual's personal information without the limitations on use imposed by the Scheme applying. If the individual does provide this express consent, and the data is shared with the accredited user, subclause 20E(5) provides that the user is taken to hold an exited copy of the personal information at the time it collects it from the data custodian (unless the individual's consent specifies a later time, in which case the accredited user does not hold an exited copy of the personal information until the later time).

221. An example of a situation where the exit mechanism in subclause 20E(4) may be used is as follows. An individual claims a statutory benefit from an Australian Government agency, agency A. Agency A requires personal information to assess the individual's claim. The relevant personal information about the individual is already held by another Australian

Government agency, agency B. Agency A (as accredited user) and agency B (as data custodian) are parties to a data sharing agreement for the purpose of the delivery of government services. Agency A may offer the individual the choice of either supplying the required personal information to the agency directly, or expressly consenting to agency B sharing the relevant personal information with agency A under the data sharing agreement and to agency A being able to use the shared information without the requirements of the Scheme applying.

222. If the individual expressly consents, agency A will be taken to have collected the shared personal information from the individual (refer subclause 20E(6)). Any secrecy provisions applying to the personal information held by agency B will not apply to the exited data held by agency A.

223. Where a project permits shared personal information to exit the Scheme under subclause 20E(4), this must be specified in the data sharing agreement covering the project (refer subclause 16B(2)).

Clause 20F – Data custodian of output of project

224. A data sharing agreement for a project may provide that the accredited user is the data custodian of specific output if the accredited user is a Commonwealth body and other requirements are satisfied (refer clause 20F). In these circumstances, the accredited user is taken to have a copy of the specified output at the time specified for exit to occur in the data sharing agreement, provided that the data sharing agreement does not allow the accredited user to provide access to the specific output to another person under a provision of a data sharing agreement permitted by clause 20C or 20D, and the conditions for exit in subclause 20F(3) are met (see below).

225. Generally, the accredited user under a data sharing agreement for a project does not become the data custodian of output, even if the accredited user is a Commonwealth body (refer subclause 20F(4)).

226. A data sharing agreement may appoint an entity that is not the accredited user as the data custodian of specified output, if the conditions set out in subclause 20F(5) are met. The entity appointed as data custodian must be a Commonwealth body and not an excluded entity. The specified output may not be simply the output that was collected by the accredited user under the data sharing agreement. The data sharing agreement must allow the accredited user to provide the entity appointed as the data custodian of the specified output with a copy of that output under clause 20C. The entity appointed as data custodian does not actually become to data custodian of the output until it is provided with access to a copy of the output (refer subclause 20F(1)).

227. Subclause 20F(2) provides that the accredited user under a data sharing agreement for a project may be appointed as the data custodian of specified output if it is a Commonwealth body, the specified output is not simply the output that was collected by the accredited user and either:

- the data sharing agreement permits the accredited user to provide access to the specified data to another person pursuant to a clause of the data sharing agreement permitted by clause 20C or 20D (in which case the specified output is taken to exit the Scheme at the time it is created – refer paragraph 20F(1)(a)); or
- the conditions for exit in subclause 20F(3) are met and the data sharing agreement does not permit the accredited user to provide access to the specified data to another person pursuant to a clause of the data sharing agreement permitted by clause 20C or 20D (in which case the specified output is taken to exit the Scheme at the time specified in the data sharing agreement – refer subclause 20E(7)).

228. The conditions of exit specified in subclause 20F(3) are similar to the conditions set out in subclause 20C(1).

229. The condition in paragraph 20F(3)(a) provides that the provision of access, or the release, of the specified output by the accredited user would not contravene any other law of the Commonwealth or a law of a State or Territory. When considering this, the operation of clause 23 (which provides that the authorisations in clauses 13, 13A, 13B and 13C have effect despite anything in another law of the Commonwealth, or a law of a State or Territory) is disregarded. Thus, for example, if secrecy provisions in another Commonwealth law would prevent the specified output being released (disregarding the operation of clause 23), the condition is not satisfied.

230. Paragraph 20F(3)(b) applies if the specified output includes personal information about an individual. In this case, the condition is only satisfied if the individual has expressly consented to their personal information being used by the accredited user without the requirements of the Scheme applying to that use.

231. The condition in paragraph 20F(3)(c) is only met if the data sharing agreement requires the data custodian to be satisfied that all requirements in the data sharing agreement relating to the exit of the specified data are met, before the time that the agreement provides for exit to occur.

Part 2.8 – Relationship with other laws

Clause 22 – Other authorisations for data custodians not limited

232. To avoid any doubt, clause 22 clarifies that the Scheme does not limit other legislative authority empowering data custodians to share, collect or use public sector data. For example, some Commonwealth legislation permits data custodians to disclose data in the public interest. This Bill does not affect such powers to disclose.

Clause 23 – Authorisations override other laws

233. Clause 13 provides data custodians with an authorisation to share, collect and use public sector data and clauses 13A, 13B and 13C provide authorisations for accredited users, ADSPs and data custodians to collect and use certain data. Clause 124 extends these authorisations to certain individuals and bodies corporate.

234. Subclause 23(1) provides that the authorisations in Chapter 2 (including as extended by clause 124 to individuals and bodies corporate) apply despite anything in another Commonwealth law or in a law of a State or of a Territory. This is the case however the other law is drafted. For example, the authorisation in clause 13 to share particular data has effect despite a provision in another Commonwealth law that would otherwise prevent the sharing of that data for the purpose of sharing.

235. Subclause 23(2) confirms that subclause 23(1) is intended to have effect in relation to laws enacted after this Bill that limit the sharing, collection and use of particular data.

236. This Bill is not intended to override the *Privacy Act* and the sharing, collection and use of data under the Scheme must be consistent with the *Privacy Act* (subclause 17(5) has the effect that sharing is barred if it would be inconsistent with the *Privacy Act*, and a data custodian is not authorised to share under clause 13 if the sharing is barred under clause 17).

Chapter 3 – Responsibilities of data scheme entities

Part 3.1 – Introduction

237. This Part sets out the key responsibilities of data custodians and accredited entities under the Scheme, including in relation to data breaches.

Clause 24 – Simplified outline of this Chapter

238. Clause 24 provides a simplified outline of Chapter 3, which establishes key Scheme entity responsibilities, including responsibilities in relation to the management of data breaches. The outline also clarifies that there are important responsibilities set out elsewhere in the Bill and civil penalties may apply if responsibilities are not met.

239. 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 this Chapter.

Part 3.2 – General responsibilities

240. This Part sets out some key responsibilities for Scheme entities. Civil penalties apply in some cases if these responsibilities are not met. Certain other important responsibilities are set out elsewhere in the Bill (refer Chapter 2).

Clause 25 – No duty to share but reasons required for not sharing

241. Subclause 25(1) emphasises that the Bill 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 to share public sector data.

242. Under subclause 25(2), data custodians must, however, consider requests from accredited users that are made in the approved form (if there is no approved from, the request must be made in writing) for access to data through the Scheme within a reasonable period.

243. Subclause 25(3) provides that the data custodian must provide reasons for refusing data sharing requests to the accredited user. This approach ensures that data custodians follow due process to consider requests before accepting or rejecting those requests, and promotes procedural fairness.

244. The requirement to provide reasons for refusing data sharing requests within 28 days provides transparency and accountability to the decision making process of data custodians in relation to a data request under the Scheme. This is so that a data request will not be unreasonably refused or delayed.

245. This clause interacts with clauses 34 and 138, which require data custodians to report their sharing activities, including reasons for refusals to share, to the Commissioner for the annual report.

Clause 26 – Comply with rules and data codes

246. This clause requires Scheme entities to comply with the rules and data codes that are made under this Bill (refer Part 6.4). Data codes and the rules are binding legislative instruments.

247. The Bill and the rules set the parameters and requirements of the Scheme; data codes shape how entities implement and comply with those requirements. For instance, the rules may

supplement particular elements of the Bill, such as additional criteria for accreditation under subclause 77(2), and a data code could set particular considerations to be made when applying particular data sharing principles in clause 16.

248. The Minister's power to make the rules is in clause 133 and the Commissioner's power to make data codes is found in clause 126.

Clause 27 – Have regard to guidelines

249. Under clause 27, Scheme entities must have regard to guidelines issued by the Commissioner under clause 127 when engaging with the Scheme.

250. The Commissioner's guidelines are a legislative instrument and will explain expectations and best practice for how the Scheme should operate. Requiring entities to have regard to these guidelines is important to build data management capacity and enhance voluntary compliance with the Scheme.

Clause 30 – Comply with conditions of accreditation

251. The accreditation framework established by Part 5.2 will set conditions that accredited entities must comply with, to maintain their accreditation. Under clause 30, an accredited entity may be liable for a civil penalty, if it fails to comply with these conditions.

252. This is necessary to ensure the Scheme operates as intended, as accreditation is the threshold requirement to ensure an entity is suitable to handle public sector data shared through the Scheme.

253. 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 31 – Report events and changes in circumstances affecting accreditation to Commissioner

254. Clause 31 requires accredited entities to report events or changes in their circumstances which are relevant to the exercise of the functions of the accreditation authority for the entity, or the Minister or Commissioner's regulatory functions under Part 5, other than circumstances prescribed by the rules for the purpose of this clause. Reports must be made in writing (in the approved form, if any) to the Commissioner.

255. It is essential that the Commissioner holds up-to-date information about accredited entities because accreditation governs entry into the Scheme. Certain events or changes in circumstances may reasonably affect the Commissioner's decision-making in relation to an entity's accreditation under Part 5.2 of the Bill. Additionally, certain information the Commissioner holds is made available through publicly accessible registers of ADSPs (refer clause 128), accredited users (refer clause 129), and data sharing agreements (refer clause 130). Facilitating a Scheme entity's ability to access information about other Scheme entities through the registers is intended to support Scheme entities to make informed decisions. For example, consideration of the data sharing principles in clause 16 when negotiating a data sharing agreement, or considering a request to share public sector data under clause 25.

256. Events or changes that trigger this responsibility would typically relate to the entities' ability to meet ongoing conditions of accreditation, governance or structural changes to the entity itself, and its ability to perform activities it has been accredited to do under the 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 the Scheme, and it must notify the Commissioner under this clause.

257. A failure to report may constitute a civil penalty of 300 penalty units.

258. Core accreditation requirements will be established in the accreditation framework in Part 5.2. The Commissioner may issue guidelines under clause 127 to provide clarity about accredited entities' responsibilities.

Clause 32 – Not provide false or misleading information

259. Clause 32 provides that Scheme entities must not provide false or misleading information to the Minister, the Commissioner, or another Scheme entity when operating in the Scheme.

260. Subclause 32(1) provides that Scheme entities must not provide false or misleading information to the Minister or Commissioner, including where the document or information is false or misleading because of an omission. This is crucial as the Minister or Commissioner must have correct information in order to effectively regulate the 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 or when considering regulatory action.

261. Subclause 32(2) similarly requires that Scheme entities not provide false or misleading information to other 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 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.

262. A civil penalty of up to 300 penalty units may apply for breach of this clause. This penalty is specific to this Bill. Penalties and offences under other legislation may also apply, however, for instance under Division 136 or 137 of the *Criminal Code*.

263. The maximum penalty for breach of this clause aligns with other civil penalties in the 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 33 – Registration of data sharing agreements

264. This clause provides the Commissioner with oversight of sharing activities necessary for its regulatory function and ensures compliance with a data code.

265. Subclause 33(1) requires a data custodian to provide the Commissioner with an electronic copy of any data sharing agreement (including varied agreements) it enters into. The copy must be provided in a form approved by the Commissioner (if any) within 30 days of making the agreement or variation.

266. Parties to a data sharing agreement, or a variation of an agreement, may wish to provide a copy to the Commissioner as soon as practicable after execution. This is because a data sharing agreement has no effect until the agreement is registered (refer subclause 18(4)) and a variation has no effect until the variation, or the agreement as varied, is registered (refer subclause 18(5)).

267. Subclause 33(2) requires the data custodian to provide the Commissioner with any other information or document required by a data code. This must be given to the Commissioner at the same time as the document mentioned in subclause 33(1).

268. The Commissioner is required to maintain a public register of data sharing agreements, which will support the Commissioner in administering and reporting on the Scheme, and provide transparency about data sharing activities for Scheme entities and the public more broadly (refer clause 130).

Clause 34 – Assist Commissioner in relation to annual report

269. Clause 34 requires Scheme entities to support the Commissioner to prepare an annual report on the operation of the Scheme. These provisions promote the enhanced integrity and transparency of sharing public sector data and support transparency under the Scheme.

270. Subclause 34(1) outlines the specific information that a data custodian must notify the Commissioner in relation to for the financial year. This includes the number of data sharing requests from accredited users and the reasons for agreement or refusal to share, the number of complaints received (if any), and the number of data sharing agreements it entered into.

271. Subclauses 34(2) and 34(3) provide that a data custodian and an accredited entity must give the Commissioner any other information and provide reasonable assistance in relation to the preparation of the annual report.

272. Subclause 34(4) provides for the period of notification, which is prescribed under a data code or otherwise as soon as practicable.

Part 3.3 – Data breach responsibilities

273. Part 3.3 sets out Scheme entities' responsibilities with respect to data breaches, building on the requirement for privacy coverage in clause 16E. This Part applies to all scheme data, not just data that is personal information.

274. The clauses preserve the 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*.

275. A separate mechanism for reporting breaches of non-personal information to the Commissioner is also established, recognising the variety of public sector data that may be shared under the Scheme.

276. These responsibilities operate while a Scheme entity holds scheme data.

Clause 35 – Definition of data breach

277. 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.

278. For the purposes of this Bill, a data breach will have occurred where there is unauthorised access to, or disclosure of, scheme data held by a Scheme entity. The definition extends to a loss of data that is likely to result in unauthorised access or disclosure, as well as to events prescribed by any applicable data codes.

279. As provided by paragraph 35(a), this clause applies to Scheme entities that hold data, although it is more likely to apply to accredited entities that have received and created scheme data (that is, output and ADSP-enhanced data). Data custodians collect and hold most of their data outside of the Scheme. A breach involving non-Scheme data is not covered by this clause. This clause may, however, apply where a data custodian holds output or ADSP-enhanced data. This could occur in a number of scenarios, such as: where an accredited user provides the data custodian with output pursuant to a data sharing agreement and that output has not exited the

Scheme (refer subclause 19(9) and clause 20E); where ADSP-enhanced data is submitted to a data custodian for the purpose of the data custodian ensuring that the ADSP-enhanced data is as agreed (refer clause 20A); or, where the data custodian holds scheme data that was returned to it by an accredited entity pursuant to a direction from the Commissioner (refer clause 112).

280. The 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, paragraph 35(b) provides that a data breach of the entity will have occurred if there is access to, or disclosure of, the data that is not authorised by this Bill.

281. For the purposes of this Part, 'unauthorised access' means access to scheme data by a person who does not have express or delegated authority (refer Part 2.2) or relevant designation (refer clause 123) 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 malicious attacker.

282. Unauthorised disclosure describes any disclosure that is inconsistent with the authorisation in Chapter 2. For example, deliberate or accidental disclosure by an ADSP with an unaccredited entity, or an accredited user not specified in the data sharing agreement. This concept would also capture an accredited entity using scheme data for a precluded purpose. This definition also includes where a user discloses an output without authorisation (refer subclause 19(10) and clauses 20A, 20B, 20C and 20D) and there is no legal basis for the user to release that data (a legal basis may include a direction under clause 112 or a disclosure authorised by clause 135).

283. 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 disclosure of, the data. For example, a 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.

284. The concepts of "unauthorised access" and "disclosure" are consistent with guidance on data breaches from the Information Commissioner (July 2019).

285. Paragraph 35(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 future-proof the Scheme.

286. Once a Scheme entity reasonably suspects or becomes aware that a data breach has occurred, the entities involved have mitigation and notification obligations under other clauses in this Part.

287. An output that has exited the Scheme in accordance with clauses 20A, 20B, 20C and 20D is no longer regulated by this Bill; redress for data breach involving such an output may be sought through the *Privacy Act* or other applicable avenues, such as the *Criminal Code*.

Clause 36 – Take steps to mitigate data breach

288. This clause requires Scheme entities to take reasonable steps to mitigate harm arising from an actual or suspected data breach (refer clause 35).

289. Subclause 36(1) makes Scheme entities accountable for their actions when a data breach occurs. The responsibility to mitigate any 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 Scheme entity may reasonably suspect a

breach if it detects unauthorised access to computer servers upon which scheme data is stored. A civil penalty of 300 penalty units will apply if an entity does not comply with this subclause.

290. Data custodians have responsibilities under subclause 36(1) in addition to the obligations under subclause 36(2).

291. Subclause 36(2) requires a data custodian to take reasonable steps to mitigate harm where the breach involves data of which it is the custodian or data created as a result of data shared by the data custodian in a data sharing project (that is, output or ADSP-enhanced data). 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. A civil penalty of 300 penalty units will apply if an entity does not comply with this subclause.

292. Subclause 36(3) specifies the period in which Scheme entities must take steps to address actual or suspected data breaches. Entities must take reasonable steps to address breaches in accordance with timeframes specified in a data code, or if there is no such period, as soon as practicable after the breach occurs.

293. Steps taken under subclauses 36(1) and 36(2) to prevent or reduce any harm resulting from the breach to entities, groups of entities and things to which the data involved in the breach relates should be reasonable in the circumstances. The requirement applies to any harm, not just where serious harm may occur. 'Entity' is defined in clause 9, and may include an individual, business, or governmental 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, ecosystems, or buildings.

294. What steps are 'reasonable' will depend on the circumstances, including the severity of the breach, the nature of potential harm to any affected entities, groups of entities or thing, and the resources of the Scheme entity. Notifying affected entities (including other parties to the data sharing agreement) and relevant regulators may be a reasonable mitigation step, but this alone may not be 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.

295. 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.

296. Where a data breach involves personal information, a Scheme entity's remedial action under this clause may affect its notification obligations under clause 37 and the *Privacy Act*.

Clause 37 – Interaction with Part IIIC of the Privacy Act 1988 (notification of eligible data breaches)

297. Where there is a data breach involving personal information shared under the Scheme, the requirements under the Notifiable Data Breach Scheme in Part IIIC of the *Privacy Act* continue to apply. Clause 37 gives effect to this intent, ensuring a consistent, national approach to regulatory oversight.

298. Subclause 37(2) is a deeming provision that creates default responsibility for the data custodian to undertake relevant obligations under Part IIIC of the *Privacy Act*, including in relation to personal information held by an accredited entity as a result of data sharing under the Scheme, even if the accredited entity is not otherwise covered by the *Privacy Act*. By bringing all notifications under the Commonwealth 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.

299. Subclause 37(3) requires an accredited entity to notify the data custodian if it reasonably suspects or becomes aware that a data breach of that entity has occurred. This notification must occur in sufficient time, and contain sufficient detail to enable the data custodian to comply with its obligations under Part IIIC of the *Privacy Act*.

300. Where both the data custodian and the accredited entity are APP entities, subclause 37(4) 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 37(2) or may shift to the accredited entity under 37(4). In both cases, notification is made through the Commonwealth privacy scheme, ensuring consistent regulatory oversight.

301. Subclause 37(5) requires the entity with notification responsibilities under subclauses 37(2) or 37(4) 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 38 to ensure the Commissioner has a holistic picture of data breaches involving scheme data (personal information or otherwise).

302. Subclause 37(5A) allows the Information Commissioner to give the Commissioner a copy of statements received under section 26WK of the *Privacy Act*. The Information Commissioner may provide the statement if they are satisfied that it is relevant to the Commissioner's functions, for example, because the statement relates to data shared under this Bill, or if the statement evidences insufficient privacy practices by an entity accredited under the Scheme.

303. Subclause 37(6) 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.

Clause 38 – Notify Commissioner of non-personal data breach

304. Clause 38 provides a notification mechanism for data breaches that do not involve personal information within the meaning of the *Privacy Act*. The intent is to support the Commissioner to monitor the operation and integrity of the Scheme and the effectiveness of its safeguards. It will also support the Commissioner's ability to exercise their regulatory powers to minimise potential harms when data breaches occur.

305. Subclause 38(1) sets out the criteria that must be satisfied before the obligation to notify the Commissioner is triggered, and introduces a civil penalty provision for Scheme entities that fail to notify the Commissioner within periods specified under subclause 38(1A) and in accordance with any requirements prescribed by a data code.

306. The penalty is intended to deter non-compliance and build confidence in the Scheme by incentivising proactive data breach management. 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.

307. Subclause 38(1A) requires that the Commissioner be notified in accordance with timeframes specified in the data code, or, if there is no such period, as soon as practicable after the end of the financial year in which the breach occurred. This aligns with annual reporting requirements under the *PGPA Act*.

308. Subclause 38(2) allows a data code to prescribe different periods in which Scheme entities must notify the Commissioner of data breaches under this clause. Periods can be differentiated according to whether the breach is such that a reasonable person would conclude that it would be likely to result in serious harm.

309. To determine the likelihood of serious harm, subclause 38(3) requires the Scheme entity to apply a reasonable person test. The paragraphs within subclause 38(3) are a non-exhaustive list of factors to assist entities to determine what constitutes serious harm. These factors draw upon section 26WG of the *Privacy Act* (with some modifications to meet the needs of the Scheme) to promote 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.

310. Breaches involving personal information are addressed separately (refer clause 37) to preserve the operation of the Notifiable Data Breaches Scheme in Part IIIC of the *Privacy Act*.

Chapter 4 – National Data Commissioner and National Data Advisory Council

Part 4.1 – Introduction

311. 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 39 – Simplified outline of this Chapter

312. This clause provides a simplified outline of Chapter 4, which establishes the functions of the Commissioner and the Council, including the constitutional basis for their roles.

313. 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 40 – Commissioner to have regard to objects of Act

314. Clause 40 requires that the Commissioner upholds the objects of this Bill under clause 3 in carrying out their functions under clause 42.

Part 4.2 – National Data Commissioner

315. This Part establishes the statutory role and functions of the Commissioner, and sets out related administrative arrangements to support this role.

Division 1 – Establishment, functions and powers

Clause 41 – National Data Commissioner

316. This clause provides for the role of a Commissioner. The Commissioner is a statutory office holder, as recommended by the Productivity Commission's Inquiry Report into Data Availability and Use (2017). 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*.

317. This clause works in conjunction with clause 46, 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 the *PGPA Act* as such an official of the Department.

Clause 42 – Functions

318. Clause 42 sets out the functions of the Commissioner.

319. The Commissioner is the regulator of and educator for the 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 Scheme entities to promote better and safer sharing and release of public sector data.

