



# **Data Availability and Transparency Act 2022**

**No. 11, 2022**

**An Act to authorise the sharing of public sector  
data, and for related purposes**

Note: An electronic version of this Act is available on the Federal Register of Legislation  
(<https://www.legislation.gov.au/>)



---

# Contents

<b>Chapter 1—Preliminary</b>	<b>2</b>
<b>Part 1.1—Introduction</b>	<b>2</b>
1 Short title .....	2
2 Commencement .....	2
3 Objects .....	2
4 Simplified outline of this Act .....	3
5 Act binds the Crown .....	4
6 Extension to external Territories .....	4
7 Extraterritorial operation .....	4
<b>Part 1.2—Definitions</b>	<b>5</b>
9 Definitions .....	5
10 References to access to data .....	12
11 Entity definitions .....	12
11A The data sharing project .....	14
<b>Chapter 2—Authorisations</b>	<b>16</b>
<b>Part 2.1—Introduction</b>	<b>16</b>
12 Simplified outline of this Chapter .....	16
<b>Part 2.2—Authorisations</b>	<b>18</b>
13 Authorisation for data custodian to share public sector data .....	18
13A Authorisation for accredited user to collect and use data .....	20
13B Authorisation for ADSP to act as intermediary .....	20
13C Authorisation for data custodian to collect and use submitted data .....	21
14 Penalties for unauthorised sharing .....	21
14A Penalties for unauthorised collection or use .....	23
<b>Part 2.3—Data sharing purposes and principles</b>	<b>27</b>
15 Data sharing purposes .....	27
16 Data sharing principles .....	29
<b>Part 2.4—Privacy protections</b>	<b>32</b>
16A General privacy protections .....	32
16B Purpose-specific privacy protections .....	32
16C Project involving use of de-identification or secure access data services .....	35
16D Project involving complex data integration services .....	36

---

16E	Privacy coverage condition .....	38
16F	Compliance with APP-equivalence term .....	39
<b>Part 2.5—When sharing is barred</b>		<b>41</b>
17	When sharing is barred .....	41
<b>Part 2.6—Data sharing agreements</b>		<b>44</b>
18	Data sharing agreement .....	44
19	Requirements to be met by all data sharing agreements .....	45
<b>Part 2.7—Allowed access to output of project</b>		<b>49</b>
20A	Allowed access: providing data custodian of source data with access to ADSP-enhanced data or output .....	49
20B	Allowed access: providing access to output for validation or correction.....	49
20C	Allowed access: providing access to or releasing output in other circumstances .....	50
20D	Allowed access: sharing under section 13 .....	51
20E	Exit of ADSP-enhanced data or output of project .....	51
20F	Data custodian of output of project.....	53
<b>Part 2.8—Relationship with other laws</b>		<b>55</b>
22	Other authorisations for data custodians not limited.....	55
23	Authorisations override other laws .....	55
<b>Chapter 3—Responsibilities of data scheme entities</b>		<b>56</b>
<b>Part 3.1—Introduction</b>		<b>56</b>
24	Simplified outline of this Chapter.....	56
<b>Part 3.2—General responsibilities</b>		<b>57</b>
25	No duty to share but reasons required for not sharing .....	57
26	Comply with rules and data codes .....	57
27	Have regard to guidelines .....	57
30	Comply with conditions of accreditation .....	57
31	Report events and changes in circumstances affecting accreditation to Commissioner .....	58
32	Not provide false or misleading information .....	58
33	Registration of data sharing agreements .....	59
34	Assist Commissioner in relation to annual report .....	59
<b>Part 3.3—Data breach responsibilities</b>		<b>61</b>
35	Definition of <i>data breach</i> .....	61
36	Take steps to mitigate data breach .....	61