320. Specifically, under subclause 42(1), the Commissioner has:

- advice related functions (refer clause 43);
- guidance related functions (refer clause 44);
- regulatory functions (refer clause 45);
- education related functions (refer clause 45A);
- any other function conferred by this Bill, an instrument under this Bill, or any other Commonwealth law; and
- anything incidental or conductive to the performance of the listed functions.

321. Subclause 42(2) provides some constitutional limitations on the Commissioner's performance of their functions. The Commissioner may only perform their functions with respect to the sharing of data under, or purportedly under, clause 13, and only in respect of matters incidental to the execution of the legislative powers of the Parliament or the executive power of the Commonwealth. Subclause 13(4) identifies applicable constitutional requirements for relevant data sharing under clause 13.

Clause 43 – Advice related functions

322. Clause 43 outlines the Commissioner's advice functions. The Commissioner will advise the Minister and relevant entities on the operation of the Scheme. The Commissioner may also be required to provide advice to government agencies and Ministers under other pieces of legislation as they relate to this Bill.

323. 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 Scheme. This may include providing comments on draft legislation, appearing before Senate Committee Inquiries, and engaging in consultations with government agencies.

324. The Commissioner also may advise Scheme entities on how, in their opinion, the Scheme applies or would apply in various circumstances. This could include, for example, how data sharing could comply with this Bill for a particular project. Performance of this function is intended to drive best practice by supporting safe sharing of data.

325. The advice function also relates to advising the Minister in relation to the exercise of the Minister's powers under Part 5.2 (Accreditation Framework). This will allow the Commissioner to support the Minister in the exercise of their powers in relation to the accreditation framework (that is, the accreditation of the Commonwealth, States and Territories, and Commonwealth, State and Territory bodies as accredited users).

Clause 44 – Guidance related functions

326. Clause 44 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 Scheme.

327. As data codes are legislative instruments, all Scheme entities must comply with their requirements (refer clause 26). For example, data codes may set out how to comply with requirements for sharing public sector data under the Scheme, and other relevant matters (refer clause 126).

328. Guidelines are legislative instruments that Scheme entities must have regard to when operating under the Scheme (refer clause 27). Guidelines may set out principles and processes related to any aspect of the Scheme, and any matters incidental to the Scheme (refer clause 127).

Clause 45 – Regulatory functions

329. Clause 45 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 Scheme.

330. 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.

331. 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).

332. Subclause 45(2) places an important limitation on any assistance provided to the Commissioner in relation to their regulatory functions. Under this subclause, the Commissioner must be satisfied that a person (such as an APS employee made available to the Commissioner under clause 47) assisting the Commissioner in the performance of their regulatory functions has the skills, qualifications or experience necessary to provide assistance.

333. When considering whether a person's skills, qualifications or experience meet the required standard, the Commissioner should consider the relevance of the skills, qualifications or experience to the regulatory functions that the person will be assisting with. It is not necessary that such a person must have the required skills, qualifications or experience across all areas relevant to the Commissioner's regulatory functions, provided that they relate to the aspect of assistance which the person would provide. The Commissioner should also consider the extent of the person's skills, qualifications or experience, including the length of experience. For example, the person may have extensive practical experience in regulatory work, but no relevant formal training or tertiary qualifications in the area.

Clause 45A – Education and support related functions

334. Clause 45A establishes the Commissioner's education and support related functions. The Commissioner's education related functions give the Commissioner a role in assisting data custodians and Commonwealth bodies to support the overall functioning and operation of the Scheme.

335. The Commissioner's education and support related functions are also intended to foster best practice and safe data handling by Commonwealth bodies and build confidence in the use of public sector data, allowing the Commissioner to make information and educational material

available on using public sector data. Such information and educational materials will allow the Commissioner to support best practice and promote new or emerging ways of managing and sharing data.

Clause 46 – Application of finance law

336. 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.

337. 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 47 – Staff

338. Clause 47 provides that the Secretary of the Department responsible for this Bill must make APS staff of the Department available to the Commissioner.

339. 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 42), and may be delegated functions or powers in order to do so (refer clause 50).

340. The Secretary must make adequate staff available to meet the Commissioner's needs, in terms of both numbers and abilities. Under paragraph 47(1)(a) the Commissioner will determine the necessary skills, experience or qualifications that staff must have.

341. Subclause 47(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 Scheme, so there is no overlap.

Clause 48 – Contractors

342. Clause 48 allows the Commissioner to engage contractors on behalf of the Commonwealth to assist the Commissioner in the performance of their functions and powers.

343. 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.

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

Clause 49 – Consultants

345. 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.

346. 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 50.

Clause 50 – Delegation by Commissioner

347. Clause 50 enables the Commissioner to delegate functions and powers conferred by this Bill, with some exceptions, to Departmental staff made available to them (refer clause 47).

Delegation is at the discretion of the Commissioner; the Commissioner may continue to personally perform their functions and exercise their powers.

348. 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 Scheme matures.

349. 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 Information Commissioner, Australian Competition and Consumer Commission, and Australian Prudential Regulation Authority.

350. The restrictions to the Commissioner's delegations are detailed in subclause 50(2). Paragraph 50(2)(a) prevents the Commissioner delegating functions and powers relating to the issuing of directions under clause 112, the making of data codes under clause 126, and the making of guidelines under clause 127.

351. Paragraph 50(2)(b) prevents the Commissioner delegating a regulatory function or power to the extent that the function would be performed, or the power exercised, by a delegate in relation to the Department in which the delegate is an APS employee. This paragraph intends to avoid actual or perceived conflicts of interest which might arise if a delegate were to exercise regulatory powers in relation to the Department in which the delegate is an employee.

352. Paragraph 50(2)(c) prevents the Commissioner delegating functions or powers under Part 4.3 (National Data Advisory Council). The restriction on delegation of powers relating to the Council reflects the important role of the Commissioner in the Council. The intention of this paragraph is that the Commissioner's powers with regard to the Council, such as appointing members, are carried out by the Commissioner, rather than a delegate.

353. Subclause 50(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.

354. Where the Commissioner has delegated functions or powers, subclause 50(4) requires the Commissioner to make information publicly available about the (classes of) delegates to ensure transparency in the operation and administration of the Scheme.

Clause 51 – Independence of Commissioner

355. This clause establishes the Commissioner's independence.

356. The Commissioner is established as an independent statutory office holder, responsible for integrity of the 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 or exercises their functions or powers under the Scheme, other than in circumstances where the Commissioner is exercising delegated powers on behalf of, or at the direction of, the Minister (for example, in relation to the Minister's accreditation functions under Part 5.2, refer clause 137A).

357. This clause does not limit the capacity of the Minister or Scheme entities to seek advice on the operation of the Scheme (refer clause 43).

358. This clause does not limit the Commissioner's accountability under this Bill or other laws.

Clause 52 – Commissioner not to be sued

359. Clause 52 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 Scheme. This aligns with standard protections for regulators and their staff acting within the limits of their legal authority.

Division 2 – Terms and conditions etc.

Clause 53 – Appointment

360. Clause 53 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 Bill and the needs of the times.

361. Appointment by the Governor-General supports the independence of the Commissioner.

362. This clause does not prevent a person from being re-appointed as the Commissioner, consistent with section 33AA of the *Acts Interpretation Act*.

Clause 54 – General terms and conditions of appointment

363. 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 that are not dealt with under this Bill may be determined by the Governor-General.

Clause 55 – Other paid work

364. The Commissioner is a full-time office holder (refer subclause 54(2)). As such, clause 55 provides that the Commissioner may only engage in paid work outside the duties of the office with the Minister's approval.

Clause 56 – Remuneration

365. Clause 56 provides that the Commissioner is to be paid remuneration as 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.

366. In line with convention for the remuneration of statutory office holders, subclause 56(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 57 – Leave of absence

367. Aligning with convention, clause 57 provides that the Commissioner's recreational leave entitlements are determined by the Remuneration Tribunal.

368. Other non-recreational forms of leave, such as personal or carer's leave, may be granted by the Minister, on conditions determined by the Minister.

Clause 58 – Resignation

369. This clause provides that the 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 58A – Disclosure of interests to Minister

370. Clause 58A requires the Commissioner to give the Minister notice of any interests, pecuniary or otherwise, that might conflict with the proper performance of their functions (refer clause 42). The note also highlights that the Commissioner holds a separate obligation to report any conflicts of interest with regards to their role on the Council (refer clause 67).

371. The requirement to disclose conflicts of interest aligns with the Bill's underlying philosophy of accountability and transparency. It will also help to ensure that the Commissioner uses their powers under the Scheme objectively and fairly.

Clause 59 – Termination of appointment

372. The Governor-General may terminate the appointment of the Commissioner on grounds listed in clause 59. The grounds cover circumstances where the Commissioner may be unable to exercise their functions or powers independently, diligently, or is otherwise unable to perform their duties appropriately.

373. A ground for termination includes where the Commissioner fails, without reasonable excuse, to give the Minister notice of any conflicts of interest with regards to the proper performance of their functions as required by clauses 58A or 67 of the Bill or section 29 of the *PGPA Act*.

374. 'Reasonable excuse' is not defined, but is an excuse that an ordinary person would accept as reasonable in the circumstances. For example, if unforeseeable circumstances outside of the Commissioner's control prevented the Commissioner from meeting their disclosure obligations, this may provide a reasonable excuse.

Clause 60 – Acting appointments

375. Clause 60 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.

376. A person appointed to act as the Commissioner must have appropriate qualifications, skills or experience to fulfil the role (refer clause 53). The Minister may consult with the Governor-General to confirm appropriate qualifications, skills or experience.

377. 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.

378. Terms and powers of acting appointments are subject to the rules within sections 33AB and 33A of the *Acts Interpretation Act*.

Part 4.3 – National Data Advisory Council

379. This Part establishes the Council, establishing its functions, members, and various other administrative matters.

Clause 61 – Establishment and function of Council

380. This clause establishes the Council, and its function to provide advice to the Commissioner on the list of matters provided in subclause 61(1) relating to the operation of the Scheme.

381. Subclause 61(2) identifies the constitutional basis for the role of the Council. The Council may perform functions with respect to the sharing of data under clause 13 and the collection and use of data in relation to such sharing. Clause 13 identifies applicable constitutional requirements for relevant data sharing in subclause 13(4). Further, the constitutional basis for the role of the Council extends to matters relating to the execution of any of the legislative powers of the Parliament or the executive power of the Parliament.

382. 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 the operation of the Scheme in relation to best practice data management, ethical processes, privacy, or how emerging technologies and related standards might affect the Scheme.

Clause 62 – Membership of Council

383. This clause establishes the membership of the Council.

384. Consistent with subclause 61(1), the Council will include four ex-officio members (the Commissioner, Australian Statistician, Information Commissioner, and Chief Scientist), as well as between five and eight members appointed by the Commissioner.

385. The Council's ex-officio members have been chosen by virtue of their position and depth of experience in matters relevant to the Scheme. In particular, the Information Commissioner was selected as an ex-officio member due to their privacy, information, and freedom of information role and functions. Other public office holders with relevant expertise may be engaged as appointed members.

386. 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.

387. Subclauses 62(2) and 62(3) relate to designating the Chair of the Council. The Commissioner may designate themselves as the Chair of the Council, or may alternatively designate one of the other appointed members to serve in this role. If the Commissioner does not designate a Chair, the Council may designate one of the appointed members as Chair. These options for allocating a Chair provide the Commissioner with flexibility to run the Council as they see fit.

388. Subclause 62(4) provides that a Chair may be designated for a period of up to three years. A Chair may be re-appointed at the end of their term, by one of the methods in subclauses 62(2) and 62(3).

Clause 63 – Appointment of members

389. 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 64 – Term of appointment

390. 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.

391. This provision does not prevent a person being re-appointed, refer to section 33AA of the *Acts Interpretation Act*.

392. Ex-officio members will remain on the Council for as long as they hold their respective offices.

Clause 65 – Remuneration and allowances

393. This clause sets out the remuneration arrangements for appointed members, subject to the requirements of the *Remuneration Tribunal Act 1973*.

394. Subclause 65(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.

395. In line with convention for the remuneration of statutory office holders, appointed members will be paid the allowances prescribed by rules.

396. 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 66 – Leave of absence

397. 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 70).

Clause 67 – Disclosure of interests to Minister or Commissioner

398. This clause requires the Commissioner and other members of the Council to provide written notice of pecuniary and other interests that conflict or may conflict with the proper performance of their role on the Council.

399. The Commissioner must report their conflicts of interest to the Minister, while other members must report conflicts of interest to the Commissioner.

400. 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 the Scheme.

Clause 68 – Disclosure of interests to Council

401. Under this clause, a member with pecuniary or other interests in a matter before the Council must disclose that interest to a meeting of the Council. The disclosure must be minuted. This approach will help to manage and reduce bias in the Council's advice to the Commissioner.

Clause 69 – Resignation of members

402. 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.

403. Ex-officio members cannot resign from their duties on the Council; they remain members for as long as they hold their offices.

Clause 70 – Termination of appointment of members

404. This clause provides a list of circumstances in which the Commissioner may terminate the appointment of members of the Council. The grounds for termination reflect existing laws that establish similar councils, and include misbehaviour, extended unapproved absences, and physical or mental incapacity.

405. In particular, subclause 70(da) provides that membership may be terminated if the member fails to meet their disclosure obligations under clause 67, and the member does not have a reasonable excuse for the failure to disclose. Clause 67 requires an appointed member to disclose to the Commissioner all of the member's interests, pecuniary or otherwise, that the member has or acquires and that conflict or could conflict with the proper performance of the member's office as a member of the Council. The additional ground will assist in ensuring the Council provides objective advice on the operation and administration of the Scheme and is consistent with other Commonwealth laws. 'Reasonable excuse' is not defined, but is an excuse that an ordinary person would accept as reasonable in the circumstances. For example, if unforeseeable circumstances outside of the member's control prevented the member from meeting with disclosure obligations, this may provide a reasonable excuse.

406. Subclause 70(e) provides that a member can be terminated if the member's expertise is no longer relevant to the Council's functions, or if the member no longer occupies a professional role that is relevant to their membership of the Council. This enables the Council to remove members who have changed expertise focus or their profession, whilst also ensuring that membership can continue to remain aligned with any changes in focus of the Council that may occur over time.

Clause 71 – Other terms and conditions of members

407. 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 72 – Procedures

408. 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 73 – Simplified outline of this Chapter

409. This clause provides a simplified outline of Chapter 5 which sets out the substantive provisions on the regulation and enforcement of the Scheme. The outline is not intended to be comprehensive, readers should rely on substantive provisions of the Chapter.

Part 5.2 – Accreditation framework

410. This Part establishes the accreditation framework for the Scheme, administered by the Commissioner under their regulatory functions. Accreditation decisions may be reviewable under clause 118.

Division 1 – Accreditation

Clause 74 – Accreditation

411. Clause 74 sets out an accreditation authority's powers. Accreditation is an essential precondition to entities' participation in the Scheme.

412. Paragraph 74(1)(a) allows an accreditation authority to accredit an entity if the entity applies for accreditation under clause 76, and if the entity seeking accreditation is an 'Australian entity' (refer clause 9) and not be an excluded entity under subclause 11(3).

413. The requirement of being an 'Australian entity' means only an entity that falls within the definition, and is not an excluded entity may participate in the Scheme. Individuals, partnerships, trusts, unincorporated entities and bodies corporate (other than those that are Australian universities) are not eligible to apply for accreditation under the Scheme. This does not preclude individuals who are not Australian citizens or permanent residents from accessing shared data. Individuals who have an appropriate relationship with an accredited entity, such as an employee or researcher of an Australian university, may still be able to access shared data under the Scheme. The Commissioner may make codes in relation to these individuals. For example, the code may require the entity to record details relating to the individuals in the data sharing agreement.

414. Paragraph 74(1)(b) requires that the accreditation authority be satisfied that the entity meets the criteria for accreditation under clause 77 to a standard appropriate for the accreditation for which it is applying, either as a user or an ADSP.

415. Paragraph 74(1)(c) requires that the accreditation authority be satisfied that it is appropriate to accredit the entity in all the circumstances. This operates as a separate criterion, in addition to the criteria under clause 77, that the accreditation authority must consider before granting accreditation. This requires the accreditation authority to consider the application for accreditation holistically, including the broader Scheme operation, when making a decision to grant accreditation.

416. Subclause 74(2) allows the accreditation authority to accredit an entity under subclause (1) with or without imposing conditions of accreditation. The accreditation authority may impose conditions of accreditation on the ground that are appropriate for reasons of security (defined to have the same meaning as in the *ASIO Act* (refer clause 9), or where the conditions are reasonable and appropriate to ensure scheme data is collected and used in accordance with the Bill. Reasons of security can relate to acts of foreign interference, and is applied as a separate consideration from what is appropriate and reasonable in the circumstances. For example, a condition that requires the entity to access scheme data through secure access data service provided by an ADSP may be a reasonable and appropriate condition to impose in order to ensure scheme data is used in accordance with the Bill.

417. When considering the imposition of conditions on an entity's accreditation, clause 79 requires the accreditation authority to give notice before making a decision to accredit an entity with conditions. Note that the rules may prescribe conditions of accreditation (refer clause 77B).

418. Subclause 74(3) provides that the accreditation authority may be satisfied that an entity meets the criteria of accreditation under clause 77 on the basis that the entity will comply with any conditions imposed on them. Alternatively, the entity may not be required to meet one or more criteria of accreditation, on the basis that the entity will comply with conditions of accreditation imposed on them. For example, an entity may not be required to have its own secure IT environment (for the purpose of satisfying the accreditation authority that the entity can minimise the risk of unauthorised access and disclosure of data) if the accreditation authority imposes a condition requiring the entity to engage an ADSP to provide secure access data services (refer subclause 16C(4)) to access scheme data. This is intended to provide greater efficiency in how accreditation operates, including broadening the scope of entities who are able to participate in the Scheme where they would otherwise not have been able to, while maintaining the integrity of the Scheme.

419. Subclause 74(4) gives an example to illustrate how subclause 74(3) operates. This is designed to assist with interpretation of paragraph 74(1)(c), for when an accreditation authority might not consider it appropriate to grant an entity accreditation in all the circumstances. The example provided is where the entity's participation in the Scheme may pose concerns for reasons of security. This may be on the basis of an adverse or qualified security assessment, or advice from a national security agency. This example is not intended to limit the consideration under paragraph 74(1)(c) to matters only relating to security.

Clause 75 – Notice of accreditation decision

420. This clause sets out notice requirements in relation to accreditation decision made under clause 74. Subclause 75(1) requires the accreditation authority to give the entity written notice of its accreditation decision as soon as practicable after making the decision.

421. Subclause 75(2) sets outs the content requirements for the notice under subclause (1). In particular, the notice must state whether the entity has been accredited and in what capacity, the date of when the accreditation comes into force, and, if the accreditation authority decides to impose conditions on accreditation, the reasons for imposing those conditions, and the entity's rights of review for the decision. This supports procedural fairness by detailing the entity's rights of review and reasons for decision. Where the entity is accredited as an ADSP, the notice must also state that their accreditation as an ADSP must be renewed every five years (refer clause 84).

422. Subclause 75(3) deals with the notice requirements in circumstances where the entity's application for accreditation is refused. This subclause requires the accreditation authority to provide their reasons for refusing the application for accreditation and detail the entity's rights of review for the decision.

Clause 76 – Application for accreditation

423. This clause provides for the procedural requirements for accreditation applications for both ADSPs and accredited users.

424. Subclause 76(1) provides that an entity may apply to the appropriate accreditation authority for accreditation as an ADSP or an accredited user. Subclause 76(2) lists requirements for a valid accreditation application. In particular, paragraphs 76(2)(a) and (b) provide that the application must be made by an authorised officer on behalf of the entity (refer clause 137), and be in the form approved by the Commissioner, if one is approved under clause 132.

425. Paragraph 76(2)(c) requires that where an entity applies for accreditation, it must supply evidence prescribed by the rules of its ability to meet the accreditation criteria to the appropriate standard. The entity must supply the evidence prescribed by the rules to satisfy the accreditation authority that it meets the accreditation criteria relevant to the type of accreditation for which it is applying.

426. Paragraph 76(2)(d) requires each applicant consent to the Commissioner obtaining relevant information from third parties, or verifying information provided by the entity with third parties. This will assist the Commissioner to undertake their regulatory functions under Chapter 5.

Clause 77 – Criteria for accreditation

427. This clause specifies the mandatory criteria that an entity must meet to become an accredited user or an ADSP.

428. Subclause 77(1) provides accreditation criteria into the following requirements:

- appropriate data management and governance policies and practices, and an appropriately qualified individual with responsibility for data management and governance within the organisation; and
- ability to minimise the risk of unauthorised access, sharing and loss of data; and
- necessary skills and capability to ensure privacy, protection and appropriate use of data, including the ability to manage any risks in relation to those matters.

429. The requirements under paragraph 77(1)(a) focus on the policies, guidelines and practices the entity has in place to appropriately handle data, including managing risks and responding to incidents. This criteria also includes that the entity has an appropriately qualified person in a role, for example a Chief Data Officer. This role can have different responsibilities in different types of entities, but must provide leadership and accountability for the entity's data agenda.

430. Paragraph 77(1)(b) requires the organisation to have both physical and cyber control security settings in place to protect against unauthorised use of the data. No specific controls are prescribed in this paragraph, but the accreditation authority could have regard to the entity's application of relevant security standards, such as the Australian Government's Protective Security Policy Framework, applicable State or Territory government security policies, or the ISO/IEC 27001 framework.

431. Paragraph 77(1)(c) requires the organisation to have the necessary data skills and capability to handle data. This may include consideration of the entity's hiring practices, such as personnel vetting and on boarding and off boarding processes, as well as role descriptions to support the appropriate use and protection of data.

432. The entity will also need to meet criteria prescribed by the rules (if any) under subclause 77(2).

433. Subclause 77(1A) sets out additional criteria for ADSP accreditation. An entity applying for accreditation as ADSP must have the necessary policies, practices, skills and capability to perform de-identification data services, secure access data services, and complex data integration services. In accordance with paragraph 76(2)(c), the rules will prescribe the evidence required to show the entity meets the criteria relevant for ADSP accreditation. This approach allows the Bill itself to remain technology neutral, while enabling the Scheme to adapt to emerging technologies and future needs over time.

434. In accordance with clause 74, the accreditation authority must be satisfied that the entity meets criteria to the standard appropriate for accreditation. The accreditation authority must also be satisfied that it is appropriate to accredit the entity in all the circumstances. While appropriate is not defined, it is intended to mean that the accreditation authority will consider responses to the criteria as a whole and in the context of the entity's business operations, such as its organisational structure, size and business purpose. For example, where an entity is large, more sophisticated documentation of data practices may be appropriate, as a mechanism to assist with defining the organisation's expectations across a large volume of staff. However, it may also be appropriate that the entity have a greater level of education, training, and monitoring to ensure this policy is reflected their practices.

Clause 77A – General provisions relating to accreditation

435. This clause outlines matters which apply generally to accreditation.

436. Subclause 77A(1) provides that an ADSP has the status of ADSP at all times until its accreditation is cancelled under clause 81, which is the provision that empowers an accreditation authority to suspend or cancel accreditation. This means the entity continues to be

subject to the responsibilities and requirements of the Scheme even when its accreditation is suspended (refer paragraph 13(1)(h)).

437. Subclause 77A(2) provides the same clarification under subclause 77A(1) for accredited users. This approach ensures accredited entities remain regulated under the Bill 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 clause 14A).

438. Paragraphs 77A(3)(a) to (c) clarify that accreditation is granted subject to the accreditation authority's powers to place conditions on, suspend, and cancel an entity's accreditation (refer clauses 78 and 81). The Minister may prescribe conditions for accredited entities in the rules (refer clause 77B). Accreditation may also be affected by other legislation or future amendments to this legislation.

439. Paragraph 77A(3)(d) reflects that accreditation is granted on the basis that no compensation is payable if conditions of accreditation are imposed or varied, or the accreditation is suspended or cancelled. Accreditation and related interests are not property for the purposes of section 51(xxxi) of the *Constitution*, which allow Parliament to make laws for the acquisition of property on just terms. Accredited entities are therefore not entitled to just terms compensation where their accreditation status is altered. 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.

440. Paragraph 77A(3)(d) is modelled on subsection 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.

441. Once an entity has successfully applied and been granted accreditation, it has responsibilities under the Bill, in particular under Chapters 2, 3, and 5. These responsibilities include complying with conditions of accreditation and providing updated evidence to maintain their accreditation (refer clauses 30, 31, and 78), reporting sharing activities and relevant changes in circumstances to the Commissioner (refer clauses 31 and 34), and data breach responsibilities under Part 3.3.

Division 2 – Conditions of accreditation

Clause 77B – Conditions of accreditation

442. Clause 77B deals with matters related to the imposition of conditions of accreditation and gives examples of how conditions may function.

443. Subclause 77B(1) provides that the Minister may prescribe conditions of accreditation using rules. The conditions so prescribed may apply to all entities, or a class of entities. For example, the prescribed conditions may require all accredited users that are Australian universities to use secure access data where the data sharing project involves data which contains personal information.

444. Subclause 77B(2) clarifies that conditions of accreditation, whether prescribed by the rules or under the Bill, may require, permit or prevent entities from doing a thing. For example, a condition of accreditation may require an entity to only allow specified personnel within the entity to access scheme data.

445. Subclause 77B(3) provides a list of examples of the kinds of conditions that could be imposed. This list is not exhaustive and is not intended to limit the kind of conditions that may be imposed on an entity.

446. Clause 77B is designed to allow broad flexibility in imposition of conditions of accreditation. This enables the conditions to address issues that the accreditation authority may encounter when assessing the application or in exercising their regulatory functions. This is intended to encourage more entities to participate in the Scheme, as it allows entities to participate in the Scheme where they may not otherwise have been able to.

Clause 78 – Imposition, variation or removal of conditions of accreditation by accreditation authority

447. Under this clause, the accreditation authority may impose, vary or remove conditions of accreditation imposed on entities while the entity is accredited. Conditions can be imposed for safeguarding scheme data and ensuring compliance with the Bill.

448. Clause 78 explicitly recognises that an entity can be accredited in different capacities (that is, as an accredited user and as an ADSP), which is reflected under subclause 78(3) (refer also clause 11A(5)). Note that failure to comply with a condition of accreditation is a contravention of a civil penalty provision and may mean a collection or use of scheme data by the accredited entity is not authorised and may be subject to other penalty provisions.

449. Subclause 78(1) provides that the accreditation authority for an entity may impose conditions of accreditation on the entity if it is appropriate for reasons of security or is otherwise reasonable or appropriate in the circumstances to ensure collection and use of scheme data in accordance with the Bill. Reasons of security includes an adverse or qualified security assessment of a person, for example in respect of an employee of the entity. As in the case of subclause 74(2), reasons of security can be potential foreign interference, and is applied as a separate criterion from consideration for what is appropriate and reasonable in the circumstances. For example, a condition that requires the entity to access scheme data through an ADSP may be an appropriate condition to impose to ensure the safe sharing of data.

450. Subclause 78(2) requires the accreditation authority to consider suspending or cancelling an entity's accreditation or to impose conditions if a court finds that the entity has committed an offence against the Bill, or a civil penalty is made against the entity in relation to a serious contravention for the purposes of subclause 14(2). Conditions, if imposed under this subclause, are to mitigate the risk of further contravention by the entity. For example, a condition could limit the individuals within the entity who are authorised to handle any scheme data collected or held by the entity.

451. Where an entity is accredited both as user and ADSP, subclause 78(3) requires the accreditation authority to apply their considerations under subclause (2) in relation to both of the entity's accredited capacities.

452. Subclause 78(4) allows the accreditation authority to vary or remove a condition of accreditation imposed under subclause (1) if it is appropriate for reasons of security, or otherwise appropriate in circumstances. Reasons of security is a separate criterion from consideration for what is appropriate in the circumstances.

453. Subclause 78(5) requires the Minister to notify the Commissioner of the Minister's decision to impose, vary or remove a condition of accreditation. This supports the performance of the Commissioner's regulatory functions and to ensure information in the register of accredited users is current (refer clause 129).

Clause 79 – Notice before decision relating to conditions of accreditation

454. Subclause 79(1) requires the accreditation authority to give an entity written notice of the proposed decision to accredit the entity with conditions, to impose, vary or remove conditions

imposed on the entity, or to renew an ADSP accreditation with conditions. In the case of ADSP renewal, a notice is required even if the proposed conditions are the same conditions previously imposed.

455. Subclause 79(2) requires a notice under subclause (1) to state the proposed decision and request the entity respond to the notice in writing. The accreditation authority can specify a period within which the entity must respond. Subclause 79(3) puts additional obligation on the accreditation authority to consider any written statement given under subclause 79(2) before making its decision.

456. Subclauses 79(2) and (3) are designed to provide procedural fairness and allow the entity an opportunity to provide more information to the accreditation authority to ensure the authority has all the relevant information before the decision is made. This may occur if the information was initially omitted, or the entity's circumstances have since changed, or if the entity wishes to provide further information for the accreditation authority's consideration.

457. Subclause 79(4) provides that where changes to an entity's accreditation conditions are to address issues related to security, or urgent and serious issues, the accreditation authority may choose to not notify an accredited entity, before applying a new condition or varying or removing an existing condition. The accreditation authority may alternatively choose to issue a notice but not request a response, as is otherwise required under paragraph 79(2)(b). This subclause does not prevent the accreditation authority from considering submissions by the affected entity that were not solicited under this clause.

458. Subclause 79(4) ensures the accreditation authority is able to act quickly to mitigate serious and urgent risks. An example is where an accreditation authority reasonably believes a change in an entity's IT data storage arrangements has occurred that makes scheme data vulnerable. Entities will receive a notice under clause 80 of the condition imposed to ensure it can comply with obligations under the Bill.

Clause 80 – Notice of conditions

459. Clause 80 requires the Commissioner to provide written notice to an accredited entity of a decision under clause 78, as soon as practicable after making the decision. It also sets out notice requirements in relation to that decision.

460. The notice must contain all the matters listed under subclause 80(2), which include what condition is being imposed, varied or removed, when this will take effect, and the entity's review rights under part 6.2 (refer clause 118).

Division 3 – Suspension and cancellation of accreditation

Clause 81 – Suspension or cancellation of accreditation

461. Clause 81 provides grounds for when an accreditation authority may suspend or cancel an entity's accreditation. The effect of suspension is that the accredited entity remains a Scheme entity but cannot participate in sharing activities (refer paragraphs 13(1)(f) and 13(1)(h). Cancellation involves removing accreditation, so the entity ceases to be a Scheme entity.

462. Clause 81 imposes obligations on the accreditation authority to consider each type of accreditation the entity may hold when making a decision to suspend or cancel, for example in circumstances where an entity is accredited as a user and as an ADSP.

463. Subclause 81(1) provides grounds for when an accreditation authority may suspend or cancel the entity's accreditation. In particular, the grounds include where another accreditation authority refused to accredit, suspend, or cancel the accreditation of the entity in its other capacity.

464. A Commonwealth body's accreditation as an ADSP may need to be suspended and investigated if necessary, if the Minister refuses to accredit it as a user or its accreditation as a user is suspended or cancelled. This is to ensure the criteria of accreditation under clause 77 are enforced consistently across all the different capacities of an entity's participation in the Scheme.

465. Subclause 81(1) is accompanied by a note clarifying that an accredited entity remains accredited until its accreditation has been cancelled.

466. Subclause 81(2) allows the accreditation authority to suspend an entity's accreditation if the accreditation authority reasonably suspects that the entity has breached this Bill or a data sharing agreement.

467. Subclause 81(3) allows the accreditation authority to cancel an entity's accreditation if the Commissioner determines, following investigation under clause 102, that the entity has breached the Bill or a data sharing agreement.

468. Subclause 81(4) allows the Minister to cancel the accreditation of a Commonwealth body as a user if the Minister reasonably believes that the entity has breached this Bill or a data sharing agreement. The purpose of subclause 81(4) is to provide an alternative pathway for the Minister, as the accreditation authority for accrediting bodies politic and Commonwealth bodies, State bodies, and Territory bodies as users, to cancel accreditation.

469. Where an entity is accredited in more than one capacity, for example, where the entity is accredited as both an accredited user and an ADSP, subclause 81(5) allows the accreditation authority to take into account the entity's conduct in any one or all of those capacities when making a decision under subclauses 81(1), (2), (3) or (4). For example, where an entity is accredited as both a user and an ADSP, if the Commissioner determined following an investigation under clause 102 that the entity had breached a data sharing agreement to which they are a party as a user (such as by allowing unauthorised access to shared data), this breach might be relevant to assessing whether the entity continues to meet the criteria relevant to their accreditation as an ADSP, and whether a suspension of their ADSP accreditation, might be appropriate.

470. Similarly, where a Commonwealth body is accredited as an ADSP, subclause 81(6) requires the Commissioner (the accreditation authority for ADSPs) to consider cancelling or suspending its accreditation, or imposing or varying conditions of accreditation applicable to the entity's accreditation as ADSP. This is where the Minister has refused to accredit the Commonwealth body as a user or has suspended or cancelled its accreditation as a user.

471. Similar to subclause 81(5) and (6) where an entity, who is an ADSP, as well as an accredited user, has its accreditation as ADSP cancelled or suspended, subclause 81(7) requires the relevant accreditation authority to consider cancelling or suspending its accreditation, or imposing or varying conditions of accreditation applicable to the entity's accreditation as an accredited user.

472. Subclause 81(8) requires the Commissioner to suspend an entity's accreditation as an ADSP if the entity fails to apply for renewal of accreditation within five years of the last grant of accreditation. The Commissioner is also required to suspend or cancel an entity's accreditation as an ADSP if its application for renewal is refused, noting that the entity remains accredited until its accreditation is cancelled.

473. Subclause 81(9) allows the accreditation authority to cancel an entity's accreditation if an authorised officer of the entity requests cancellation and that request has been made in the approved form where there is one.

474. Subclause 81(10) 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 112(3), unless the accreditation authority for the entity 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. This approach ensures the entity remains subject to relevant responsibilities and liabilities, as a Scheme entity. In practice, this may involve the Commissioner issuing a direction and taking steps to verify or enforce compliance (which could include suspension of accreditation if the direction is not complied with, before making a decision to cancel accreditation.

Clause 82 – Notice before decision about suspension or cancellation

475. Subclause 82(1) requires the accreditation authority to give written notice to an accredited entity prior to suspending or cancelling its accreditation under subclauses 81(1), (2), (3) or (4), unless the suspension or cancellation is done for reasons relating to security, or the accreditation authority reasonably believes there are serious and urgent reasons to suspend or cancel accreditation (refer subclause 82(4)).

476. Subclause 82(2) prescribes information the accreditation authority's notice must contain. All notices must state the grounds for the proposed suspension or cancellation, and identify the dates of suspension or cancellation. For suspension, the notice must also specify the proposed period of suspension, or if the proposed suspension is indefinite. Notices must also request the accredited entity respond with a written statement showing cause why their accreditation status should not change, within a time period specified by the accreditation authority.

477. Under subclause 82(3) the accreditation authority must consider an accredited entity's statement, if provided within the specified time as per the notice, before making a decision under clause 81.

478. Subclause 82(4) provides that if the decision to suspend or cancel an entity's accreditation is to address matters related to security, or urgent and serious issues, the accreditation authority may choose not to notify an accredited entity before making a decision to suspend or cancel accreditation. The accreditation authority may alternatively choose to issue a notice, but not request a response, as is otherwise required under paragraph 82(2)(c). This subclause does not prevent the accreditation authority from considering submissions by the affected entity that were not solicited.

479. Subclause 82(4) ensures the accreditation authority is able to act quickly to mitigate serious and urgent risks. An example of such a situation is if the accreditation authority reasonable believes there is a risk of serious non-compliance with a data sharing agreement that requires investigation. The Commissioner may immediately suspend the entity's accreditation without giving the entity any written notice.

Clause 83 – Notice of suspension or cancellation

480. Clause 83 ensures an accredited entity receives written notice of a decision to suspend or cancel its accreditation. In accordance with subclauses 83(1) and 83(2), such notice must be provided to the entity by the accreditation authority as soon as practicable after making the decision.

481. A notice must contain the information prescribed by subclause 83(3). In particular, a notice must set out the grounds for the suspension or cancellation of accreditation, and the time period for the suspension or the date the cancellation takes effect. For suspension, the notice must also specify the period of suspension, or if the suspension is indefinite. The notice must also set out what rights the entity has to seek review of the accreditation authority's decision under Part 6.2.

Clause 83A – Lifting of suspension

482. Clause 83A allows the accreditation authority to lift suspension by written notice, where the accreditation authority is satisfied that circumstances have changed so that grounds no longer exist for the suspension, or it is otherwise no longer appropriate to continue the suspension on the entity's accreditation.

483. For example, the accreditation authority may suspend a user's accreditation because they reasonably suspect that unauthorised individuals within an accredited entity are accessing scheme data and have grounds for suspecting that this may be a systemic issue. The accreditation authority can lift the suspension if appropriate, after an investigation demonstrates that there are no grounds for continuing the suspension.

484. This is to ensure that accredited entities can resume participating in the Scheme once the accreditation authority is satisfied the reasons for suspension no longer exist.

Division 4 – Renewal of accreditation of ADSPs

Clause 84 – Renewal

485. Clause 84 sets out requirements for renewal of ADSP accreditation. Subclause 84(1) outlines the criteria under which the Commissioner can renew the accreditation of an ADSP. The criteria to renew accreditation of an ADSP aligns with the criteria under clauses 74 and 77 for initial accreditation. This ensures consistency in the accreditation process.

486. Subclause 84(2) allows the Commissioner to renew the accreditation of an entity under subclause 84(1) with or without imposing conditions of accreditation. The conditions can be the same conditions that were imposed on the entity previously. The Commissioner may impose conditions of accreditation if the condition is appropriate for reasons of security, or is otherwise reasonable and appropriate in the circumstances to ensure that scheme data is collected and used in accordance with the Bill.

487. For example, if an entity was accredited as an ADSP with the condition not to provide secure access data services, the Commissioner may impose the same condition if the entity continues to not meet the criteria for providing the service at the time of renewal.

488. Note 1 under subclause 84(2) signposts the Commissioner's obligation to give an entity notice under clause 79 before making a decision to renew the entity's accreditation with conditions. Note 2 clarifies that the Minister can prescribe conditions of accreditation through rules and these rules would apply despite the Commissioner's decision not to impose any conditions.

489. Subclause 84(3) provides that the Commissioner may be satisfied that the criteria of accreditation under clause 77 may be met with conditions of accreditation imposed, on the basis that the entity will comply with the conditions. Alternatively, the entity may not be required to meet one or more criteria of accreditation, on the basis that the entity will comply with conditions of accreditation imposed. For example, an entity may not have the capability to provide all of the ADSP services so a condition could be applied to limit the kinds of data services the entity may provide.

490. Subclause 84(4) gives an example to illustrate how paragraph 84(1)(c) operates. An accreditation authority might not consider it appropriate to renew an entity's accreditation where the entity's participation in the scheme may pose concerns for reasons of security. This may be on the basis of an adverse or qualified security assessment or advice from a national security agency. This example is not intended to limit the consideration under paragraph 84(1)(c) to matters only relating to security.

Clause 85 – Notice of renewal decision

491. This clause sets out notification requirements in relation to the Commissioner's decision under clause 84. Subclause 85(1) requires the Commissioner to give an entity written notice of a decision to renew, or refuse to renew the entity's accreditation as soon as practicable after the decision is made. The requirement to give notice supports procedural fairness.

492. Where the Commissioner decides to renew the accreditation, subclause 85(2) requires the notice to include certain information, including that the renewal is in effect for five years, any conditions of accreditation, and the entity's rights of review under Part 6.2. Where the Commissioner decides to renew with the same conditions of accreditation imposed before the renewal, the conditions must also be set out in the notice.

493. If the Commissioner refuses to renew the accreditation, subclause 85(3) requires the Commissioner to give the entity written notice setting out the reason for the refusal, that the entity's accreditation will be suspended or cancelled under clause 81, and the entity's rights of review under Part 6.2.

Clause 85A – Application for renewal

494. This clause sets out procedural requirements for how an entity can apply to renew its accreditation as an ADSP. Under subclause 85(1), an entity accredited as an ADSP may apply for renewal of its accreditation. The note under subclause 85A(1) clarifies that an ADSP, whose accreditation is suspended as a result of failure to apply for renewal, may still apply for renewal under this subclause.

495. Subclause 85A(2) requires the application to be made by an authorised officer of the entity, and if there is an approved form, the application needs to be made in that form. The application must also include the evidence prescribed by the rules to support criteria for accreditation. The rules may prescribe, for example, evidence to demonstrate the entity's ability to de-identify data.

496. The entity is also required to provide consent for the Commissioner to obtain information relevant to the entity's application from third parties and verify information provided by the entity with third parties.

Division 5 – Rules and further information

Clause 86 – Rules relating to the accreditation framework

497. This clause enables rules to be prescribed for the accreditation framework, pursuant to the Minister's rule-making power in clause 133.

498. The rules may provide for procedures and requirements to support the operation of the accreditation framework, as well as other matters relating to accreditation of entities for the purposes of the Scheme. For example, the rules may establish what evidence is required to satisfy the accreditation criteria.

499. Consistent with this part, the Minister may set additional items in rules to allow the Scheme to evolve, for instance to cater for changes in technology or data management that should be reflected in the accreditation criteria (refer clause 77).

500. The note clarifies that the rules may also prescribe fees in relation to services provided under the accreditation framework (refer clause 139).

Clause 87 – Further information or evidence

501. To inform a decision under this Part, the accreditation authority may issue a written request under subclause 87(1) for an entity to provide further information or evidence, including information or evidence prescribed by the rules. For instance, this power could be used where an entity has not provided sufficient evidence to allow the accreditation authority to make a fully informed decision on its accreditation application.

502. Subclause 87(2) clarifies if the accreditation authority makes a request under subclause 87(1), the accreditation authority does not need to make a decision about accreditation until the information or evidence has been provided and reviewed.

503. This power to request further information is different to the Commissioner's power in clause 104 to require production of information, though both serve regulatory purposes.

Part 5.3 – Complaints

504. This part establishes two complaints mechanisms, which aim to manage disputes between Scheme entities ('scheme complaints') and to manage concerns in relation to the operation and administration of the Scheme ('general complaints'). The complaints mechanisms are some of the 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. The complaints mechanisms relate directly to the Commissioner's regulatory functions and powers, as outlined under clause 45, to oversee operation of the Scheme.

Division 1 – Scheme complaints

505. This Division establishes a complaints mechanism for Scheme entities. It allows for a Scheme entity to complain to the Commissioner in relation to another entity's breach or potential breach of this Bill or a data sharing agreement to which both entities were party when the alleged breach occurred.

Clause 88 – Making scheme complaints

506. This clause provides a means for 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 Scheme, as well as identify areas where additional guidance may be needed to support voluntary compliance.

507. Subclause 88(1) enables Scheme entities ('complainants') that reasonably suspect another Scheme entity ('respondent') has breached this Bill or a data sharing agreement to make a complaint to the Commissioner. A breach includes an act, practice, or omission, whether present or past, that contravenes or is inconsistent with this Bill or a data sharing agreement. The standard of reasonable suspicion indicates that it is less than a reasonable belief but more than a mere possibility. It reflects that entities may require action by the Commissioner in order to be able to gather evidence on alleged breaches.

508. Complaints may be made about former Scheme entities, where the suspected breach occurred while the entity was a Scheme entity. This aligns with the Commissioner's ability to exercise regulatory powers in relation to the activities of former Scheme entities that occurred when the entity had Scheme entity status. This recognises that some breaches may not come to light immediately when they occur.

509. Scheme entities cannot make a scheme complaint about a data custodian's decision to not share data, as this does not constitute a breach of the Bill due to there being no duty to share under

clause 25. However, scheme complaints may be made about other decisions that may breach the Bill, for example if a data custodian has not given reasons for its decision to refuse to share, or if data has been shared for a precluded purpose, or agreed safeguards under the data sharing principles were improperly applied. Otherwise, Scheme entities may make a 'general complaint' under clause 94 in relation to matters that do not constitute a breach of the Bill or a data sharing agreement.

510. Subclause 88(2) clarifies that former Scheme entities may make complaints within 12 months of losing their Scheme entity status. This period provides an appropriate window for former Scheme entities to seek to resolve any latent or ongoing issues with their participation in the Scheme. The 12 month window mirrors the Commissioner's ability to dismiss complaints under paragraph 92(1)(d) if they are made more than 12 months after the complainant first reasonably believed the respondent breached, or was breaching, the Bill or a relevant data sharing agreement.