---

---

37	Interaction with Part IIIC of the <i>Privacy Act 1988</i> (notification of eligible data breaches) .....	62
38	Notify Commissioner of non-personal data breach .....	64
<b>Chapter 4—National Data Commissioner and National Data Advisory Council</b>		<b>65</b>
<b>Part 4.1—Introduction</b>		<b>65</b>
39	Simplified outline of this Chapter .....	65
40	Commissioner to have regard to objects of Act .....	65
<b>Part 4.2—National Data Commissioner</b>		<b>66</b>
<b>Division 1—Establishment, functions and powers</b>		<b>66</b>
41	National Data Commissioner .....	66
42	Functions .....	66
43	Advice related functions .....	66
44	Guidance related functions .....	67
45	Regulatory functions .....	67
45A	Education and support related functions .....	67
46	Application of finance law .....	68
47	Staff .....	68
48	Contractors .....	68
49	Consultants .....	69
50	Delegation by Commissioner .....	69
51	Independence of Commissioner .....	70
52	Commissioner not to be sued .....	70
<b>Division 2—Terms and conditions etc.</b>		<b>71</b>
53	Appointment .....	71
54	General terms and conditions of appointment .....	71
55	Other paid work .....	71
56	Remuneration .....	71
57	Leave of absence .....	72
58	Resignation .....	72
58A	Disclosure of interests to Minister .....	72
59	Termination of appointment .....	72
60	Acting appointments .....	73
<b>Part 4.3—National Data Advisory Council</b>		<b>75</b>
61	Establishment and function of Council .....	75
62	Membership of Council .....	75
63	Appointment of members .....	76

---

---

64	Term of appointment .....	76
65	Remuneration and allowances .....	76
66	Leave of absence .....	77
67	Disclosure of interests to Minister or Commissioner .....	77
68	Disclosure of interests to Council .....	77
69	Resignation of members .....	77
70	Termination of appointment of members .....	78
71	Other terms and conditions of members .....	78
72	Procedures .....	78
<b>Chapter 5—Regulation and enforcement</b>		<b>80</b>
<b>Part 5.1—Introduction</b>		<b>80</b>
73	Simplified outline of this Chapter .....	80
<b>Part 5.2—Accreditation framework</b>		<b>82</b>
<b>Division 1—Accreditation</b>		<b>82</b>
74	Accreditation .....	82
75	Notice of accreditation decision .....	83
76	Application for accreditation .....	84
77	Criteria for accreditation .....	84
77A	General provisions relating to accreditation .....	85
<b>Division 2—Conditions of accreditation</b>		<b>86</b>
77B	Conditions of accreditation .....	86
78	Imposition, variation or removal of conditions of accreditation by accreditation authority .....	86
79	Notice before decision relating to conditions of accreditation .....	87
80	Notice of conditions .....	88
<b>Division 3—Suspension and cancellation of accreditation</b>		<b>89</b>
81	Suspension or cancellation of accreditation .....	89
82	Notice before decision about suspension or cancellation .....	91
83	Notice of suspension or cancellation .....	92
83A	Lifting of suspension .....	92
<b>Division 4—Renewal of accreditation of ADSPs</b>		<b>94</b>
84	Renewal .....	94
85	Notice of renewal decision .....	95
85A	Application for renewal .....	96
<b>Division 5—Rules and further information</b>		<b>97</b>
86	Rules relating to the accreditation framework .....	97
87	Further information or evidence .....	97

---

---

<b>Part 5.3—Complaints</b>	98
<b>Division 1—Scheme Complaints</b>	98
88 Making scheme complaints .....	98
89 Respondents.....	98
90 Communicating with complainant.....	99
91 Dealing with complaints .....	99
92 Grounds for not dealing with complaints.....	100
93 Admissibility of things said or done in conciliation .....	101
<b>Division 2—General complaints</b>	102
94 Making general complaints .....	102
95 Dealing with complaints .....	102
96 Admissibility of things said or done in conciliation .....	102
<b>Part 5.4—Assessments and investigations</b>	104
99 Assessments.....	104
100 Notices of assessment.....	104
101 Investigations.....	104
102 Determination on completion of investigation.....	106
103 Notices relating to investigation .....	107
103A Recommendations .....	107
<b>Part 5.5—Regulatory powers and enforcement</b>	108
104 Power to require information and documents .....	108
105 Legal professional privilege .....	109
106 Limits on power to require information and documents .....	110
107 Transfer of matters to appropriate authority .....	111
108 Authorisation for Commissioner to disclose and receive information .....	112
109 Monitoring powers .....	113
110 Investigation powers.....	114
112 Directions .....	116
113 Civil penalty provisions.....	117
114 Infringement notices.....	118
115 Enforceable undertakings .....	119
116 Injunctions.....	120
<b>Chapter 6—Other matters</b>	121
<b>Part 6.1—Introduction</b>	121
117 Simplified outline of this Chapter.....	121
<b>Part 6.2—Review of decisions</b>	122