511. Subclause 88(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.

512. While this mechanism allows for Scheme entities to complain about non-compliance under the Scheme or a data sharing agreement, it does not prevent Scheme entities, other entities or individuals from contacting the Commissioner through administrative channels or complaining about the Scheme or Scheme entities' activities through existing legal mechanisms. For instance, any entity or person may make general complaints regarding a Scheme entity or the Scheme under Division 2, and any entity or person may complain to the Information Commissioner about mishandling of their personal information under the *Privacy Act*. The Commissioner has the ability to collaborate with other regulators including transferring or disclosing matters that would be more appropriately dealt with by them, as supported by clauses 107 and 108.

Clause 89 - Respondents

513. This clause clarifies who the respondent to a complaint is, depending on the nature of the entity.

514. Conduct of individuals may be attributed to Scheme entities. Part 6.3 provides guidance on when such attribution occurs.

Clause 90 - Communicating with complainant

515. This clause ensures the complainant receives notice of how the Commissioner is responding to their scheme 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.

516. The Commissioner may, but is not required to, notify respondents about complaints. However complainants are expected to have first raised their complaint with the respondent directly unless it would not be appropriate to do so (refer paragraph 92(1)(b)). This minimises the burden on the Commissioner and respondents when dealing with vexatious or unsubstantiated complaints. If the Commissioner decides to proceed with an assessment or investigation of the complaint they must notify the respondent of this fact (refer clauses 100 and 103).

517. Subclause 90(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. This allows the Commissioner to collect information needed for preliminary inquiries when the complaints provided insufficient information.

518. If the Commissioner makes a request under subclause 90(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.

519. Subclause 90(4) states that the Commissioner need not provide notice under subclause 90(1) if the Commissioner has given the complainant notice that they will not deal with the complaint (refer clause 92) on or before the day the written notice under subclause 90(1) was due.

Clause 91 - Dealing with complaints

520. This clause provides the essential steps, at a high level, that the Commissioner must follow in order to determine how best to deal with a complaint. The Commissioner must make preliminary inquiries of any relevant person to determine how to deal with the complaint. The Commissioner must also consider and make arrangement for conciliation or an external dispute resolution scheme, if appropriate to resolve the complaint.

521. Conciliation may be conducted informally among the parties, facilitated by the Commissioner or undertaken with external assistance. An external dispute resolution scheme refers to an independent service that generally provides a structured dispute resolution mechanism, such as mediation or arbitration. The use of such processes is encouraged as they maximise the autonomy of parties to resolve the complaint and can avoid the need for court proceedings. It also reflects similar approaches in the *Privacy Act* and the *Corporations Act 2001*.

522. If the Commissioner considers that it would be appropriate to resolve the complaint by conciliation or an external dispute resolution scheme, the Commissioner need not proceed with dealing with the complaint (refer paragraph 92(1)(h)).

523. If conciliation or an external dispute resolution scheme is not appropriate to deal with the complaint, and there are no grounds that exist under clause 92 to not deal with the complaint, the Commissioner must start an investigation under clause 101.

Clause 92 - Grounds for not dealing with complaints

524. This clause provides grounds that may form the basis for a decision by the Commissioner to cease dealing with a complaint. Subclause 92(1) lists circumstances in which the Commissioner may decide to cease dealing with a complaint. The Commissioner may rely on one or more circumstance(s). The listed circumstances are intended to prevent regulatory duplication and limit unnecessary use of time and resources. For example, the Commissioner may decide to not deal with a complaint that is vexatious, where the complainant fails to provide further information requested by the Commissioner within a specified period, or where the matter is being resolved through conciliation or an external dispute resolution scheme recognised under clause 131, regardless of whether the respondent and the complainant agree to do so.

525. Subclause 92(2) ensures transparency by requiring the Commissioner to give a written notice to the complainant if the Commissioner decides to not deal with a complaint under the listed circumstance(s). The written notice must outline the Commissioner's decision and the reasons for it, as well as the complainant's review rights under Part 6.2.

526. Subclause 92(3) requires the Commissioner to provide a copy of the notice to the respondent regarding the Commissioner's decision to not deal with a complaint, if the Commissioner has previously notified the respondent of the complaint.

Clause 93 - Admissibility of things said or done in conciliation

527. This clause provides that anything said or done in the course of conciliation is not admissible in relevant legal proceedings under this Bill or any other law. The exception is where participants otherwise agree, or when the conduct occurred during the course of conciliation constitutes an offence or civil contravention.

528. This clause encourages Scheme entities to fully commit to conciliation by encouraging frank discussions in order to resolve disputes. This aligns with the standard protections for matters and parties involved in conciliation processes.

Division 2 – General complaints

529. The Division establishes a mechanism for general complaints, which provides a means for members of the general public or Scheme entities to raise concerns with the Commissioner on the operation and administration of the Scheme. This mechanism will help the Commissioner to identify any systemic issues in the Scheme, as well as providing an avenue for complaints from individuals impacted by decisions to share data under the Scheme.

530. General complaints under this Division supplement existing avenues for redress under other schemes. For example, an affected person may also complain about government activities to the Commonwealth Ombudsman, to other Ombudsmen and regulators, or to the Information Commissioner about suspected mishandling of their personal information.

531. The inclusion of general complaints in this Bill supports a 'no wrong door' approach to engaging with the Australian Government. The operation of clause 107 allows general complaints received under this Division to be transferred to other regulatory bodies, such as the Information Commissioner.

Clause 94 - Making general complaints

532. This clause provides a separate complaints mechanism under the Scheme for individuals, non-Scheme entities, and for Scheme entities on matters that do not involve breaches under the Bill or a data sharing agreement. This clause provides a means for any person to raise issues on the administration or operation of the Scheme with the Commissioner. This intends to allow members of the general public to raise concerns and issues, including where their personal information may have been shared under a data sharing agreement. For example, a complainant may raise concerns about the details of a particular data sharing agreement, or the accreditation of a particular Scheme entity due to their conduct in other schemes.

Clause 95 - Dealing with complaints

533. This clause sets out the powers of the Commissioner when dealing with general complaints. The Commissioner may make preliminary inquiries of any person or entity, request additional information, and arrange conciliation if appropriate. Conciliation is encouraged where possible as it maximises the autonomy of the parties to resolve the complaint. In accordance with the Attorney-General's Department's *Your Guide to Dispute Resolution 2014,* conciliation is suitable where participants want a third person to assist in the discussion for participants to reach an agreement on technical and legal issues, being advised on the facts in dispute, while having the autonomy to control the outcome and agreement reached. This intends to guide and empower participants to resolve complaints through less formal means before formal proceedings are pursued as an option.

534. If the complaint gives the Commissioner reasonable cause to believe that an entity has breached the Bill or a data sharing agreement, the Commissioner may start an investigation under

clause 101. The Commissioner may also exercise other powers under this Bill, including conducting an assessment under clause 99, or transferring the complaint to a body better placed to address it under clause 107.

535. The Commissioner may take no action with regard to a general complaint if satisfied that none is required; for example, because the complaint is vexatious or unsubstantiated. While there are no specific grounds prescribed for not dealing with a general complaint made under clause 94, the grounds for not dealing with a scheme complaint under clause 92 provides non-exhaustive guidance when considering whether action should be taken. There are also no prescribed requirements on the process for dealing with general complaints, such as timeframes and notifications. This is intended to give the Commissioner greater flexibility in handling general complaints, including the ability to tailor their internal complaints handling policy and processes to the volume and types of general complaints.

Clause 96 - Admissibility of things said or done in conciliation

536. This clause provides that anything said or done in the course of conciliation is not admissible in any legal proceedings, unless otherwise agreed to by the parties or where the conduct occurred during the course of conciliation constitutes an offence or civil contravention.

537. This clause has a similar scope of protection as clause 93 in relation to scheme complaints. It allows parties to the complaint to fully commit to conciliation and aligns with standard protections for matters and parties involved in conciliation.

Part 5.4 – Assessments and investigations

538. This Part establishes mechanisms for the Commissioner to monitor, assess and gather information about the operation of the Scheme and Scheme entities within it.

Clause 99 – Assessments

539. Subclause 99(1) empowers the Commissioner to assess whether a Scheme entity's activities are consistent with the requirements of the Bill. Assessments are intended to be constructive, regular processes that support voluntary compliance and provide assurance to the Commissioner that the Scheme is operating as intended.

540. Subclauses 99(2) to (4) relate to conduct of assessments by the Commissioner.

541. The Commissioner may undertake an assessment in any manner they consider appropriate. This may include inviting submissions, and exercising their information gathering and monitoring powers (refer clauses 104 and 109). This non-prescriptive approach allows the Commissioner to adapt assessments to different circumstances and Scheme entities, as well as update and improve on the assessment processes and compliance targeting in response to the Scheme's maturity and development over time. For instance, assessments may focus on compliance with specific aspects of this Bill, such as application of a particular data sharing principle (refer clause 16), or in line with the Commissioner's general regulatory priorities and activities.

542. Subclause 99(1) makes it clear that the Commissioner may assess the conduct of former Scheme entities, provided that the conduct being assessed occurred while the entity was a Scheme entity. This supports the integrity of the Scheme, and ensures former Scheme entities are accountable for any conduct engaged in while participating in the Scheme.

Clause 100 – Notices of assessment

543. To ensure procedural fairness, clause 100 requires the Commissioner to give a Scheme entity notice before starting, and on the completion of, an assessment of the operations of that entity.

544. Assessments are intended to be collaborative processes between the entity and Commissioner. To facilitate this approach, notices are to be given before starting assessments and must specify their intended scope. This will allow Scheme entities to make any preparations necessary to facilitate the assessment and respond to the scope of assessment such as requesting that the assessment cover other matters, if desired. The Commissioner will take the response into account, but is not required to agree to the entity's proposed scope of assessment.

Clause 101 - Investigations

545. Investigations provide a means for the Commissioner to determine whether an entity is breaching or has breached requirements of the Scheme. Under clause 101, investigations occur in response to a scheme complaint (as defined in clause 88), on the Commissioner's own initiative, or as directed by the Minister.

546. Subclause 101(1) requires that the Commissioner investigate a scheme complaint unless a ground exists to cease dealing with the complaint under clause 92. In the absence of the Commissioner being satisfied that a listed circumstance under subclause 92(1) exists, such as where it is not appropriate to deal with the complaint by conciliation or an external dispute resolution scheme, or those mechanisms have failed to resolve the complaint, the Commissioner must investigate the complaint.

547. Subclause 101(1A) requires the Commissioner to investigate conduct of an entity engaged in while the entity is or was a Scheme entity, if directed by the Minister. Subclause 101(1B) clarifies when the Minister has the power to direct such investigation. The Minister may direct an investigation of an entity in respect of which the Minister is or was the accreditation authority, and the Minister has reasonable suspicion that the entity has or is proposing to breach requirements under the Bill or a data sharing agreement. The investigation can be carried out while the entity is still accredited under the Scheme or is no longer a Scheme entity.

548. Subclause 101(2) specifies that the Commissioner may investigate an entity on the Commissioner's own initiative where they hold a reasonable suspicion that the entity is breaching or is proposing to breach, this Bill or a data sharing agreement. This means that the Commissioner does not need to wait for a scheme complaint before investigating an entity that was or is a Scheme entity. Such reasonable suspicion could be formed based on a tip-off by an employee of the entity, a general complaint, information received from other regulators, information gathered during an assessment, or a pattern of breaches or data reporting discrepancies across the Scheme that provide a realistic likelihood of non-compliance. There is no requirement to form a view regarding the entity's intention of breaching the Bill or a data sharing agreement, provided that the Commissioner has reason to suspect the occurrence or potential occurrence of a breach.

549. Subclause 101(3) provides that the Commissioner may investigate former Scheme entities if the conduct being investigated occurred at a time when the entity was still a Scheme entity. This supports scheme integrity as breaches may not come to light immediately after they occur.

550. Subclause 101(4) identifies situations in which the Commissioner may choose to cease an investigation. For an investigation triggered by a scheme complaint, the Commissioner may stop the investigation if satisfied that one or more grounds for not dealing with the complaint apply under clause 92.

551. If an investigation has commenced under the Minister's direction, the Commissioner may stop investigating if the Minister no longer reasonably suspects that the entity has breached or is proposing to breach this Bill or a data sharing agreement, and the Minister informs the Commissioner. This situation could arise where the Commissioner reports to the Minister information obtained during an investigation which sufficiently satisfies the Minister of the

entity's compliance under the Bill or a data sharing agreement, and the Minister informs the Commissioner of that fact. Otherwise, the Commissioner may cease the investigation if they consider it appropriate to do so.

552. Similarly, if an investigation has commenced under the Commissioner's own initiative, the Commissioner may stop investigating when the Commissioner no longer reasonably suspects the entity has breached the Bill or a data sharing agreement, or otherwise considers it appropriate to do so. Circumstances where it would be appropriate to cease an investigation may include when additional information comes to light which demonstrates the entity is compliant with its obligations, or the complaint which triggered the investigation was not made in good faith.

553. Subclauses 101(5) to 101(7) contain procedural matters for how the Commissioner may undertake investigations, such as the ability to conduct an investigation in any manner the Commissioner considers appropriate. The Commissioner may obtain information from any person and make any inquiries that the Commissioner considers appropriate. This may involve requiring a person to give information or document under clause 104 or exercising powers available under the *Regulatory Powers Act* to investigate certain breaches (refer clause 110). Where the Commissioner invites submissions in relation to an investigation, they must have regard to any submissions made in response to the investigation.

554. This clause applies to entities, rather than Scheme entities, so the Commissioner may investigate non-compliance with their power to compel production of information in clause 104, which applies to current and former Scheme entities as well as other persons. Clauses 102 and 103 take the same approach as they flow from investigations under clause 101, as do certain consequences of a determination of breach set out in later clauses.

Clause 102 - Determination on completion of investigation

555. This clause requires the Commissioner to make a written determination setting out findings of an investigation conducted under clause 101, after its completion.

556. Subclause 102(1) prescribes the content to be included in a determination. 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, or is proposing to breach, the requirements of this Bill or a data sharing agreement. If the Commissioner finds a breach has occurred or is occurring, or is proposed to occur, the determination will also describe what regulatory or enforcement action the Commissioner intends to take to address the situation.

557. The determination, along with other notice requirements, will be provided to the relevant entity under clause 103, to inform on outcomes from the investigation. Subclause 102(2) provides that the Commissioner may also publish determination, for example when they relate to a breach which may impact other Scheme entities. A decision to make a determination publicly available, for any period of time, is a reviewable decision (refer clause 118).

558. Subclause 102(2A) ensures the Minister is informed of the outcome of an investigation that commenced under the Minister's direction. It requires the Commissioner to give the Minister a copy of the determination of an investigation conducted under the Minister's direction under subclause 101(1B) after completion of the investigation.

559. Subclause 102(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 Scheme entity provides evidence that changes the Commissioner's opinion as to whether the breach has occurred.

560. Subclause 102(4) clarifies that determinations made under this clause are not legislative instruments within the meaning of subsection 8(1) of the *Legislation Act*.

561. Certain enforcement actions in this Bill, such as issuing infringement notices and seeking injunctions or judicial penalties, rely on a determination of breach first being made by the Commissioner.

Clause 103 - Notices relating to investigation

562. Clause 103 sets out the notice requirements relating to investigation to ensure procedural fairness. Subclause 103(1) and (2) provides for a notice requirement before commencing an investigation. The Commissioner must give entities notice providing the intended scope of an investigation before commencing it.

563. Subclause 103(3) outlines the required actions following the completion of investigation. The Commissioner must also give determinations made under clause 102 to the entity that was investigated upon completion of that investigation. In addition to the requirement that the Commissioner must give the entity the determination under clause 102 in relation to the investigation setting out the Commissioner's opinion and reasons, this clause requires the Commissioner to also include information on the entity's review rights under Part 6.2 if the Commissioner decides to make the determination publicly available under subclause 102(2). This will provide a clear outcome from each investigation, and clarify next steps, if any.

564. 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 this would tend to disclose sensitive details about the data or processes under investigation.

565. Subclause 103(3A) requires the Commissioner to give written notice to the relevant entity and complainant if it decides to cease an investigation triggered by a complaint. This mirrors subclause 92(2), which requires the Commissioner to give written notice to affected entities if it decides to cease dealing with a complaint.

566. Subclause 103(4) provides that 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.

Clause 103A - Recommendations

567. Clause 103A allows the Commissioner to give recommendations to a Scheme entity upon completion of an assessment or investigation. These recommendations may relate to any action the Commissioner considers appropriate for the entity to take. This further supports the Commissioner's functions to provide guidance on the Scheme.

Part 5.5 – Regulatory powers and enforcement

568. This Part provides the Commissioner's regulatory powers to monitor and enforce the requirements of the 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 99), recommendations (refer clause 111), and activities under the Commissioner's other functions (refer clause 42).

Clause 104 - Power to require information and documents

569. Clause 104 empowers the Commissioner to compel the production of information and documents relevant to the exercise of the Commissioner's regulatory functions (refer clause 45)

from any person. This is known as a 'notice to produce' power, or an information gathering power.

570. The Commissioner's information gathering power supplements their monitoring and investigation powers derived from the *Regulatory Powers Act*, which allow for the collection of information and documents when physically inspecting a premises (see clauses 109 and 110). Being able to collect information and documents remotely is less invasive and often more practical than gathering information on-site. This supports a proportional approach to managing non-compliance and enforcing the Scheme.

571. Subclause 104(1) enables the Commissioner to make requests to any person, so long as they reasonably believe the person has relevant information. This coverage mirrors the monitoring and investigation powers under the *Regulatory Powers Act*. Inclusion of non-Scheme entities is necessary given the scope of civil penalty provisions and criminal offences in the Bill which cover, for example, unauthorised sharing of data with entities that are not accredited.

572. The information or documents requested must be relevant to the exercise of the Commissioner's regulatory functions. These functions include monitoring and investigating compliance with the Scheme and data sharing agreements, 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 public interest certificate issued by the Attorney-General under clause 106.

573. 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.

574. Subclauses 104(2) and 104(3) introduce penalties for failure to comply with subclause 104(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.

575. The consequences for breach of the penalty or offence provisions established by this clause – up to 30 penalty units or up to six months imprisonment, respectively – align with analogous laws and the *Guide to Framing Commonwealth Offences*. The penalty is comparable to a similar offence for failure to provide information at section 60 of the *Privacy Act*, where the penalty is imprisonment for 12 months or 20 penalty units for an individual and 100 penalty units for a body corporate.

576. Consistent with the *Guide to Framing Commonwealth Offences*, the Bill sets maximum penalties; a court will determine what is appropriate on a case-by-case basis. The maximum caps set have regard to the penalties of other frameworks, such as the *Privacy Act* and *Online Safety Act 2021* (Cth), as well as contemporary offences for mishandling public sector and consumer data, taking into account that the person may be an individual. This approach intends for the Scheme to align with other applicable frameworks, without duplicating them, as well as with community expectations.

577. Subclause 104(4) explains the scope of the Commissioner's power to deal with documents obtained under this clause.

Clause 105 - Legal professional privilege

578. This clause provides for the circumstances and corresponding implications where legal professional privilege is not a basis for refusing to provide information or documents sought by the Commissioner under clause 104.

579. Subclause 105(1) promotes effective oversight and regulation of the Scheme by preventing legal professional privilege being used to deny the Commissioner access to materials relevant to an investigation under certain circumstances. These circumstances are where the communication is legal advice given to a Minister or a Commonwealth body, or a communication between a designated individual for a Commonwealth body and another person or body. This means that Commonwealth entities are not able to rely on grounds of legal professional privilege to protect against disclosure of information that has been required by the Commissioner under clause 104.

580. Legal professional privilege is an important right that ought to be abrogated only where there is strong justification. Abrogation is justified here in order to serve higher public policy interests in the effective regulation and enforcement of the Bill, to ensure integrity of the Scheme and protection of public sector data. The abrogation of legal professional privilege under this clause is therefore confined to limited circumstances involving a Commonwealth body, recognising that the Commissioner is an independent statutory office holder of the Commonwealth.

581. This limited abrogation of legal professional privilege is necessary for the Commissioner to perform functions under the Scheme, as Scheme entities (a large number of which are Commonwealth 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 alternative source. The limited abrogation of this privilege will allow the Commissioner to effectively hold Scheme entities that are Commonwealth bodies to account for their handing of public sector data, an outcome in which there is a strong public interest. This is consistent with the objectives of enhancing transparency and accountability by the Australian Government under the Scheme.

582. This approach is also informed by other regulators' experiences, whose investigatory activities have been delayed or hampered by an inability to access relevant information, and the difficulty of 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).

583. The application of subclause 105(1) is based on meeting the threshold to require information or documents under subclause 104(1), which takes into account the limits placed on the Commissioner's power to require information and documents (refer clause 106). The Commissioner may only seek information and documents under clause 104 where they hold a reasonable belief the materials are relevant to one of their regulatory functions, and not in the circumstances set out in clause 106.

584. Subclause 105(2) offers a level of protection that legal professional privilege would otherwise provide if not for subclause 105(1), by providing a 'use immunity'. The effect of this subclause is that information and documents given to the Commissioner pursuant to clauses 104, 105(1) and 106, and the act of giving them, are not admissible in evidence to be used against a person in proceedings involving imposition of a penalty. This is a broad use immunity, as it protects all persons, not only the person who produced the materials or is entitled to claim the privilege, and applies in both civil and criminal proceedings. The immunity does not extend to derivative use, as that would exclude all evidence discovered in reliance on leads from the disclosure (in

contrast to the use immunity that renders inadmissible only the evidence that was disclosed under this provision).

585. Like other Australian regulators, this approach has been taken to constrain the abrogation of the privilege without frustrating the point of empowering the Commissioner to compel production of information, enabling an effective regulation and enforcement of the Scheme. Courts retain their usual powers to exclude evidence that would render proceedings unfair. Further information on use immunities in Commonwealth laws is found in the Australian Law Reform Commission's *Report 129: Traditional Rights and Freedoms: Encroachment by Commonwealth Laws* (2016) chapters 11 and 12.

586. Subclause 105(3) clarifies that subclause 105(1) does not affect other claims of legal professional privilege which may be made over the relevant information or document.

587. This clause also does not abrogate legal professional privilege outside of the context of the request for materials under clause 104, for example legal advice obtained for the purpose of proceedings that follow an investigation. This clause does not displace the common law privilege against self-incrimination or affect Parliamentary privilege (refer subclause 106(4)).

588. Subclauses 105(4) and 105(5) expand on the process involved when a person claims on grounds of legal professional privilege to prevent the disclosure of information that has been required by the Commissioner under clause 104. A person seeking to protect privileged information from disclosure must give written notice to the Commissioner claiming legal professional privilege that would otherwise be available if subclause 105(1) did not operate. The Commissioner must withdraw the notice to produce unless satisfied that requiring the person to give the information is reasonably necessary and proportionate to the investigation. The Commissioner must also ensure that the information and documents are held securely and destroyed when the investigation ends. Subclause 105(4) does not apply if there are no reasonable grounds for the person's claim.

589. The Commissioner may only disclose the information or documents to certain persons when satisfied that the disclosure is reasonably necessary for the purposes of the investigation. The persons whom the Commissioner may subsequently disclose privileged information to must be either a member of the staff under clause 47, or a contractor or consultant engaged under clauses 48 and 49, or otherwise providing services to the Commissioner.

590. This clause 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*.

Clause 106 – Limits on power to require information and documents

591. Clause 106 limits the Commissioner's information gathering power in clause 104. 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.

592. Subclause 106(1) prevents the Commissioner from requesting information from excluded entities (refer subclause 11(3)). The information that these entities hold may have particular national security or law enforcement sensitivities, so it should not be provided except when the relevant entity agrees. Subclause 106(1) does not prevent these entities from providing information to the Commissioner if they choose to.

593. Subclause 106(2) prevents the Commissioner from requesting information that is subject to a certificate issued by the Attorney-General under subclause 106(3), stating that provision of that information would be contrary to the public interest. It would not be appropriate for the Commissioner to receive information that could prejudice any of the listed circumstances:

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 a person's safety. As the Cabinet Minister responsible for these matters, the Attorney-General forms the opinion that giving information or document would be contrary to the public interest and issues certificates under this clause.

594. This approach aligns with that of certain other regulators with information gathering powers such as the Information Commissioner, the Commonwealth Ombudsman, and the Law Enforcement Integrity Commissioner.

595. If the Commissioner receives a certificate under subclause 106(3), any existing requests under clause 104 relating to the relevant information or documents are void.

596. Subclause 106(4) clarifies that the information gathering power in clause 104 does not affect Parliamentary immunities or privileges, within the meaning of the *Parliamentary Privileges Act 1987*.

Clause 107 - Transfer of matters to appropriate authority

597. Clause 107 allows the Commissioner to request a body prescribed by subclause 108(2) to take carriage of a matter where the body is better placed to manage and/or resolve it. The Commissioner may do this at any time while dealing with a matter under the Bill. 'Matter' is intended to be interpreted broadly to include matters arising from the Commissioner's performance of functions under the Scheme (refer clause 42) and includes dealing with a scheme complaint or general complaint.

598. Enabling transfer of matters to appropriate regulators will reduce inefficiency and duplication of work or matters. 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 Information Commissioner deal with the matter instead of the Commissioner under this clause.

Clause 108 - Authorisation for Commissioner to disclose and receive information

599. As part of performing functions under this Bill, clause 108 authorises the Commissioner and their staff to exchange information with a prescribed body, for the purpose of assisting that body to perform its functions or exercise its powers.

600. Subclause 108(1) provides the preconditions to the disclosure of information or a document to prescribed bodies, in particular the preconditions are that the information or document is collected by the Commissioner or staff member in the course of performing functions under this Bill, which will assist the prescribed body's functions or its exercise of powers, and does not have a claim in legal professional privilege under subclause 105(4). This means that information or a document protected by legal professional privilege under clause 105 is not authorised to be disclosed under subclause 108(1). This is consistent with other Commonwealth laws and the treatment of information with legal professional privilege.

601. Prescribed bodies are listed in subclause 108(2), which covers a range of regulatory and integrity bodies. The Minister may prescribe additional bodies with which the Commissioner may exchange information in rules under paragraph 108(2)(o). Such rules will enable the Commissioner to continue to effectively oversee and regulate the Scheme in the event of machinery of government changes, and the introduction of other relevant bodies.

602. Subclause 108(3) authorises the Commissioner or staff member to receive information or a document disclosed by a prescribed body for the purposes of assisting the Commissioner or staff member to perform their functions or exercise their powers under the Scheme.

603. Similar to clause 107, this clause facilitates ongoing cooperation among regulators to resolve issues, and may support collaborative activities such as the development of joint guidelines (refer clause 127). Such powers 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 public sector data securely, the Commissioner may need information from other bodies (refer clause 76). Similarly, the Commissioner may identify and need to share information that gives rise to a matter within the remit of another regulatory body (such as fraud, or the mishandling of personal, protected, or consumer information) while monitoring and enforcing compliance with the Scheme.

604. This clause is a regulatory mechanism, distinct from the authorisation in clause 13 which enables data custodians to share public sector data under the Scheme. It aligns with powers of other regulators such as the e-Safety Commissioner. Note also that the Commissioner has the power to do anything necessary or incidental to their legislated functions (refer clause 42), so the Commissioner may communicate with Scheme entities in the course of administering the Scheme without needing to rely on this clause.

605. This clause operates as an 'authorisation by law' for the purposes of the *Privacy Act*, where the information exchanged involves personal information.

606. The power of the Commissioner (and their staff) to disclose and receive information under this clause does not impact or override secrecy provisions which may prevent listed entities disclosing their information.

Clause 109 – Monitoring powers

607. This clause grants the Commissioner standard monitoring powers under Part 2 of the *Regulatory Powers Act* in relation to certain provisions of this Bill.

608. 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.

609. Subclause 109(1) grants the Commissioner standard regulatory monitoring powers in relation to all civil penalty provisions under this Bill and criminal offence provisions relating to unauthorised sharing, collection or use of data in this Bill, as well as the responsibilities of Scheme entities under Chapter 3 of this Bill.

610. Subclause 109(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 Scheme. This includes information provided in relation to accreditation (refer clause 31 and Part 5.2), and information provided for the purpose of preparing the Commissioner's annual report (refer clause 34).

611. Subclause 109(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.

612. Subclause 109(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. The person assisting must have the necessary skills, qualifications or experience, consistent with the requirements under subclause 45(2) in relation to persons assisting the Commissioner in the performance of their regulatory functions.

Clause 110 - Investigation powers

613. Clause 110 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 Scheme entities in Chapter 3. Investigation powers may only be exercised in relation to an investigation under clause 101, by people identified in this clause (or their delegates).

614. 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.

615. Subclause 110(1) specifies the matters in relation to which the Commissioner may exercise investigatory powers. Consistent with paragraph 110(1)(b), these powers extend to investigating third parties who assist a Scheme entity to contravene the Bill, or who are accessories to an offence after the fact (refer clause 9, definition of 'offence against this Act').

616. Subclause 110(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.

617. Subclause 110(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 112 - Directions

618. Clause 112 empowers the Commissioner to issue a written direction to a Scheme entity that requires them to act or cease acting in a particular manner, which must be complied with. Directions can 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. This clause sets out circumstances where directions may be issued.

619. The first circumstance, outlined in subclause 112(1), is in situations of urgency to address non-compliance or an emergency or high risk situation. The Commissioner may issue directions either where the Scheme entity, or another entity, has acted or is likely to act inconsistently with this Bill or a data sharing agreement, or where an emergency or high risk situation has arisen or is likely to arise. There must also be an element of immediate necessity for an entity to take, or not take, an action in order to address or prevent the situation.

620. What may constitute a situation of urgency or an emergency or high risk situation is assessed on a case-by-case basis. Such a situation exists when the Commissioner reasonably believes a threat has arisen that poses serious risks to activities or participants in the Scheme if not promptly addressed. Some factors that would give rise to such situations are where the negative consequences from not issuing a direction would likely have a significant impact on the privacy and security of individuals or entities, cause irreparable harm to individuals or entities, lead to the breach of other laws, or likely to become a matter of national concern. 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 the unauthorised sharing or release of sensitive data, that is likely to compromise the integrity or wellbeing of entities to which the data relates.

621. The second circumstance, outlined in subclause 112(2), is when the Commissioner is satisfied a Scheme entity has acted or is likely to act inconsistently with this Bill or a data sharing agreement, and where there is a necessity for the entity to take, or not take, an action. The Commissioner may detect a breach in the course of an assessment or investigation, and in doing so be satisfied that the entity has acted, or is likely to act, in a way that is inconsistent with the Bill or a data sharing agreement. 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, a direction could be issued to correct non-compliant or contributory behaviours, and mitigate associated risks or harm.

622. The third circumstance, outlined in subclause 112(3), enables the Commissioner to issue directions to accredited entities to deal with scheme data in a certain way to mitigate risks associated with the 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.

623. Subclause 112(4) provides that the specified actions in a direction may include providing another entity with access to scheme data. This is appropriate in the circumstance where a Scheme entity's relevant functions to which the project relates have been transferred to another Scheme entity due to a machinery of government change, and the continued operation of the existing data sharing arrangement without further action is likely to lead to non-compliance with this Bill or a data sharing agreement.

624. Subclause 112(5) states the consequences for breach of a direction, which is up to 300 penalty units. This aligns with analogous laws and the *Guide to Framing Commonwealth Offences*. Consistent with the *Guide to Framing Commonwealth Offences*, the Bill sets maximum penalties; a court will determine what is appropriate on a case-by-case basis. The maximum cap balances the penalties of other frameworks, such as the *Privacy Act* and *Online Safety Act 2021* (Cth), as well as more contemporary offences for mishandling public sector and consumer data. This approach intends for the Scheme to align with other applicable frameworks, without duplicating them, as well as with community expectations.

625. Subclause 112(6) clarifies that any direction made under this clause is not a legislative instrument within the meaning of subsection 8(1) of the *Legislation Act*.

626. Directions will allow the Commissioner to act quickly to protect the integrity of the 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, targeting both urgent and less urgent circumstances.

627. The Commissioner's directions power is not intended to impinge upon, or overlap with, judicial injunction powers. Instead, the Commissioner's directions power are 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. Other than urgent directions issued under subclause 112(1), other directions may also be reviewed on their merits, and the Administrative Appeals Tribunal may make an order to stay directions while under review (refer clause 118).

Clause 113 – Civil penalty provisions

628. 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.

629. Subclause 113(2) clarifies that penalties may be sought only once the Commissioner has investigated and determined that a civil penalty provision has been breached (see clauses 101 and 102).

630. This clause also clarifies procedural matters, including the federal, State and Territory courts that may hear matters arising under this Bill.

Clause 114 – Infringement notices

631. Clause 114 allows the Commissioner to issue infringement notices under Part 5 of the *Regulatory Powers Act*.

632. The Commissioner may issue an infringement notice if they have determined that a breach has occurred, or is occurring (see clauses 101 and 102). 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.

633. 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 115 – Enforceable undertakings

634. Clause 115 empowers the Commissioner to accept and enter into enforceable undertakings under Part 6 of the *Regulatory Powers Act*.

635. 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 Scheme. The Commissioner may enter into undertakings in various situations, including when they have assessed a Scheme entity (see clause 99) and identified ways in which the entity could better comply with requirements.

636. 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.

637. In the interest of transparency, the Commissioner may publish enforceable undertakings made under this clause.

Clause 116 – Injunctions

638. Clause 116 enables the Commissioner to seek injunctions from specified federal and jurisdictional courts to enforce obligations arising under civil penalty provisions of the Bill. Such injunctions are made under Part 7 of the *Regulatory Powers Act*.

639. 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 a temporary remedy while courts hear related matters.

640. The Commissioner must have determined a breach has, or is occurring, under clause 102 before seeking an injunction.

Chapter 6 – Other matters

Part 6.1 – Introduction

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

Clause 117 – Simplified outline of this Chapter

642. Clause 117 provides a simplified outline of Chapter 6 of the Bill, which provides for various matters relevant to the operation of the 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

643. This Bill provides tailored redress mechanisms for the Scheme, including an avenue for scheme complaints and general complaints, and provision for administrative and judicial review. Avenues for redress under other frameworks and bodies continue to be available, such as avenues under the *Privacy Act* (for example, making a privacy complaint) and engagement with the Commonwealth Ombudsman.

644. This Part sets out internal and external merits review available under the Scheme.

645. Reviewable decisions are subject to merits review by a 'reviewer' (which may be the Minister or the Commissioner) or by the Administrative Appeals Tribunal. Only decisions that are adverse to the interests of a person are subject to merits review. Decisions under the Bill that are not subject to merits review may be subject to judicial review. Judicial review may be available under the *Administrative Decisions (Judicial Review) Act 1977*, section 39B of the *Judiciary Act 1903*, or section 75(v) of the Constitution.

Clause 118 – Reviewable decisions

646. Clause 118 identifies specific decisions of the Minister and Commissioner under the Scheme that are subject to merits review. Subclause 118(1) specifies the four types of accreditation decisions made by the Commissioner that are reviewable decisions. The Commissioner is responsible for making decisions about the accreditation of entities as ADSPs, and decisions about the accreditation of entities that are not bodies politic, Commonwealth bodies, State bodies or Territory bodies as users. Decisions by the Commissioner not to accredit an entity as an ADSP or as a user, or to accredit but with conditions of accreditation, may or will be adverse to the entity, and are therefore subject to merits review. Likewise, a decision by the Commissioner to impose or vary a condition of accreditation after accreditation, will or may be adverse to the entity, and is therefore subject to merits review. A decision by the Commissioner to remove a condition of accreditation can never be adverse to the interests of the entity concerned, and is therefore not subject to merits review. A decision to suspend or cancel an entity's accreditation is subject to merits review.

647. The accreditation of an entity as an ADSP must be renewed every five years (the accreditation of an entity as a user does not need to be renewed). Subclause 81(8) requires the Commissioner to suspend the accreditation of an entity as an ADSP that fails to apply for renewal of its ADSP

accreditation within five years of the initial accreditation (or subsequent renewal), and to suspend or cancel the accreditation of an entity as an ADSP if the Commissioner decides under clause 84 not to renew the accreditation of an entity as an ADSP. A decision by the Commissioner under subclause 81(8) is mandatory in nature and, in accordance with ARC Guidance is unsuitable for merits review. Subclause 118(2) therefore provides that decisions by the Commissioner under subclause 81(8) are not subject to merits review. Importantly, however, a decision by the Commissioner not to renew an entity's accreditation as an ADSP, or to renew the accreditation with conditions of accreditation (even if these conditions of accreditation were previously imposed on the entity's accreditation) are subject to merits review (refer paragraph 118(1)(d)).

648. Part 5.3 of the Bill provides for two types of complaints to be made to the Commissioner – scheme complaints under Division 1 and general complaints under Division 2. Scheme complaints may be made by a Scheme entity in the circumstances specified in clause 88 of the Bill. The Commissioner must deal with a complaint unless the Commissioner is satisfied that a ground for not dealing with the complaint in clause 92 applies, either before the Commissioner commences an investigation relating to the complaint (under subclause 91(2)) or after the Commissioner has commenced an investigation (under paragraph 101(4)(a)). In either case, a decision by the Commissioner not to deal with a scheme complaint is subject to merits review (refer paragraph 118(1)(e)).

649. The Commissioner has a broad discretion under clause 95 of the Bill to deal with general complaints made to the Commissioner under clause 94, including by taking no action in relation to such complaints. Decisions taken by the Commissioner under clause 95 in relation to general complaints are not subject to merits review. This is consistent with ARC Guidance, because such decisions are preliminary in nature. Under clause 107, in certain circumstances the Commissioner may transfer scheme complaints or general complaints to an agency or body mentioned in clause 108. A decision by the Commissioner to transfer a general complaint is not subject to merits review. This is consistent with ARC Guidance, because such decisions are preliminary in nature.

650. The Commissioner has powers under Part 5.4 of the Bill to conduct assessments and investigations. A decision to conduct an assessment or an investigation is not subject to merits review. This is consistent with ARC Guidance, because such decisions are preliminary in nature and are of a law enforcement nature. On completion of an investigation, under subclause 102(1) the Commissioner must make a written determination setting out matters specified in subclause 102(1). Under subclause 102(2), the Commissioner has discretion to make such determinations public. A decision to make a determination public may be adverse to the interests of an entity. Therefore, a decision under subclause 102(2) to make a determination publicly available is subject to merits review (refer paragraph 118(1)(f)). However, a decision by the Commissioner not to make a determination publicly available is not subject to merits review, because such a decision will not be adverse to the interests of an entity.

651. The Commissioner has powers under Part 5.5 of the Bill to make decisions to: require the production of information and documents (refer clause 104); exercise monitoring powers (refer clause 109) and investigation powers (refer clause 110); give urgent written directions (refer subclause 112(1)); apply to a court for an order in relation to civil penalties (refer clause 113); accept and apply to a court to enforce enforceable undertakings (refer clause 115) and apply to a court for injunctions (refer clause 116); and issue infringement notices (refer clause 114). None of these decisions are subject to merits review. This is consistent with ARC Guidance. Requiring the production of information or documents, and deciding to exercise monitoring or investigation powers, are decisions of a law enforcement nature. It is not appropriate for decisions to approach a court to be subject to merits review, nor is it appropriate for a decision

to issue an infringement notice, which is in the nature of law enforcement, to be subject to merits review.

652. A decision by the Commissioner under subclauses 112(2) or 112(3) to issue a written direction to an entity is a reviewable decision (refer paragraph 118(1)(g)). However, a decision by the Commissioner to issue a written direction to an entity under subclause 112(1) is not a reviewable decision. A direction under subclause 112(1) may only be given if the Commissioner is satisfied that it is necessary for an entity to take actions immediately or as soon as practicable, or to stop taking actions the entity is currently taking or may take imminently. It is intended that such directions are complied with immediately, in order to ensure that shared data, or data to be shared, is properly protected. For example, if the Commissioner is satisfied that an accredited user is holding output in a manner that does not comply with the security requirements specified in the applicable data sharing agreement, the Commissioner may direct the accredited user under subclause 112(1) to improve security controls immediately. This direction would need to be complied with without delay, to avoid the risk that malicious third parties might access the output.

653. Decisions to give directions under subclause 112(1) are incompatible with external merits review for two reasons. Firstly, if external review of such a decision was sought, in many cases the only practical way to preserve the practical value of the applicant's right of review would be to stay the operation of the direction, pending a substantive review of the decision. A stay of the decision would undermine the purpose of subclause 112(1), which is to ensure that the Commissioner has the power to direct Scheme entities to take prompt action to protect public sector data when necessary. Secondly, because the Scheme imposes very strict limitations on how accredited entities may use ADSP-enhanced data or output, a direction given under subclause 112(1) would often require accredited entities to handle data in a manner that would otherwise be unlawful. Accredited entities directed under subclause 112(1) to take immediate action that, but for the direction, would be unlawful, would be placed in a difficult position if the entity seeks external merits review of the decision to give the direction.

654. It would not be possible to provide for internal merits review of decisions to give directions under subclause 112(1) because all such decisions must be made by the Commissioner personally (clause 50 provides that the Commissioner may not delegate their powers under clause 112).

655. Under Chapter 4 of the Bill, the Commissioner may decide to delegate powers and functions under clause 50 and to appoint members of the Council under clause 63. Consistent with ARC Guidance, neither of these decisions are subject to merits review.

656. Where a reviewable decision mentioned in subclause 118(1) is made by a delegate of the Commissioner, the Commissioner is the reviewer for the decision. If an application is made for reconsideration of such a decision, the decision may be reviewed by the Commissioner personally or by a delegate of the Commissioner. Where the original reviewable decision is made by the Commissioner personally, internal merits review of the decision is not available and an application for merits review must be made to the Administrative Appeals Tribunal under clause 122.

657. Subclause 118(2) specifies the three types of accreditation decisions made by the Minister that are reviewable decisions. The Minister is responsible for making decisions about the accreditation of bodies politic, Commonwealth bodies, State bodies and Territory bodies as users. Decisions by the Minister not to accredit an entity as a user, or to accredit but with conditions of accreditation, may or will be adverse to the entity, and are therefore subject to merits review. Likewise, a decision by the Minister to impose or vary a condition of accreditation after accreditation will or may be adverse to the entity and is therefore subject to

merits review. A decision by the Minister to remove a condition of accreditation can never be adverse to the interests of the entity concerned, and is therefore not subject to merits review. A decision to suspend or cancel an entity's accreditation is subject to merits review.

658. The Minister may decide under clause 137A to delegate any or all of the Minister's powers under Part 5.2 to the Commissioner. Consistent with ARC Guidance, this decision is not subject to merits review.

659. Where a reviewable decision mentioned in subclause 118(2) is made by the Commissioner as delegate of the Minister, the Minister is the reviewer for the decision. If an application is made for reconsideration of such a decision, the decision will be reviewed by the Minister personally. Where the original reviewable decision is made by the Minister personally, internal merits review of the decision is not available and an application for merits review must be made to the Administrative Appeals Tribunal under clause 122.

Clause 119 – Applications for reconsideration of decisions made by delegates of the reviewer

660. This clause establishes a formal process for internal merits review. A decision that is a reviewable decision under clause 118 may be internally reviewed if the decision was made by a delegate of the reviewer (refer clause 118, the reviewer could be the Commissioner or the Minister).

661. 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).

662. If a delegate has made a reviewable decision, subclause 119(1) allows an affected person to apply to the reviewer (the Commissioner or the Minister) for reconsideration of the decision. This internal review will be undertaken by the reviewer personally, or in the circumstance where the Commissioner is the reviewer, may also be undertaken by another delegate of the reviewer. The Commissioner may delegate functions and powers to members of staff (refer clause 50). The Minister may delegate functions and powers to the Commissioner (refer clause 137A).

663. Decisions made personally by the Commissioner (other than as a delegate) or the Minister cannot be reviewed internally, and affected persons must seek external review by the Administrative Appeals Tribunal (refer clause 122).

664. Under subclause 119(2), applications for internal review must be in an approved form (if any).

665. In circumstances where the Minister has made rules prescribing fees for the purpose of this clause, subclause 119(3) 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 taken not to have been made unless the prescribed fee is paid.

Clause 120 – Reconsideration by reviewer

666. Clause 120 applies where a reviewable decision (refer clause 118) is made by a delegate, and a person affected by the decision applies under clause 119 to the reviewer of the decision (the Minister or the Commissioner) seeking reconsideration of the decision. Under clause 120, the reviewer (who may be the Commissioner or a delegate of the Commissioner for decisions covered by subclause 118(1), and will be the Minister for decisions covered by subclause 118(2)) must reconsider the initial decision on the merits and then affirm the decision, vary the

decision or revoke the decision and substitute a new decision. The reviewer's decision has effect as if it had been made under the provision under which the original decision was made (refer subclause 120(2)).

667. Where a reviewer decides to vary the original decision, or to revoke the original decision and substitute a new decision, the reviewer may specify when the varied decision or new decision has effect (this could be at the time the original decision was made, or at the time of the reconsideration decision). Where the reviewer affirms the original decision, the original decision continues to have effect from the date it was made.