---

---

118	Reviewable decisions .....	122
119	Applications for reconsideration of decisions made by delegates of the reviewer .....	123
120	Reconsideration by reviewer .....	123
121	Deadline for reconsideration.....	124
122	Review by the Administrative Appeals Tribunal.....	124
 <b>Part 6.3—Extension of authorisations and attribution of conduct</b> .....		
		125
123	Designated individuals and designation.....	125
124	Extension of authorisations to share, collect or use data.....	126
125	Other things an entity may or must do under the data sharing scheme.....	127
125A	Contraventions by entities of civil penalty provisions and other non-criminal breaches of this Act.....	127
125B	Offences by entities against this Act.....	129
 <b>Part 6.4—Data sharing scheme instruments</b> .....		
		130
126	Data codes .....	130
127	Guidelines.....	131
128	Register of ADSPs.....	132
129	Register of accredited users.....	132
130	Register of data sharing agreements .....	133
131	Recognition of external dispute resolution schemes .....	135
132	Approved forms.....	136
133	Rules.....	136
134	Regulations.....	136
 <b>Part 6.5—Other matters</b> .....		
		138
135	Disclosure of scheme data in relation to information-gathering powers .....	138
135A	Data held by National Archives of Australia .....	138
136	Geographical jurisdiction of civil penalty provisions and offences .....	139
137	Authorised officers and individuals authorised to do particular things.....	142
137A	Delegation by Minister .....	144
138	Annual report.....	144
139	Charging of fees by Commissioner .....	146
140	Charging of fees by data scheme entities.....	146
141	Commonwealth not liable to pay a fee .....	147
142	Periodic reviews of operation of Act .....	147
143	Sunset of the data sharing scheme .....	148

---





# **Data Availability and Transparency Act 2022**

**No. 11, 2022**

---

---

**An Act to authorise the sharing of public sector  
data, and for related purposes**

*[Assented to 31 March 2022]*

The Parliament of Australia enacts:

Section 1

---

## Chapter 1—Preliminary

### Part 1.1—Introduction

#### 1 Short title

This Act is the *Data Availability and Transparency Act 2022*.

#### 2 Commencement

- (1) Each provision of this Act specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table. Any other statement in column 2 has effect according to its terms.

Commencement information		
Column 1	Column 2	Column 3
Provisions	Commencement	Date/Details
1. The whole of this Act	The day after this Act receives the Royal Assent.	1 April 2022

Note: This table relates only to the provisions of this Act as originally enacted. It will not be amended to deal with any later amendments of this Act.

- (2) Any information in column 3 of the table is not part of this Act. Information may be inserted in this column, or information in it may be edited, in any published version of this Act.

#### 3 Objects

The objects of this Act are to:

- (a) serve the public interest by promoting better availability of public sector data; and
- (b) enable the sharing of public sector data consistently with the *Privacy Act 1988* and appropriate security safeguards; and
- (c) enhance integrity and transparency in sharing public sector data; and

Section 4

---

- (d) build confidence in the use of public sector data; and
- (e) establish institutional arrangements for sharing public sector data.

#### **4 Simplified outline of this Act**

This Act establishes a data sharing scheme under which Commonwealth bodies are authorised to share their public sector data with accredited users, and accredited users are authorised to collect and use the data, in a controlled way.

The sharing, collection and use of data must be part of a project that is for one or more of the defined data sharing purposes, and must be done consistently with the data sharing principles and under a registered data sharing agreement that meets the requirements of this Act. Privacy protections apply to the sharing of personal information.

Data may be shared directly with an accredited user, or through an intermediary accredited for the purpose (called an ADSP, short for accredited data service provider).

The National Data Commissioner is the regulator of the data sharing scheme and also has the function of providing education and support in relation to handling public sector data.