668. The reviewer must provide the applicant for reconsideration with written notice of the decision on reconsideration (refer subclause 120(3)). The reviewer must also provide the applicant with written reasons for the reconsideration decision within 28 days after making the decision (refer subclause 120(4)). The notice of the decision and the reasons for the decision do not need to be provided to the applicant at the same time.

669. Where the Minister is the reviewer for a reviewable decision made by the Commissioner as the Minister's delegate, the Minister must personally make the reconsideration decision. Where the Commissioner is the reviewer of a reviewable decision, the reconsideration decision may be made by the Commissioner personally or by another delegate of the Commissioner. However, where the reconsideration decision is made by a delegate, subclause 120(5) provides that the new delegate must not have been involved in the making of the original decision and must be at least the same level as the delegate who made the original decision. These requirements ensure that the decision on reconsideration involves a fresh consideration on the merits, and that the new delegate's decision is not influenced by the original decision.

Clause 121 – Deadline for reconsideration

670. Clause 121 imposes a timeframe for decisions on reconsideration. Reconsideration decisions must be made within 90 days of receiving an application for reconsideration under clause 119. If an application for reconsideration is purportedly made under clause 119 but the requirements of clause 119 are not met (for example, the application is not in the approved form made by the Commissioner for the purpose of clause 119), the 90 day timeframe under clause 121 does not commence. There is no provision for the applicant to agree to a longer period for the making of a reconsideration decision.

671. If a reconsideration decision is not made within the 90 day period provided for by subclause 121(1), and the reviewer has not informed the applicant of that decision in writing before the end of that period, subclause 121(2) operates to deem that the reviewer has affirmed the original decision. This permits the applicant to seek merits review by the Administrative Appeals Tribunal under clause 122. Clause 121 only requires the applicant to be informed of the decision on reconsideration before the end of the 90 day period. Written reasons for the decision may be provided to the applicant after the end of the 90 day period. However, subclause 120(4) requires reasons for a reconsideration decision to be provided within 28 after the making of the decision.

Clause 122 – Review by the Administrative Appeals Tribunal

672. This clause enables the Administrative Appeals Tribunal to review the merits of decisions that are reviewable under clause 118.

673. Clause 122 provides that a clause 118(1) reviewable decision made personally by the Commissioner, or a reviewable decision made personally by the Minister, may be reviewed by the Administrative Appeals Tribunal, without any need for internal reconsideration.

674. A subclause 118(2) reviewable decision made by the Commissioner as delegate of the Minister must be subject to internal reconsideration by the reviewer of the decision (that is, the Minister) before being reviewed by the Administrative Appeals Tribunal.

675. Subclause 118(1) reviewable decisions initially made by a delegate of the Commissioner must also be subject to internal review before being reviewed by the Administrative Appeals Tribunal.

676. If a reviewable decision is affirmed or varied upon reconsideration by the reviewer (or a delegate of the reviewer), an application may be made to the Administrative Appeals Tribunal under paragraph 122(b).

677. 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 – Extension of authorisations and attribution of conduct

678. This Part includes provisions about how conduct of individuals is attributed to entities and how the authorisations in Chapter 2 for Scheme entities to share, collect and use data extends to certain individuals and bodies corporate.

679. Responsibility of legal entities, such as bodies corporate, will be determined in accordance with other applicable laws, such as Part 2.5 of the *Criminal Code* and section 97 of the *Regulatory Powers Act*.

680. These clauses, together with other applicable laws, hold all Scheme entities accountable for actions within the Scheme, to a consistent standard.

Clause 123 – Designated individuals and designation

681. Subclause 123(1) includes a table that identifies individuals who are 'designated individuals' for entities, and defines the 'designation' of each of those individuals. For example, an APS employee of a data custodian is a designated individual for the data custodian, and the designation of that APS employee is the employee's duties as an APS employee. Where an individual or a body corporate is engaged by an accredited entity to perform services under an 'approved contract' (refer subclause 123(3), discussed below), that individual, or the employees, officers and members of that body corporate, are designated individuals of the accredited entity, and the approved contract determines the designation of those designated individuals.

682. Certain actions under the Scheme (such as entering into a data sharing agreement on behalf of a data sharing entity) may only be done by authorised officers of the relevant Scheme entity, or other authorised individuals. The appointment of authorised officers is covered by clause 137. Subclause 123(2) clarifies that, where an individual is an authorised officer of an accredited entity, or an individual authorised for the entity under subclauses 137(3) or 137(4), their designation as a designated individual includes both their designation under clause 137 and the designation they may have under another item of the table in subclause 123(1) – for example, their designation as an employee of the accredited entity.

683. Subclause 123(3) defines the term 'approved contract'. To be an approved contract, the contract must: (a) be between an individual and an accredited entity, or between a body corporate and an accredited entity; (b) be authorised in or approved under the relevant data sharing agreement; and (c) comply with any requirements in a data code, if a data code is made for the purposes of this clause. For example, an accredited user may have an ongoing contract with a body corporate to provide consulting services (the data analytics provider) in relation to data

analytics (the data analytics contract). The accredited user enters into two data sharing agreements with different data custodians. The first data sharing agreement authorises the data analytics contract. In the context of activities covered by the first data sharing agreement, employees of the data analytics provider are designated individuals of the accredited user, and their designation is determined by the scope of services in the analytics contract. However, the second data sharing agreement does not authorise the analytics contract and the data analytics contract is not approved under that agreement. In the context of activities covered by the second data sharing agreement, employees of the data analytics provider are not designated individuals of the accredited user.

Clause 124 – Extension of authorisations to share, collect or use data

684. Chapter 2 of the Bill provides authorisations for Scheme entities to share, collect and use data in certain circumstances. For example, clause 13 authorises a data custodian to share data with an accredited user if certain conditions are met. Subclause 124(1) provides that, generally, the authorisation provided in Chapter 2 to an entity extends to the designated individuals of that entity. For example, the authorisation provided to a data custodian to share data with an accredited user will also cover APS employees of the data custodian who perform activities as part of the process of making the data available to the accredited user, so long as the relevant activities are within the scope of the APS employees' duties.

685. Subclause 124(2) provides that the authorisation to designated individuals provided for in subclause 124(1) does not apply if that would be inconsistent with a condition of accreditation imposed on, or applicable to, the entity, or the terms of the applicable data sharing agreement. For example, an employee of an accredited user who is not an Australian citizen or permanent resident may be a designated individual of the accredited user. However, a condition of accreditation applicable to the accredited user may prohibit any employees that are not Australian citizens or permanent residents from collecting or accessing output. In these circumstances, subclause 124(1) would not extend the accredited user's authorisation to collect and use output to the employee.

686. Subclause 124(3) provides that, generally, where an accredited entity has an approved contract with a body corporate in the context of a particular data sharing agreement, the accredited entity's authorisation under Chapter 2 of the Bill to collect and use data extends to conduct of the body corporate, if the conduct is within the scope of the approved contract. For example, if an accredited user has a contract with a body corporate to provide analytics services and that contract is authorised by the relevant data sharing agreement, the accredited user's authorisation under Chapter 2 in relation to the use of data covered by the data sharing agreement extends to the body corporate, if the production of output authorised under the data sharing agreement is to be in part undertaken by the body corporate and within the scope of the approved contract.

687. However, subclause 124(4) restricts the operation of subclause 124(3) in some circumstances. Subclause 124(4) provides that the authorisation to a body corporate provided for in subclause 124(3) does not apply if that would be inconsistent with a condition of accreditation imposed on, or applicable to the accredited entity, the terms of the approved contract or the data sharing agreement for the project. For example, if an accredited user has a contract with a body corporate to provide analytics services that is authorised by the relevant data sharing agreement, but the approved contract or the applicable data sharing agreement limits what the body corporate may do, if the body corporate acts contrary to this limitation, such actions are not covered by the authorisation extension in subclause 124(3).

688. Subclause 124(5) clarifies that when a designated individual for an entity (such as an employee) or a body corporate acting under an approved contract with an accredited entity is given access

to data, and clause 124 provides that the entity's authorisation to use data extends to the designated individual or body corporate, the provision of the data to the designated individual or body corporate is taken to be a use of the data, rather than the provision of access to (that is, a disclosure of) the data to the designated individual or the body corporate. This is a similar position to what applies under the *Privacy Act* – where an entity makes information available to an employee or a contractor but the information remains in the effective control of the entity, the provision of access to the information is taken to be a use rather than a disclosure.

Clause 125 – Other things an entity may or must do under the data sharing scheme

689. Scheme entities have various powers and obligations under the Scheme. Subclause 125(1) provides that, generally, an entity's powers may be exercised by, and its obligations may be performed by, a designated individual for the entity acting within the actual or apparent scope of their designation. Thus, an employee of a Commonwealth body in a position of Chief Data Officer would be able to act on behalf of the Commonwealth body and bind the Commonwealth body in relation to Scheme matters that would normally fall within the range of duties of a Chief Data Officer. This is so despite any specific limitation on their role imposed by the Commonwealth body, unless such limitation was reasonably apparent to the person with whom the Chief Data Officer was dealing.

690. However, certain actions under the Scheme (such as entering into a data sharing agreement) may only be performed on behalf of a Scheme entity by an authorised officer or an officer authorised under subclauses 137(3) or 137(4). Subclause 125(2) clarifies that subclause 125(1) does not apply in these circumstances. Therefore, where a person is a designated individual for the entity, but not an authorised officer or an officer authorised under subclauses 137(3) or 137(4), that person's actions will not be taken to have been done for the entity, if the thing to be done must be done by an authorised officer or an officer authorised under subclauses 137(3) or 137(4).

691. Subclauses 124(1) and 124(2) set out the circumstances where an authorisation given to a Scheme entity under Chapter 2 covers a designated individual of the entity. Subclause 125(2) clarifies that subclause 125(1) does not apply in relation to authorisations under Chapter 2. Subclause 125(1) is not intended to extend the operation of subclauses 124(1) or 124(2). Therefore, because of the operation of subclause 124(2), the conduct of a designated individual of an entity would not be covered by the entity's authorisation under Chapter 2 if the designated individual's conduct is contrary to conditions of accreditation imposed on or applicable to the entity, or the applicable data sharing agreement.

Clause 125A – Contraventions by entities of civil penalty provisions and other non-criminal breaches of this Act

692. Clause 125A sets out the principles to be applied to determine whether an entity, other than an individual, has contravened a civil penalty provision in the Bill, or has otherwise breached a provision in the Bill. If an accredited entity breaches a provision of the Bill, the accreditation authority for the entity may consider the cancellation of the entity's accreditation (refer clause 81).

693. Paragraph 125A(1)(a) provides that, generally, when determining whether an entity (other than an individual) has contravened a civil penalty provision in the Bill, or has otherwise breached a provision in the Bill, the entity is taken to have engaged in conduct engaged in by a designated individual for the entity (if the conduct is within the actual or apparent scope of the individual's designation, which is determined under clause 123), or by a body corporate that is party to an approved contract (if the conduct is within the actual or apparent scope of the approved contract). The term 'approved contract' is defined in subclause 123(3). The inclusion of

'apparent scope' means that conduct engaged in by a designated individual, or a body corporate that is party to an approved contract, can in some circumstances be attributed to an entity even where the conduct is outside the scope of the designated individual's actual designation or the actual scope of the approved contract.

694. In any circumstance where it is necessary to establish an entity's state of mind to determine whether the entity (other than an individual) has contravened a civil penalty provision in the Bill, or has otherwise breached a provision in the Bill, paragraph 125A(1)(b) provides that it is sufficient to establish the state of mind of a designated individual whose conduct is attributed to an entity under paragraph 125A(1)(a).

695. The term 'government entity' is defined in subclause 125A(4) to mean all Commonwealth bodies (including bodies corporate that are Commonwealth bodies), State bodies and Territory bodies that are not bodies corporate, and the bodies politic that come within the definition of 'Australian entity' (the Commonwealth, a State or a Territory). Subclause 125A(2) provides that, where a government body would otherwise be taken to contravene a civil penalty provision in the Bill because conduct of a designated individual or a body corporate is attributed to the government entity by the operation of subclause 125A(1), the government entity does not contravene the civil penalty provision if it is established that the government entity took reasonable precautions and exercised due diligence to avoid the conduct occurring. The availability of this defence will provide data custodians with confidence to share data under the Scheme rather than using other mechanisms, and will also encourage all Commonwealth bodies, and State bodies and Territory bodies that are not bodies corporate, to seek accreditation under the Scheme. The precautions and due diligence required for subclause 125A(2) to apply could include the provision of appropriate training to designated individuals, ensuring policies are clear and available, ensuring designated individuals are clear about the scope of their duties, including appropriate provisions in contracts, having appropriate internal governance arrangements and fostering a culture of compliance in relation to the Scheme. The government entity bears an evidential burden to establish that subclause 125A(2) applies.

696. Where the conduct of a designated individual is attributed to a government entity by the operation of subclause 125A(1), subclause 125A(3) provides that the designated individual is not personally liable for a contravention of a civil penalty provision in the Bill in relation to that particular conduct. This protection extends to ancillary contraventions of civil penalty provisions arising from the operation of section 92 of the *Regulatory Powers Act*, but subclause 125A(3) does not provide any protection in relation to offences under the Bill. Section 92 of the *Regulatory Powers Act* provides, amongst other matters, that a person must not aid, abet, counsel or procure a contravention of a civil penalty provision and, if they do, they are taken to have contravened the civil penalty provision.

697. Clauses 14 and 14A provide for civil penalties to apply to individuals who engage in conduct, where the conduct is, or is part of:

- providing access to data, purportedly under clause 13, where the provision of access is not authorised by clause 13; or
- collecting or using data, that is output or ADSP-enhanced data, by an entity where the collection or use is not authorised by the Bill.

698. Clause 5 clarifies, for the avoidance of doubt, that the Crown may be made liable to pay a pecuniary penalty for contravening a civil penalty provision in the Bill.

699. Section 97 of the *Regulatory Powers Act* provides that, if an element of a civil penalty provision is done by an employee of a body corporate within the actual or apparent scope of their employment, or by an agent or officer of the body corporate within the actual or apparent

scope of their authority, the element of the civil penalty provision is attributed to the body corporate. Subclause 125A(5) clarifies that, when determining whether a body corporate that is a Commonwealth body has contravened a civil penalty provision in the Bill, subclause 125A(1) applies, rather than section 97 of the *Regulatory Powers Act*. However under subclause 125A(6), to determine whether any other body corporate (including a body corporate that is a State body or a Territory body) has contravened a civil penalty provision in the Bill, section 97 of the *Regulatory Powers Act*, rather than subclause 125A(1), must be applied. Subclause 125A(1) applies to all bodies corporate when determining whether the body corporate has breached a provision of the Bill that is not a civil penalty provision.

Clause 125B – Offences by entities against this Act

700. Clause 125B provides that, generally, when determining whether an entity has committed an offence created by the Bill, the entity is taken to have engaged in any conduct engaged in by a designated individual for the entity (if the conduct is within the actual or apparent scope of the individual's designation, which is determined under clause 123), or by a body corporate that is party to an approved contract (if the conduct is within the actual or apparent scope of the approved contract). The term 'approved contract' is defined in clause 123(3). This means that conduct engaged in by a designated individual or a body corporate that is party to an approved contract can in some circumstances be attributed to an entity even where the conduct is outside the scope of the designated individual's actual designation or the actual scope of the approved contract.

701. Where it is necessary to establish an entity's state of mind to determine whether the entity (other than an individual or a body corporate) has committed an offence established by the Bill, paragraph 125B(b) provides that it is sufficient to establish the state of mind of a designated individual whose conduct is attributed to an entity under paragraph 125B(a).

702. Clause 125B does not have any operation in relation to determining whether a body corporate (including a body corporate that is a Commonwealth body, a State body or a Territory body) has committed an offence. Part 2.5 of the *Criminal Code* sets out the principles of how offences apply to bodies corporate. The Bill does not alter the operation of the Part 2.5 of the *Criminal Code*, as it applies to offences established by the Bill. Clause 5 provides that nothing in the Bill makes the Crown liable to be prosecuted for an offence.

Part 6.4 – Data sharing scheme instruments

703. This part covers the instruments to be made under the Scheme.

704. There are four kinds of legislative instruments under the Scheme. Regulations and Ministerial rules set parameters of the Scheme and establish key criteria and thresholds for engaging with the Scheme. Data codes, which are made by the Commissioner, are primarily intended to clarify how the Scheme operates and how the legislative requirements should be complied with. Guidelines, which are also made by the Commissioner, are primarily intended to cover matters relating to the Commissioner's functions and powers under the Scheme to support best practice and provide guidance about how the Scheme operates. These instruments could also address how using certain technology or methodologies affect Scheme entities' obligations under the Bill. This approach allows the Bill itself to remain technology neutral, while enabling the Scheme to adapt to emerging technologies and future needs over time.

705. Non-legislative instruments in the Scheme include registers made by the Commissioner to support best practice and transparency in the Scheme. The registers are of ADSPs, accredited users and data sharing agreements. Each register has a section that must be publicly accessible and another section that is not publicly accessible. The publicly accessible section of each

register will be available through the Commissioner's website. It is expected that Scheme entities will regularly access the registers when negotiating data sharing agreements and sharing data, but the registers will also make key information available to the general public. The Commissioner has discretion to maintain the registers in any form they consider appropriate, provided that the parts of registers that are required to be publicly accessible may be readily accessed by the public free of charge.

706. Registers are not legislative instruments, however the Minister can make rules prescribing what is to be included in the publicly accessible register.

Clause 126 – Data codes

707. Subclause 126(1) empowers the Commissioner to make, by legislative instrument, codes of practice about the Scheme ('data codes'). It intend that these data codes provide further clarification about the operation of the Scheme and deal with matters the Commissioner considers necessary or convenient to deal with for carrying out or giving effect to the Scheme, similar to the purpose and function of registered privacy codes under the *Privacy Act*. Data codes will allow the Commissioner to respond quickly and effectively to emerging technologies and risks which may impact on the Scheme. Data codes are binding on Scheme entities (refer clause 26). The Commissioner will consult with experts and other bodies on the development of data codes.

708. Subclause 126(2) provides a non-exhaustive list of what data codes may address.

709. Paragraphs 126(2)(a) and 126(2)(b) provide that a data code may set out how Scheme entities are to apply data definitions in clauses 9, 10 and 11A, or comply with requirements for sharing in Chapters 2 and 3 including additional requirements to those imposed in these Chapters. A data code cannot be inconsistent with the Bill and, furthermore, a data code that is inconsistent with the Regulations or rules made under the Bill has no effect to the extent of the inconsistency (refer subclause 126(3)). Use of data codes in this manner will clarify core requirements for sharing, and standardise their application by Scheme entities and enable the Scheme to adapt to future needs over time.

710. Data codes may also deal with the management of complaints, including by imposing additional requirements on their submission and management under paragraphs 126(2)(c) and 126(2)(d). 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 administer the complaints mechanism.

711. Paragraph 126(2)(e) enables data codes to deal with any other matters the Commissioner considers necessary or convenient to deal with for carrying out or giving effect to the Scheme. This clarifies the broad power the Commissioner has to make data codes to ensure consistent application of requirements in the Bill.

712. Subclause 126(2A) requires the Commissioner to make one or more data codes about:

- the data sharing principles described in clause 16,
- the general privacy protections in clause 16A, and
- the purpose-specific privacy protections in clause 16B.

713. Subclause 126(2B) requires that the data code made in relation to clause 16A cover the consent of individuals to share their personal information. Specifically, subclause 16A(1) provides that biometric data may only be shared with the express consent of the individual to whom it applies. It is intended that the data code will detail how data custodians, accredited users and ADSPs should request express consent for the purpose of subclause 16A(1).

714. Subclause 126(2C) provides that the data code made in relation to the purpose-specific privacy protections in clause 16B cover the consent of individuals to share their personal information, the circumstances where it would be unreasonable or impractical to seek the consent of individuals to the sharing of their data, the principles to be applied by data custodians when determining whether it is necessary to share personal information to properly deliver a government service, and the circumstances (or categories of circumstances) where the public interest to be served by a project justifies the sharing of personal information without consent. Clause 16B imposes significant limitations on when personal information may be shared under the Scheme. The limitations imposed by clause 16B vary depending on the data sharing purpose for the project. A note under subclause 16B(4) confirms that it is not unreasonable or impracticable to seek an individual's consent merely because the consent of a very large number of individuals would need to be sought.

715. Any additional requirements imposed by data codes must be consistent with the Bill. Matters set out in data codes apply where they do not contradict, or are not inconsistent with, the requirements of this Bill. Subclause 126(3) clarifies that rules and Regulations prevail over data codes in the event of any inconsistency.

716. Data codes made under this clause are legislative instruments for the purposes of the *Legislation Act*. 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.

Clause 127 – Guidelines

717. Subclause 127(1) provides that the Commissioner may make, by legislative instrument, written guidelines in relation to matters for which the Commissioner had functions under the Bill. While guidelines are not binding on Scheme entities, clause 27 requires these entities to take guidelines into account when engaging in conduct for the purposes of the Bill. There is no obligation on the Commissioner to make guidelines.

718. Subclause 127(2) provides that guidelines may outline principles and processes related to any aspect of the 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 Scheme and data system more broadly, contributing to the Commissioner's functions and the objects of the Bill.

719. 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 Council may also advise the Commissioner on the development of guidelines, particularly those that relate to the Council's functions (refer clause 61).

720. Subclause 127(3) provides that guidelines sit below data codes in the hierarchy of legislative instruments made under the Bill. Thus, guidelines that are inconsistent with the Bill, or with regulations, rules or data codes made under the Bill, are of no effect. However, if a guideline is inconsistent with another type of legislative instrument made under the Bill, the guideline will still operate to the extent that it is not inconsistent with, and can operate concurrently with, the other legislative instrument.

Clause 128 – Register of ADSPs

721. Subclause 128(1) requires the Commissioner to maintain a register of ADSPs that includes a publicly accessible part and a part that is not publicly accessible. The register will support the Commissioner's administration of the accreditation framework (refer Part 5.2), and provide a

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

722. Subclause 128(2) provides that, for each currently accredited ADSP, the following information must be made publicly available on the register of ADSPs: the name and current contact details for the ADSP, the conditions of accreditation applicable to the ADSP (including conditions of accreditation prescribed by rules under clause 77B) and, if the accreditation of the ADSP is currently suspended, that fact and the duration of the suspension.

723. The Minister may make rules that require the Commissioner to include additional details on the publicly accessible part of the register (refer paragraph 128(2)(e)) or require the Commissioner not to include details in the publicly accessible part of the register that would otherwise be required in certain circumstances (refer subclause 128(3)), or require the Commissioner to include additional details on the part of the register that is not publicly accessible (refer paragraph 128(4)(b)). The Commissioner must include on the part of the register that is not publicly accessible any additional details prescribed in the rules or any particular details the rules exclude from the publicly accessible part of the register. If the rules require the Commissioner not to include particular details in the publicly accessible part of the register, these details must be included in the part of the register that is not publicly accessible (refer paragraph 128(4)(a)). Rules made by the Minister for the purpose of clause 128 are legislative instruments that are subject to disallowance.

724. The Commissioner has no discretion about what details are, or are not, on the publicly accessible part of the register, or the part of the register that is not publicly accessible. What details must, or must not, be included on each part of the register is determined by clause 128 and any rules made for the purpose of that clause. Accordingly, action taken by the Commissioner to include particular details on a part of the register, or not to include particular details, is not subject to merits review under clause 118.

725. Subclause 128(6) provides that the register of ADSPs is not a legislative instrument.

Clause 129 – Register of accredited users

726. Subclause 129(1) requires the Commissioner to maintain a public register of accredited users. The register will support the Commissioner's administration of the accreditation framework (refer Part 5.2), and provide a transparency mechanism to report and provide information on accredited users to Scheme entities and the public more broadly.

727. Subclause 129(2) provides that, for each currently accredited user, the following information must be made publicly available on the register of accredited users: the name and current contact details for the user, the conditions of accreditation applicable to the user (including conditions of accreditation prescribed by rules under clause 77B) and, if the accreditation of the user is currently suspended, that fact and the duration of the suspension.

728. The Minister may make rules that require the Commissioner to include additional details on the publicly accessible part of the register (refer paragraph 129(2)(e)), or require the Commissioner not to include details in the publicly accessible part of the register that would otherwise be required in certain circumstances (refer subclause 129(3)), or require the Commissioner to include additional details on the part of the register that is not publicly accessible (refer paragraph 129(4)(b)). If the rules require the Commissioner not to include particular details in the publicly accessible part of the register, these details must be included in the part of the register that is not publicly accessible (refer paragraph 129(4)(a)). Rules made by the Minister for the purpose of clause 129 are legislative instruments that are subject to disallowance.

729. The Commissioner has no discretion about what details are, or are not, on the publicly accessible part of the register, or the part of the register that is not publicly accessible. What details must, or must not, be included on each part of the register is determined by clause 129 and any rules made for the purpose of that clause. Accordingly, action taken by the Commissioner to include particular details on a part of the register, or not to include particular details, is not subject to merits review under clause 118.

730. Subclause 129(6) provides that the register of accredited users is not a legislative instrument.

Clause 130 – Register of data sharing agreements

731. The register of data sharing agreements is a key transparency and accountability mechanism. It provides useful insights on the operation of the Scheme, the data sharing activities of Scheme entities and information necessary for the effective use of redress mechanisms. It is also intended that data custodians have regard to the register of data sharing agreements when considering requests from accredited users, as this may be relevant for the application of the data sharing principles under clause 16 (for example, the types of outputs held by an accredited user may be relevant to how the setting principle is applied to a project).

732. Subclause 130(1) requires the Commissioner to maintain a public register of data sharing agreements.

733. Subclause 130(2) provides that, for each registered data sharing agreement, a number of details about the data sharing agreement and the project covered by the agreement must be made publicly available on the register of data sharing agreements. These matters are set out in paragraphs 130(2)(a) to 130(2)(r).

734. The Minister may make rules that require the Commissioner to include additional details on the publicly accessible part of the register (refer paragraph 130(2)(r)), or require the Commissioner not to include details in the publicly accessible part of the register that would otherwise be required in certain circumstances (refer subclause 130(3)) or require the Commissioner to include additional details on the part of the register that is not public accessible (refer paragraph 130(4)(c)). If the rules require the Commissioner not to include particular details in the publicly accessible part of the register, these details must be included in the part of the register that is not publicly accessible (refer paragraph 130(4)(b)). Rules made by the Minister for the purpose of clause 130 are legislative instruments that are subject to disallowance. The part of the register that is not publicly accessible must include the full text of each registered data sharing agreement, and each variation to such agreement that has been registered (refer paragraph 130(4)(a)).

735. The Commissioner has no discretion about what details are, or are not, on the publicly accessible part of the register, or the part of the register that is not publicly accessible. What details must, or must not, be included on each part of the register is determined by clause 130 and any rules made for the purpose of that clause. Accordingly, action by the Commissioner to include particular details on a part of the register, or not to include particular details, is not subject to merits review under clause 118.

736. Subclause 130(6) provides that the register of accredited users is not a legislative instrument.

Clause 131 – Recognition of external dispute resolution schemes

737. This clause empowers the Commissioner to recognise, by written notice, external dispute resolution schemes for the purposes of resolving complaints received under clause 88. The Commissioner may refer a complaint to external dispute resolution when they are satisfied it would effectively resolve the relevant matter (refer paragraph 92(1)(h)).

738. 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 and can avoid the need for court proceedings. It also reflects precedent from the *Privacy Act* and the *Corporations Act* 2001.

739. Subclause 131(1) allows the Commissioner to recognise an external dispute resolution scheme for an entity or a class of entities, or for a specified purpose.

740. Subclause 131(2) sets out matters the Commissioner must take into account before recognising a dispute resolution scheme. These matters are: accessibility; independence; fairness; accountability; efficiency; effectiveness; and any other matter the Commissioner considers relevant. The list is modelled on matters that must be considered by the Information Commissioner and the Australian Securities and Investments Commission Chair under their respective schemes.

741. Subclause 131(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).

742. Subclause 131(4) provides that the written notice of recognition is not a legislative instrument within the meaning of section 8 of the *Legislation Act*.

Clause 132 - Approved forms

743. The Commissioner may approve a form for use in the Scheme.

744. Approved forms may be used to standardise the content, format, and means of distribution of information to the Commissioner and among Scheme entities. This approach supports consistent practice and streamlining of the administrative and operational systems underpinning the 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.

745. Approved forms may be made to standardise the form of data sharing agreements (refer clause 18), non-personal data breach notifications (refer clause 38), complaints (refer clause 88), and applications for internal merits review (refer clause 119). Rules and data codes may also prescribe where an approved form must or may be used.

746. The expression ‘data sharing scheme’ is defined in clause 9 to mean “this Act and the regulations, rules data codes and guidelines made under it”. Item 3 of Schedule 3 to the *Data Availability and Transparency (Consequential Amendments) Bill 2022* provides that the Scheme is taken to include that Schedule and rules made under it. Thus, clause 132 will empower the Commissioner to approve a form if rules made under Schedule 3 of the *Data Availability and Transparency (Consequential Amendments) Bill 2022* provide for such a form to be an approved form.

Clause 133 – Rules

747. This clause empowers the Minister to make, by legislative instrument, rules for the Scheme. The rules may prescribe matters required or permitted by the Bill, such as matters relating to the accreditation framework (refer Part 5.2) or prescribing additional precluded purposes for sharing (refer clause 15). The Minister may also prescribe other matters necessary or convenient for giving effect to the Scheme, in order to cater for future needs as the Scheme evolves over time. The rules will reflect the scope of the Scheme established by this Bill, and may not contradict or be inconsistent with its clauses.

748. Covering matters in the rules will also allow the Bill to be technology agnostic and give flexibility for the 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 for accreditation (refer clause 86) are particularly important to ensure that the Scheme is appropriately safeguarded against new and emerging risks.

749. To avoid any doubt, subclause 133(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.

750. Subclause 133(3) clarifies that the regulations prevail over rules in the event of any inconsistency.

Clause 134 – Regulations

751. Clause 134 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 Scheme.

752. Primarily, the Regulations will list bodies and legislation that are exempt from the Scheme (refer clause 17). Establishing these matters in the Regulations allows exemptions to be adapted over time, while maintaining Parliamentary oversight. As exemptions set thresholds for access to the Scheme, it is more appropriate to create them through the Bill itself or in the Regulations made by the Governor-General, rather than in subordinate instruments made by the Minister or the Commissioner.

753. Regulations will also be made for the purposes of prescribing transitional matters relating to the sunset of the Scheme under clause 143.

754. Regulations prevail over both the rules and data codes in the event of any inconsistency.

Part 6.5 – Other matters

755. Part 6.5 sets out various administrative and other matters that are necessary to ensure the Scheme operates in an effective and accountable manner. Including, but not limited to, provisions on authorised officers and individuals authorised to do particular things, annual report requirements, fees, periodic reviews of the Act and a sunset provision for the Scheme.

Clause 135 - Disclosure of scheme data in relation to information-gathering powers

756. A Scheme entity may contravene a civil penalty provision or commit an offence under clauses 14 and 14A if they use scheme data in a manner that is not authorised under clauses 13A, 13B or 13C and is not otherwise authorised by the Bill. Clause 9 defines the term ‘use’ to include handle, store and provide access. If a Scheme entity provides another entity with scheme data and the provision of that access is not authorised by Chapter 2 or another provision of the Bill, the Scheme entity providing the access may contravene a civil penalty provision or commit an offence under clauses 14 and 14A, even if access was provided in response to a request, requirement or notice made or issued under other Commonwealth legislation.

757. Clause 135 authorises Scheme entities to provide access to scheme data to the Auditor-General, the Commonwealth Ombudsman, the Information Commissioner, a Commonwealth, State or Territory court or tribunal or a Commonwealth Royal Commission in certain circumstances. Where a Scheme entity provides access to scheme data to a statutory officeholder (or their delegate), a court, a tribunal or a Royal Commission in accordance with clause 135, the Scheme entity will not contravene a civil penalty provision or commit an offence under clauses 14 and 14A solely because the provision of access to the scheme data.

758. Scheme data may be subject to secrecy or confidentiality provisions in other legislation. Where clauses 13, 13A, 13B or 13C authorises the sharing, collection or use of data, clause 23 provides that the authorisation has effect despite anything in another law of the Commonwealth, or a law of a State or Territory. However, clause 23 has no operation in relation to the authorisation provided by clause 135. Therefore, a Scheme entity that proposes to provide scheme data to a statutory officeholder, a court, a tribunal or a Royal Commission as authorised by clause 135 must consider whether applicable secrecy or confidentiality provisions in other legislation permit the disclosure, or whether the power requiring the disclosure of the scheme data authorises the disclosure despite applicable secrecy or confidentiality provisions.

Clause 135A – Data held by National Archives of Australia

759. The data custodians of public sector data will transfer the care of some of that data to the National Archives of Australia (the **Archives**) prior to the commencement of the open access period for that data, as defined by the *Archives Act*. Where such transfer occurs, subclauses 135A(1) and 135A(2) clarify that the Archives is not the data custodian of the transferred data for the purpose of the Scheme. The data custodian that transferred the data to Archives remains the data custodian for the purpose of the Scheme. If such a data custodian receives a request to share the data from an accredited user under clause 25, the data custodian will have an obligation to consider the request under that section. If necessary, the data custodian will be able to obtain the data from the Archives in order to share the data under the Scheme.

760. Subclause 135A(3) provides that the authorisations in Chapter 2 generally do not apply to any public sector data that is in the open access period for that data, as defined by the *Archives Act*. Access to data in the open access period must be sought under the *Archives Act*, rather than under the Scheme. However, where a data sharing agreement in relation to particular public sector data has been registered by the Commissioner before the open access period for that data, subclause 135A(3) provides that the sharing, collection and use of data as authorised under Part 2 as part of the project covered by the agreement, may occur after the commencement of the open access period for the data. This is the case even if the data sharing agreement is varied after the commencement of the open access period.

Clause 136 - Geographical jurisdiction of civil penalty provisions and offences

761. Clause 136 limits the geographical jurisdiction of civil penalty provisions and offences in the Bill to circumstances where there is some specified connection with Australia.

762. Subclause 136(1) specifies four types of conduct that could constitute an alleged contravention or offence under this Bill. For example, the conduct, or the result of the conduct, occurs wholly or partly in Australia, or on board an Australian aircraft or Australian ship (paragraph 136(1)(a)). Paragraphs 136(1)(a) to 136(1)(d) 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.

763. Subclause 136(2) provides a defence for a primary contravention or primary offence, and sets out four circumstances where a person does not contravene a civil penalty provision or commit an offence under this Bill, despite subclause 136(1). For example, if the conduct constituting the alleged contravention or offence occurs wholly in a foreign country, but not on board an Australian aircraft or Australian ship (refer paragraph 126(2)(b)).

764. Subclause 136(3) provides a defence for an ancillary contravention or ancillary offence, and sets out five circumstances where a person does not contravene a civil penalty provision or

commit an offence under this Bill, despite subclause 136(1). For example, if the person is not an Australian entity, an Australian citizen or a permanent resident of Australia.

765. Under subclause 136(4), a person (a defendant) who is alleged to have contravened a civil penalty provision of the Bill bears an evidential burden (within the meaning of the *Criminal Code*) if they wish to rely on subclauses 136(2) or 136(3).

766. Subclause 136(6) notes 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*.

767. Subclauses 136(7) and 136(8) clarify concepts necessary to establish extraterritorial operation of the Bill. Subclause 136(7) explains that a 'result of conduct' refers to an element of the contravention or offence at issue. Subclause 136(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.

768. Subclause 139(9) provides a definition of the word 'point' as that term is used in this clause.

Clause 137 – Authorised officers and individuals authorised to do particular things

769. Various important actions that may be taken by entities under the Bill must be taken on behalf of the entity by an authorised officer of the entity or, in some cases, by another person appointed under clause 137. For example, clause 76 provides that an application for accreditation must be made by an authorised officer on behalf of the entity.

770. Subclause 137(1) (including the table that forms part of that subclause) provides that the head of each type of Scheme entity (for example, the Secretary of an Australian Government department) is an authorised officer of that entity by force of the clause. Subclause 137(2) provides that the head of the entity may, by written instrument, appoint an individual falling within the description in the "Individuals" column of the applicable item row of the table to be an 'authorised officer' for the Scheme entity. In the case of Scheme entities that are Australian Government departments, or Executive Agencies or Statutory Agencies (within the meaning of the *Public Service Act 1999*), only SES employees or acting SES employees in the entity may be appointed as authorised officers of the Scheme entity. Where the head of an entity has appointed an individual as an authorised officer, section 33(3) of the *Acts Interpretation Act* provides the entity head with the power to revoke or amend the appointment. An instrument may identify a class of individuals that are appointed as authorised officers, including the class of individuals holding or acting in particular offices from time to time.

771. It is not possible for an individual to be appointed as an authorised officer of an entity for some purposes but not others. For example, the Secretary of an Australian Government department may not appoint an SES employee as an authorised officer of the Scheme entity for the purpose of lodging an application for accreditation as a user, but not for other purposes. A person who is appointed as an authorised officer of an entity may not delegate any part of this role to another individual, or authorise another individual to perform the role on their behalf. Only individuals may be appointed as authorised officers.

772. Subclause 137(3) enables the head of a Scheme entity to appoint an individual by written instrument to enter into variations of data sharing agreements on behalf of the entity. Individuals appointed under subclause 137(3) are not 'authorised officers'. In the case of Scheme entities that are Australian Government departments, or Executive Agencies or Statutory Agencies (within the meaning of the Public Service Act 1999), only SES employees

or acting SES employees in the entity may be appointed under subclause 137(3). Where the head of an entity has appointed an individual under subclause 137(3), section 33(3) of the *Acts Interpretation Act* provides the entity head with the power to revoke or amend the appointment. An instrument may identify a class of individuals that are appointed under subclause 137(3), including the class of individuals holding or acting in particular offices from time to time. An instrument appointing an individual under subclause 137(3) must be a general appointment and may not provide that the individual is only authorised to enter into a particular variation of a data sharing agreement, or variations of agreements that have particular characteristics (for example, a variation that does not provide any additional data to be shared with the accredited user under clause 13).

773. The Agency Heads of Scheme entities that are Australian Government departments, or Executive Agencies or Statutory Agencies (within the meaning of the *Public Service Act* 1999), may appoint an individual in their agency or in another APS agency under subclause 137(4). Such individuals must be SES employees or acting SES employees. Individuals appointed under subclause 137(4) may enter into data sharing agreements and variations of such agreements, and make decisions under subclause 16D(4) (and the associated records of decisions) that the risk that a particular proposed data integration could cause substantial harm is low. For example, if the Secretary of Australian Government department A appoints an SES employee in Australian Government department B under subclause 137(4), by virtue of the appointment, the SES employee may enter into a data sharing agreement with an accredited user on behalf of department A, as the data custodian of the public sector data to be shared.

774. Where the head of a Scheme entity has appointed an individual under subclause 137(4), subsection 33(3) of the *Acts Interpretation Act* provides the entity head with the power to revoke or amend the appointment. An instrument may identify a class of individuals that are appointed under subclause 137(4), including the class of individuals holding or acting in particular offices from time to time. An instrument appointing an individual under subclause 137(4) must be a general appointment and may not provide that the individual is only authorised to enter into a particular type of data sharing agreement, or variations of agreements that have particular characteristics, or only make particular data integration decisions.

Clause 137A – Delegation by Minister

775. Clause 137A allows the Minister to delegate, in writing, to the Commissioner any or all of the Minister's powers in relation to the accreditation framework in Part 5.2. The Minister is the 'accreditation authority' for the Commonwealth, a State, a Territory, a Commonwealth body, a State body or a Territory body applying for accreditation as, or accredited as, a user (refer clause 9). The Minister therefore makes decisions about: the accreditation of these entities as users; the imposition, variation or removal of conditions of accreditation (as users); and, if necessary, the suspension or cancellation of the accreditation of these bodies as users. The Minister may only delegate their powers under Part 5.2 to the Commissioner, and the Commissioner may not sub-delegate such powers.

776. Subclause 137A(2) provides that, when exercising delegated power, the Commissioner must comply with any written directions given to the Commissioner by the Minister.

777. The Minister's power of delegation only relates to the Minister's power to make administrative decisions under Part 5.2. The Minister may make rules under clause 133 relating to accreditation matters (for example, prescribing conditions of accreditation for the purposes of clause 77B) but the Minister may not delegate the power to make rules.

778. Sections 34AA, 34AB and 34A of the *Acts Interpretation Act* apply to the Minister's power of delegation in clause 137A.

Clause 138 – Annual report

779. This clause sets out matters for the Commissioner's annual report. The report is a key accountability and transparency mechanism for the Scheme, and the Commissioner as its regulator.

780. Subclause 138(1) requires the Commissioner to prepare and give the Minister, for presentation to Parliament, an annual report on the operation of the Scheme each financial year, in accordance with the standard timing set in subclause 138(4). These requirements mirror those applicable to 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 Scheme.

781. Subclause 138(2) sets out key information that the annual report must include about the operation of the Scheme, the Commissioner, and the Council's activities. Such information include 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 agreeing to or refusing data sharing requests will be particularly important as an indicator of whether the 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.

782. The report must include details of the number of requests received by data custodians during the relevant financial year from accredited users. While any entity (including entities that are not accredited as users) may request a data custodian to share data, data custodians only have obligations under clause 25 to consider requests made by, and to provide reasons for a refusal to, accredited users. It is appropriate that the Commissioner's reporting under clause 138 aligns with the obligations of data custodians under clause 25.

783. Data custodians have no obligation under the Scheme to share data but, where an accredited user makes a written request to a data custodian to share data, clause 25 requires the data custodian to consider the request within a reasonable period and, if the request is refused, to provide the accredited user with written reasons within 28 days of the date of the refusal decision. Subparagraph 138(2)(d)(ia) will provide a measure of public accountability if data custodians fail to comply with the time limits imposed by clause 25.

784. Paragraph 138(2)(d) ensures that the annual report includes details of the number of complaints received by the Commissioner during the financial year (both scheme complaints received under Division 1 of Part 5.3 and general complaints received under Division 2 of Part 5.3) and complaints received directly by data custodians relating to the Scheme generally, or in relation to data custodians' conduct under the Scheme. The number of complaints in a financial year, and trends in the numbers of complaints over time, will provide the Minister, the Parliament and the public with additional information in relation to the operation of the Scheme.

785. Other relevant information on the operation or implementation of the Scheme that the Commissioner considers appropriate, may be included in the report under subclause 138(3).

786. The Commissioner may require Scheme entities to give information and assistance for the preparation of the annual report (refer clause 34).

Clause 139 – Charging of fees by Commissioner

787. The Commissioner may charge fees to recover costs of providing services related to their functions or powers that are not covered by appropriations funding. The Commissioner may also charge a fee covering initial accreditation decisions made by the Minister (or by the

Commissioner as the Minister's delegate) and for the internal review of such decisions. This is because the Minister is the accreditation authority for user accreditation of Scheme entities other than Australian universities. Subclause 139(1) provides that Ministerial rules may prescribe such fees.

788. Fees may be charged where the services are provided on behalf of the Commissioner by another person. 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 to support the Commissioner's decision-making under clause 74.

789. Subclause 139(3) provides that fees are payable to the Commonwealth, through the Consolidated Revenue Fund. Under subclause 139(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*.

790. Subclause 139(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 payed. The Minister may provide for the extension of time for providing services in the rules.

791. Charging of fees by the Commissioner is established in the rules to enable appropriate and flexible adjustments of fees and related processes over time, whilst maintaining Parliamentary oversight.

792. To avoid doubt, fees prescribed by rules may not impose a tax (refer clause 133). 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 140 – Charging of fees by data scheme entities

793. Subclause 140(1) authorises a data custodian to charge fees to an accredited entity to cover the costs of services it performs to deal with the request to share the data with the accredited entity. This allows the data custodian to recover costs of processing the request, and for other services such as preparing the data in order to share.

794. A data custodian may charge a fee to an accredited entity in relation to services performed on behalf of the data custodian by another entity. For example, in response to a request to share data under the Scheme made by an accredited user, the data custodian may decide to share de-identified data with the accredited user. If the data custodian engages an ADSP to perform the de-identification data service in relation to the data to be shared with the accredited user, the cost of the ADSP performing the service may be taken into account if the data custodian charges a fee to the accredited user.

795. Under subclause 140(2), a data custodian must charge fees in accordance with applicable policies of the Australian Government, to ensure a consistent approach. For instance, non-corporate bodies would have regard to guidelines issued by the Australian Government Department of Finance under section 21 of the *PGPA Act*.

796. Nothing in this clause prevents an accredited entity charging fees for services it performs in relation to the Scheme, as clarified by subclause 140(3). This means that an ADSP or accredited user may charge fees for services such as data integration or analysis, regardless of any fees that they may have to pay to a data custodian for access to public sector data.