The Commissioner's regulatory functions include accrediting ADSPs and users other than Commonwealth, State and Territory bodies. The Minister has the function of accrediting such bodies as users.

The Commissioner also has functions relating to handling complaints and powers to require information and to assess, monitor and investigate data scheme entities.

Data scheme entities have responsibilities under the Act. A range of enforcement options are available to the Commissioner.

## Section 5

---

This Act mainly relies for its constitutional basis on the matters set out in subsection 13(4) (constitutional requirements for authorisation for data custodian to share public sector data) (but see also subsections 42(2) and 61(2)).

### **5 Act binds the Crown**

- (1) This Act binds the Crown in each of its capacities.
- (2) However, this Act does not make the Crown liable to be prosecuted for an offence.
- (3) To avoid doubt, subsection (2) does not prevent the Crown from being liable to pay a pecuniary penalty under a civil penalty order under Part 4 of the Regulatory Powers Act, as that Part applies in relation to the civil penalty provisions of this Act.

### **6 Extension to external Territories**

This Act and the Regulatory Powers Act as it applies in relation to this Act extend to every external Territory.

### **7 Extraterritorial operation**

- (1) This Act, and the Regulatory Powers Act as it applies in relation to this Act, extend to acts, omissions, matters and things outside Australia.

Note: Geographical jurisdiction for civil penalty provisions and offences is dealt with in section 136.

- (2) This Act, and the Regulatory Powers Act as it applies in relation to this Act, have effect in relation to acts, omissions, matters and things outside Australia subject to:
  - (a) the obligations of Australia under international law, including obligations under any international agreement binding on Australia; and
  - (b) any law of the Commonwealth giving effect to such an agreement.

## Part 1.2—Definitions

### 9 Definitions

In this Act:

***access*** has a meaning affected by section 10.

***accreditation authority*** means:

- (a) for an entity applying for accreditation, or accredited, as an ADSP—the Commissioner; or
- (b) for a Commonwealth body, State body or Territory body, or the Commonwealth or a State or Territory, applying for accreditation, or accredited, as an accredited user—the Minister; or
- (c) for another entity applying for accreditation, or accredited, as an accredited user—the Commissioner.

***accredited entity***: see subsection 11(4).

***accredited user***: see subsection 11(4).

***ADSP***: see subsection 11(4).

***ADSP-controlled access***: see subsection 16B(6).

***ADSP-enhanced data***: see subsection 11A(3).

***adverse or qualified security assessment*** means an adverse security assessment, or a qualified security assessment, within the meaning of Part IV of the *Australian Security Intelligence Organisation Act 1979*.

***ancillary contravention*** of a civil penalty provision means a contravention that arises out of the operation of section 92 of the Regulatory Powers Act.

***ancillary offence*** has the same meaning as in the *Criminal Code*.

***APP entity*** has the same meaning as in the *Privacy Act 1988*.

## Section 9

---

***APP-equivalence term***: see subsection 16E(2).

***appointed member***: see paragraph 62(1)(e).

***approved contract***: see subsection 123(3).

***approved form*** for a provision of this Act, the rules or a data code means a form approved by the Commissioner for the purposes of the provision under section 132.

***Australia***, when used in a geographical sense, includes the external Territories.

***Australian aircraft*** has the same meaning as in the *Criminal Code*.

***Australian entity*** means an entity that is any of the following:

- (a) a Commonwealth body, a State body or a Territory body;
- (b) the Commonwealth, a State or a Territory;
- (c) an Australian university.

***Australian ship*** has the same meaning as in the *Criminal Code*.

***Australian university*** means a registered higher education provider:

- (a) that, for the purposes of the *Tertiary Education Quality and Standards Agency Act 2011*, is registered in the “Australian University” provider category; and
- (b) that is established by or under a law of the Commonwealth, a State or a Territory.

***authorised officer***: see section 137.

***biometric data***:

- (a) means personal information about any measurable biological or behavioural characteristic relating to an individual that could be used to identify the individual or verify the individual’s identity; and
- (b) includes a biometric template containing representations of information mentioned in paragraph (a).

Note: Data that is not personal information cannot be biometric data. For example, an eye colour, by itself, is not biometric data.