Clause 141 – Commonwealth not liable to pay a fee

797. 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 Chapter 2 which ensures that all Scheme entities are held to account for their actions within the Scheme. Subclauses 141(2) and 141(3) enable the Finance Minister to give such written directions to give effect to this policy.

798. In practice, this means that the Commissioner may charge other Commonwealth entities for services under clause 139, and that Commonwealth entities are notionally liable for civil penalties.

799. Subclause 141(4) defines 'Commonwealth' for the purposes of the clause.

Clause 142 – Periodic reviews of operation of Act

800. This clause ensures the operation of the Bill is periodically reviewed.

801. Subclause 141(1) provides that the Minister must cause periodic reviews to be undertaken.

802. Subclause 142(2) provides for two reviews on the operation of the Bill to be undertaken, prior to the operation of the sunset provision in clause 143.

803. Subclause 142(2) provides for an independent review three years after the Scheme's commencement, in addition to a review three months after the commencement of any amendments to the *Privacy Act* resulting from the review of that legislation, discussed below, which would have a material impact upon the Scheme. The review must be completed within 12 months, or a longer period agreed by the Minister.

804. The three year review is intended to allow an independent assessment of the operation of the Scheme. If the review were conducted earlier, the Scheme would not be sufficiently mature to properly assess its effectiveness, and whether the Scheme should continue, continue with amendments, or be allowed to cease to have effect under the sunset clause. The timing should allow the review and consideration of any response to be completed in sufficient time to provide valuable input towards informing Parliament whether to extend the Scheme or to allow the sunset provision under clause 143 to take effect.

805. On 12 December 2019, the Attorney-General announced that the Australian Government would conduct a review of the *Privacy Act* to ensure privacy settings empower consumers, protect their data and best serve the Australian economy. The review was announced as part of the government's response to the Australian Competition and Consumer Commission's *Digital Platforms Inquiry*.

806. The Bill is intended to work with, rather than override, the *Privacy Act* and several key terms in the Bill, such as 'personal information', take their meaning from the *Privacy Act*.

807. If the *Privacy Act* is amended in response to the review mentioned above, it is possible that consequential amendments to the Bill may be required. Thus, paragraph 142(2)(b) provides that the Minister must commission a review of the Bill if amendments to the *Privacy Act* made in response to the review initiated by the Attorney-General would, in the Minister's opinion, have a material impact on the Scheme.

808. Subclause 142(3) provides that if subclause 142(2) would require overlapping reviews of the Bill, the reviews may be combined. The combined review must be completed within 12 months of the day the latest of the reviews was required to commence. The Minister may agree a longer period in which the review must be completed.

809. 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.

810. Reviews will help ensure the Scheme operates as intended, and provide an opportunity to consider expansion or refinements. The Scheme could, for instance, be expanded in the future to enable greater State and Territory participation. Reviews also provide a key accountability and Parliamentary oversight mechanism, to ensure the Scheme is operating in-line with public expectations.

Clause 143 – Sunset of the data sharing scheme

811. Clause 143 provides for the Bill to cease having effect. The Bill sunsets and ceases to have effect at the end of the day that is the fifth anniversary of the day the Scheme commences. This provides another accountability mechanism to ensure the operation of the Scheme is considered by Parliament following the review undertaken under subclause 142(2).

812. Subclause 143(2) allows Regulations to be made for the purposes of prescribing transitional matters in relation to this sunset clause. The Regulations for these purposes may be made during the period commencing 12 months before the sunset date, which is at the fourth anniversary of the Scheme's commencement, and ending immediately before a year from the sunset day. The one year period leading to the sunset day allows the Commissioner to commence activities transitioning out of the Scheme ahead of the sunset.

813. Subclauses 143(4) to 143(7) provide details on the matters that the Regulations may prescribe to deal with transitional matters arising from this sunset clause. The Regulations may:

- provide for savings or application provisions so that certain provisions continue to apply, including in a modified way, such as the existence of the Commissioner as a statutory office holder;
- empower the Commissioner to direct a Scheme entity to take or not take certain actions to ensure the scheme data is appropriately dealt with when the Scheme ends; or
- create offences or civil penalties for failure to comply with directions made for the purposes of this sunset clause, as well as penalties for both individuals and entities for contravening the Regulations or offences against the Regulations.

814. Subclauses 143(4) to 143(7) will not allow modifications to provisions of the Bill. They will only allow modification of application of those provisions, to ensure that the Scheme applies appropriately after sunset.

815. Subclause 143(7) permits the Regulations made under this clause to prescribe penalties, as it would be inappropriate to create an offence or civil penalty in the Bill regarding transitional matters, as Parliament may, instead of choosing to let the Scheme sunset, amend clause 143 in some way, thereby bypassing the need for sunset Regulations and offences or civil penalties under Regulations. Further, it is not possible to anticipate all transitional matters that may arise that may require civil penalty provisions or offences.

816. A legislative safeguard is in place for the Regulations. An automatic repeal which has the effect that the longest period of time such Regulations may stay in force is one year from the sunset day (see subclause 143(9)). Further, Parliamentary oversight will occur of such Regulations as they are still required to be tabled in Parliament in accordance with the *Legislation Act*, and subject to disallowance under that Act.

817. Subclause 143(8) clarifies that these Regulations must not have the effect of allowing data to be shared under clause 13 after the sunset day. This means that the Regulations could not allow

data custodians to be able to continue providing access to data under the Scheme following the sunset day. This ensures that the Regulations do not have the effect of overriding the operation of the sunset clause when prescribing transitional matters.

818. Subclause 143(9) provides a self-repealing provision for Regulations made for the purposes of this sunset clause, which provides that they are repealed one year from the sunset day, consistent with the timeframe provided under subclause 143(2).

Statement of Compatibility with Human Rights

Prepared in accordance with Part 3 of the Human Rights (Parliamentary Scrutiny) Act 2011

1. This Bill is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*.

Overview

2. The *Data Availability and Transparency Bill 2022* (the **Bill**) establishes a new scheme for sharing Australian Government data (the **Scheme**).

3. The Bill authorises Commonwealth bodies to share (provide controlled access to) public sector data with accredited users for specific purposes in the public interest, with safeguards to mitigate risk, including in relation to privacy.

4. The Bill establishes the National Data Commissioner (the **Commissioner**) to regulate the Scheme and educate data custodians on best practice data sharing.

5. A person may commit an offence, or contravene a civil penalty provision, if they fail to comply with certain obligations under the Scheme, consistent with the objectives of enhancing integrity and enforcing security and privacy safeguards in the Scheme.

6. The Scheme will promote better availability and use of Australian Government data, empower the Australian Government to deliver better services, policies and programs, and support research and development.

Human Rights Implications

7. This Bill engages the following rights:

- right to protection from arbitrary or unlawful interference with privacy;
- right to freedom of expression, including to seek, receive and impart information; and
- right to a fair trial and fair hearing.

Protection from arbitrary or unlawful interference with privacy

8. The right to protection from arbitrary or unlawful interference with privacy is recognised in Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR). The Bill engages with this right by authorising government entities, and universities, to share, collect and use Australian Government data, which may contain personal information.

9. This right can be permissibly limited in order to achieve a legitimate objective, where the interference to privacy is for a reason consistent with the ICCPR, proportionate to the ends sought, and necessary in the circumstances of any given case.[1].

10. The Bill includes safeguards to minimise interference with the right to privacy, and to ensure any remaining impact is reasonable, necessary and proportionate to its objectives.

11. Measures which engage and support the right to privacy include:

- a starting position that data shared under the Scheme must not include personal information unless an exception applies;

- data sharing only being authorised for defined purposes (see below) that serve the public interest, in accordance with the data sharing principles, and consistent with terms and conditions set out within a data sharing agreement;

- transparency mechanisms, such as registers of data sharing agreements and accredited entities, and annual reporting, which provide a public record of who is handling scheme data including personal information under the Scheme, and for what purposes;

- requiring all entities participating in the Scheme to be accredited to participate in the Scheme before any data sharing occurs, to assess whether they are capable of handling public sector data in a way that minimises risk of unauthorised access or use;

- data minimisation requirements, that is, personal information can only be shared where necessary. If shared, data custodians must take into account the data sharing principles and private coverage conditions;

- restricting the sharing of biometric data by requiring the express consent of the individual;

- requiring all sharing of personal information, if necessary, under the Scheme be subject to the *Privacy Act*, a state or territory equivalent, or an equivalent requirement that the data sharing agreement must include terms that the entities must not do an act or engage in a practice that would breach the Australian Privacy Principles and for parties to agree to be subject to the jurisdiction of the Australian Information Commissioner (the Information Commissioner);

- requiring data sharing agreements to prohibit the re-identification of de-identified data;

- requiring entities to comply with data codes that will set out requirements for how consent is to be collected from individuals, and how principles are to be applied in determining whether it is necessary, or in the public interest, to share personal information in certain circumstances;

- precluding certain entities from participating in the Scheme, including intelligence agencies and integrity agencies with a role of oversight for the Scheme. Highly sensitive data, including intelligence data and certain health data, is similarly precluded from the Scheme.

[1] Office of the United Nations High Commissioner for Human Rights, *Toonen v* Australia, Communication No. 488/1992, UN Doc CCPR/C/50/D/488/1992 (10 April 1992, adopted 31 March 1994) para 8.3 https://juris.ohchr.org/Search/Details/702

Foreign entities, and private sector entities, are also precluded from participating in the Scheme;

- prohibiting the storage or access of data containing personal information outside of Australia;

- excluding data sharing that is inconsistent with the obligations of Australia under international law, including obligations under any international agreement binding on Australia or that would be inconsistent with Australia's obligations under international law or agreements;

- requirements in Part 3.3 for mitigation and notification of any data breaches, which align with thresholds and provisions in the *Privacy Act*;

- civil and criminal sanctions applying for unauthorised sharing, collection or use of data, and other conduct that does not comply with the Bill; and

- authorising the Information Commissioner to provide details of a privacy complaint related to the Scheme, to the Commissioner. This allows the Information Commissioner to continue to handle the complaint, whilst enabling the Commissioner to be aware of matters related to the Scheme. The Bill, as amended, imposes a new civil penalty for a serious contravention of the Bill. A serious contravention, among other things, could include non-compliance with obligations relating to the sharing of data containing personal information (such as a failure to obtain consent to share biometric data). This is intended as a deterrence against serious misconduct under the Scheme and an enforcement option allowing the Commissioner to apply for higher penalty with the court.

12. Further privacy protections apply depending on the purpose of data sharing under the Scheme (purpose-specific privacy protections, clause 16B). The Scheme establishes three data sharing purposes – delivery of government services, informing government policy programs, and research or development.

- If the sharing is for the purpose of delivering government services, the data must not include personal information about an individual, unless the government service (other than services relating to a payment, entitlement or benefit) is being delivered to the individual, or the individual consents to the sharing of their personal information, or the sharing would be a disclosure authorised under Part VIA of the *Privacy Act* (dealing with personal information in emergencies and disasters). The government service being delivered must be identified in the relevant data sharing agreement and only the minimum amount of personal information necessary to properly deliver the service can be shared.

- If the sharing is for the purpose of informing government policy and programs, or research and development, personal information must not be shared unless either: the individual consents to the sharing of their personal information and only the minimum amount of personal information necessary for the project to proceed is shared; or, the project cannot proceed without the personal information, that the public interest in the project justifies the sharing of personal information without consent, only the minimum personal information necessary for the project to proceed is shared, and at least one permitted circumstance for the data sharing project exists.

- The permitted circumstances for research and development include where it is unreasonable or impracticable to seek the individual's consent, whether the data to be collected and used is in the course of medical research and is in accordance with the guidelines under

subsection 95(1) of the *Privacy Act*, the sharing is to allow an accredited data services provider to create data that does not include any personal information, or where access to the data is controlled by an accredited data services provider.

- The permitted circumstances for informing government policy and programs are the same as for research and development, but also include where the user receiving the data is a Commonwealth body and the agreed output of the project only includes de-identified information, and where sharing would be a disclosure authorised under Part VIA of the *Privacy Act* (dealing with personal information in emergencies and disasters).

13. Development of these safeguards involved consultation with privacy experts and undertaking three independent Privacy Impact Assessments to identify and address privacy impacts. To the extent that personal information is involved in the Scheme, the privacy protections (and limited diminutions) are consistent with those in the *Privacy Act*.

Freedom to seek, receive, and impart information

14. Article 19 of the ICCPR establishes the right to freedom of expression, including freedom to seek, receive and impart information and ideas. The exercise of this right may be subject to restrictions only if provided by law and where it is necessary for the protection of national security, or to respect the rights of others. Facilitating access to data is consistent with the freedom to seek and impart information.

15. The Bill engages and supports this right by establishing a framework for accredited entities to seek, receive, and impart information (in the form of data). The Scheme does this by establishing clear authorisations for when it is lawful to share, collect and use Australian government data, and by establishing operational frameworks and tools such as standardised data sharing agreements that support access to such data.

16. Through these standardised data sharing agreements, it is clear how information (that is, data) can be lawfully sought, received and handled under the Scheme. The Scheme limits the circumstances in which data can be shared, and this is necessary to ensure Australian Government data is handled in accordance with other laws (for example, secrecy provisions in program legislation). The Commissioner is also required to make a data code on the data sharing principles and consent. These requirements support the Scheme to establish clear requirements for the sharing of data. The Commissioner will also have an education and support function, which will in turn support safe data sharing practices under the Scheme.

17. The Bill also upholds the right to impart information by requiring certain information contained in a data sharing agreement be made publicly available on a register of data sharing agreements. The information that must be published on the register includes descriptions of the project, data sharing purpose and the data to be shared. With this information, the public will have visibility of what data is being shared and how the sharing is done and for what purpose, supporting transparent and accountable management of the Scheme.

18. The Scheme also supports this right by precluding foreign entities from the Scheme. An accreditation authority (the Minister or the Commissioner) has discretion to refuse accreditation or impose conditions of accreditation where appropriate for reasons of security. This mechanism supports the protection of national security and makes clear the Scheme is intended to operate for the benefit of the Australian public.

19. Clauses 20C and 20E also supports this right by facilitating open release of outputs created under the Scheme, where release is consistent with a data sharing agreement and relevant Australian laws such, as the *Privacy Act*.

20. Building on this, an accredited user does not contravene the Bill if it grants access under the *FOI Act* to output of a project or ADSP-enhanced data, where the output or data has exited the Scheme. This is facilitated by the operation of clause 20E, which provides a mechanism for output of a project or ADSP-enhanced data to exit the Scheme. Where output or ADSP-enhanced data has exited the Scheme and is held by a Commonwealth body subject to the *FOI Act*, this has the effect of increasing the volume of records held by the Commonwealth body that are subject to the *FOI Act*. That is, those records are able to be requested under the *FOI Act*.

21. The Bill and the *Data Availability and Transparency (Consequential Amendments) Bill 2022* operate to protect and regulate Australian Government data that is shared within the Scheme. This setting aligns with the rigorous safeguards in place to regulate the Scheme and ensure shared data is protected within the Scheme. Accordingly, data shared by data custodians within the Scheme, output and ADSP-enhanced data are exempt from the *FOI Act*. While the Bill does not provide for FOI access to copies of data shared by data custodians for the purposes of the Scheme, this approach is reasonable as the Scheme rigorously limits how shared data is handled and original copies of the data held by data custodians outside the Scheme would continue to be available through the usual FOI processes.

22. Consistent with Article 19(3) of the ICCPR, the Bill imposes some limitations on the right to seek, receive, and impart information which are necessary to protect national security and to respect others' rights.

23. The accreditation framework supports this right by providing for the authorisation to share data with accredited entities, rather than the public at large. This ensures government data is only shared with entities who are capable of handling data safely and securely. The accreditation process may involve the assessment of an applicant by security agencies, and conditions of accreditation that affect how an entity participates in this Scheme may be placed and adjusted by the Minister or Commissioner to manage systemic or entity-specific risks.

24. To the extent that the Bill precludes access to data for certain purposes, the Bill seeks to uphold existing rights and privileges over public sector data in alignment with other human rights where the sharing that would contravene such interests. These exclusions are necessary to ensure that the sharing of highly sensitive data, or involving law enforcement or national security purposes and entities, continues to be handled under dedicated frameworks. Likewise, the Bill provides a preferred pathway for sharing and does not compel data custodians to share public sector data, ensuring there is no compulsion to share where risks cannot be adequately managed.

25. The Bill preserves existing legal avenues for the sharing and use of government data, so channels for data access within those dedicated frameworks and corresponding protections are not affected by this Scheme.

26. The restrictions on the scope of the Scheme align with Article 19(3), which allows limitations on the transmission of information to the extent necessary to protect national security or to respect others' rights.

Right to a fair trial and fair hearing

27. Articles 14 and 15 of the ICCPR establish rights to due judicial process and procedural fairness. These rights apply to both criminal and civil proceedings, and in cases before both courts and tribunals.

28. The Bill engages these rights as it contains a range of penalties for non-compliance, including civil and criminal penalties, and injunctions, imposed by a court, whilst upholding procedural fairness requirements.

Civil penalties and criminal offences

29. The Bill creates new civil penalties for conduct that is inconsistent with its requirements. Taking a proportionate approach to enforcement, the Bill distinguishes civil from criminal penalties. As the term 'criminal' has a specific meaning in international human rights law, civil penalty provisions in domestic law may engage criminal process rights under Articles 14 and 15 of the ICCPR. However, the Bill's civil penalty provisions should not be considered 'criminal' for the purposes of international human rights law, as failure to pay a civil penalty will not result in a prison sentence.

30. The Bill also provides that a serious contravention of certain civil penalty provisions can attract a higher civil penalty. A court may decide that the higher penalty is appropriate considering the sensitive data involved in the contravention, the consequences of the contravention, and the degree of care exercised by the entity involved in the contravention.

31. The Bill creates new criminal offences to capture instances of unauthorised sharing, collection and use of data not covered by other laws. The availability of criminal penalties in this context is appropriate as these criminal offences directly undermine the Scheme's protections and safeguards. The criminal offences are modelled on the standard for all Australian criminal laws, including default fault elements from the *Criminal Code Act 1995* and maximum penalties available under laws such as the *Privacy Act*.

32. When data is shared, collected or used in an unauthorised manner, the Bill does not override secrecy and non-disclosure provisions in other laws, so sanctions under other laws may alternatively apply.

33. Consistent with Article 14(1), an independent, impartial court will preside over all civil and criminal proceedings brought under the Bill or another Australian law. Such proceedings will be subject to established Australian court processes and procedures that protect the right to a fair trial, including requirements relating to procedural fairness, evidence and sentencing.

34. The right to be considered equal before a court or tribunal is also upheld, as all parties to proceedings under the Bill (or another law) will be given reasonable opportunity to present their case in conditions that do not disadvantage them as against other parties.

Presumption of innocence: legal burden

35. The Bill engages the right to the presumption of innocence in Article 14(2) of the ICCPR by placing a legal burden on an entity. To the extent this might be considered to limit the presumption of innocence, the limitation is reasonable in all circumstances.

36. The Bill sets out when an individual's conduct will be attributed to the Commonwealth, State or Territory body that employs or engages them, and when the individual will be personally liable for their conduct. The Bill interacts with the right to the presumption of innocence, as it requires the entity, to prove whether the government body took reasonable precautions and exercised due diligence to avoid the individual's conduct which contravened the Bill.

37. This legal burden is justifiable as the evidence required to prove reasonable precautions and due diligence would be within the entity's knowledge and means to provide. Consistent with the *Criminal Code*, an entity need only defend this burden on the balance of probabilities, a lower standard of proof than beyond reasonable doubt.

38. The right to presumption of innocence is not otherwise impacted, and would apply in criminal proceedings brought under this Bill or rebound legislation.

Administrative measures and review of decisions

39. The Bill engages the right to a fair and public hearing through the powers of the Commissioner, to investigate breaches, and to issue infringement notices, seek injunctions, and enter into enforceable undertakings where it is determined an entity has not complied with the Bill. These are administrative penalties, distinct from those imposed by a court. However, consistent with Article 14(1) and the doctrine of separation of powers in Australia, a court will be responsible for their enforcement.

40. A Commonwealth body is not excused from complying with a notice to produce documents or information to the Commissioner for their regulatory functions, on the grounds of legal professional privilege. This interacts with the right to a fair trial as it negates legal professional privilege, however the privilege is not wholly negated as a broad use immunity is provided that prevents the information being used as evidence against any persons in civil or criminal proceedings. To the extent this provision may limit the right to a fair trial or hearing, it is reasonable and proportionate to the objectives of this legislation in establishing an effective regulator that can investigate and address compliance with the Bill.

41. The Bill upholds fair hearing rights by providing court and tribunal oversight of administrative decisions. For example, pathways for judicial review will continue to be available to ensure decisions by the Commissioner and the Minister as an accreditation authority are lawful.

42. The Commissioner's decisions will also be subject to internal merits review and/or review by the Administrative Appeals Tribunal, with favourable decisions not subject to merits review. Consistent with the *Guide to Framing Commonwealth Offences*, there are also limited, reasonable exceptions for certain potentially adverse decisions involving national security or which are not appropriate for merits review. In particular, decisions made by the Commissioner that are classed as 'urgent' directions are not reviewable decisions, as directions made in these circumstances are the result of a high risk or emergency situation which requires immediate actions to address.

43. The unavailability of merits review in these limited circumstances serves the public interest by enabling the Commissioner to take necessary actions without delay to ensure the security and privacy of the individuals and entities involved in the Scheme. This aligns with the protection from unlawful interference with privacy in Article 17 of the ICCPR.

44. Avenues for individuals or other entities to seek redress, such as complaints and administrative review of government decisions, are also available under other frameworks. The Scheme does not prevent individuals and entities from accessing the right to a fair trial and hearing for matters

that fall within another government body's portfolio responsibility. The Scheme promotes the access to administrative measures and remedies under other frameworks by enabling the Commissioner to transfer matters to a more appropriate authority so that the aggrieved person can access redress measures and procedural fairness under the appropriate frameworks. For instance, a person may complain to the Information Commissioner about mishandling of personal information under the Scheme. As a result, the Bill upholds, and does not unreasonably limit, the right to a fair and public hearing with respect to administrative decisions.

Conclusion

45. The Bill is compatible with human rights as it strengthens the protection of human rights. Where the Bill may limit particular rights, the limitations are reasonable, necessary, and proportionate with human rights.

The Hon. Stuart Robert MP, Minister for Employment, Workforce, Skills, Small and Family Business