Section 9

---

***breach***: a data scheme entity ***breaches*** this Act if the data scheme entity engages in conduct that contravenes, or is inconsistent with, this Act.

***Circuit Court*** means the Federal Circuit and Family Court of Australia (Division 2).

***civil penalty provision*** has the same meaning as in the Regulatory Powers Act.

***Commissioner*** means the National Data Commissioner referred to in section 41.

***Commonwealth body***:

- (a) means:
  - (i) a Commonwealth entity, or a Commonwealth company, within the meaning of the *Public Governance, Performance and Accountability Act 2013*; or
  - (ii) any other person or body that is an agency within the meaning of the *Freedom of Information Act 1982*; but
- (b) does not include an Australian university.

***complex data integration service***: see subsection 16D(3).

***condition of accreditation*** means a condition:

- (a) prescribed by the rules for the purposes of subsection 77B(1); or
- (b) imposed under section 74, 78 or 84.

***constitutional corporation*** means a corporation to which paragraph 51(xx) of the Constitution applies.

***Council*** means the National Data Advisory Council established by section 61.

***court/tribunal order*** means an order, direction or other instrument made by:

- (a) a court; or
- (b) a judge (including a judge acting in a personal capacity) or a person acting as a judge; or

## Section 9

---

- (c) a magistrate (including a magistrate acting in a personal capacity) or a person acting as a magistrate; or
- (d) any other person or body that has the power to act judicially under a law of the Commonwealth or a State or Territory; or
- (e) a tribunal; or
- (f) a member or an officer of a tribunal;

and includes an order, direction or other instrument that is of an interim or interlocutory nature.

**data** means any information in a form capable of being communicated, analysed or processed (whether by an individual or by computer or other automated means).

**data breach**: see section 35.

**data code**: see subsection 126(1).

**data custodian**: see subsection 11(2).

**data scheme entity**: see subsection 11(1).

**data service** means any operation performed on or in relation to data, at any stage from collection or creation to destruction.

**data sharing agreement**: see section 18.

**data sharing purpose**: see subsection 15(1).

**data sharing scheme** means this Act and the regulations, rules, data codes and guidelines made under it.

**Defence Department** means the Department administered by the Minister administering the *Defence Act 1903*.

**de-identification data service**: see subsection 16C(3).

**de-identified** has the same meaning as in the *Privacy Act 1988*.

**delivery of government services**: see subsection 15(1A).

**designated individual**: see section 123.

**designation**: see section 123.



Section 9

---

***electronic communication*** means a communication of information in any form by means of guided electromagnetic energy, unguided electromagnetic energy or both.

***enforcement related purpose***: see subsection 15(3).

***engage in conduct*** means:

- (a) do an act; or
- (b) omit to do an act.

***entity*** means any of the following:

- (a) a Commonwealth body, a State body or a Territory body;
- (b) a body politic;
- (c) an Australian university;
- (d) a body corporate;
- (e) an individual.

***excluded entity***: see subsection 11(3).

***exit***: see section 20E.

***Federal Court*** means the Federal Court of Australia.

***final output*** of a project means the output specified as the agreed final output in the data sharing agreement for the project (see paragraph 19(3)(b)).

***guidelines*** means guidelines made under section 127.

***government entity***: see subsection 125A(4).

***offence against this Act*** includes an offence against section 6 of the *Crimes Act 1914*, or Chapter 7 of the *Criminal Code*, that relates to this Act.

Note: Ancillary offences that relate to this Act are also offences against this Act (see section 11.6 of the *Criminal Code*).

***operational data*** means:

- (a) data about information sources or operational activities or methods available to an agency mentioned in paragraph 17(2)(b); or

Section 9

---

- (b) data about particular operations that have been, are being or are proposed to be undertaken by such an agency, or about proceedings relating to those operations.

**output:** see subsection 11A(1).

**paid work** means work for financial gain or reward (whether as an employee, a self-employed person or otherwise).

**personal information** has the same meaning as in the *Privacy Act 1988*.

Note: Information that has been de-identified is no longer personal information.

**point:** see subsection 136(9).

**precluded purpose:** see subsections 15(2) and (4).

**primary contravention** of a civil penalty provision means a contravention that does not arise out of the operation of section 92 of the Regulatory Powers Act.

**primary offence** has the same meaning as in the *Criminal Code*.

**project:** see section 11A.

**public sector data** means data lawfully collected, created or held by or on behalf of a Commonwealth body, and includes ADSP-enhanced data.

**registered:** a data sharing agreement is **registered** if the agreement is included in the register of data sharing agreements under subsection 130(4).

**regulatory function** means a function set out in subsection 45(1).

**Regulatory Powers Act** means the *Regulatory Powers (Standard Provisions) Act 2014*.

**release:** see subsection 10(1).

**reviewable decision:** see section 118.

**reviewer:** see section 118.

Section 9

---

**rules** means rules made under subsection 133(1).

**scheme data** means:

- (a) any copy of data created for the purpose of being shared under section 13 as part of a project and held by the entity that is the sharer mentioned in that section, whether or not the data has yet been shared; or
- (b) output of a project, other than a copy that has exited the data sharing scheme (see section 20E); or
- (c) ADSP-enhanced data of a project, other than a copy that has exited the data sharing scheme (see section 20E).

**secure access data service**: see subsection 16C(4).

**security** has the same meaning as in the *Australian Security Intelligence Organisation Act 1979*.

**share**: see subsection 10(2).

**source data**: see paragraph 19(3)(a).

**State body** means any of the following, but does not include an Australian university:

- (a) a department of a State;
- (b) a body established for a public purpose by or under a law of a State, other than a body prescribed by the rules;
- (c) the holder of a statutory office appointed under a law of a State, other than an office prescribed by the rules.

**submit**: see subsection 20A(3).

**Territory body** means any of the following, but does not include an Australian university:

- (a) a department of a Territory;
- (b) a body established for a public purpose by or under a law of a Territory, other than a body prescribed by the rules;
- (c) the holder of a statutory office appointed under a law of a Territory, other than an office prescribed by the rules.

**use** includes handle, store and provide access.

## Section 10

---

Note: Examples of use of data by an accredited user include developing and modifying output.

### 10 References to access to data

- (1) For the purposes of this Act, a reference to an entity providing access to data includes a reference to the entity:
  - (a) providing another entity with access to the data; and
  - (b) providing open access to the data (***releasing*** the data).
- (2) This Act uses the expression ***share*** to refer to data custodians of public sector data providing accredited entities with access to data under this Act.
- (3) For the purposes of this Act, if an entity provides another entity with access to data:
  - (a) the entity that provides access is taken to retain a copy of the data; and
  - (b) the entity to which access is provided is taken to collect a copy of the data.

### 11 Entity definitions

- (1) The following are ***data scheme entities***:
  - (a) data custodians of public sector data;
  - (b) accredited entities.
- (2) An entity is a ***data custodian*** if the entity:
  - (a) is a Commonwealth body; and
  - (b) is not an excluded entity; and
  - (c) either:
    - (i) controls public sector data (whether alone or jointly with another entity), including by having the right to deal with that data; or
    - (ii) has become the data custodian of output of a project in accordance with section 20F.
- (2A) If a data custodian of public sector data shares the data with an intermediary under section 13 as part of a project, the data

Section 11

---

custodian is taken also to be the data custodian of any ADSP-enhanced data of the project.

- (3) Each of the following is an ***excluded entity***:
- (aa) the National Data Commissioner and any APS employee made available to the National Data Commissioner under section 47;
  - (a) the Australian Commission for Law Enforcement Integrity;
  - (b) the agency known as the Australian Criminal Intelligence Commission established by the *Australian Crime Commission Act 2002*;
  - (ba) the Australian Federal Police;
  - (c) that part of the Defence Department known as the Australian Geospatial-Intelligence Organisation;
  - (d) the Australian National Audit Office;
  - (e) the Australian Secret Intelligence Service;
  - (f) the Australian Security Intelligence Organisation;
  - (g) the Australian Signals Directorate;
  - (h) that part of the Defence Department known as the Defence Intelligence Organisation;
  - (i) the Inspector-General of Intelligence and Security;
  - (j) the Office of the Commonwealth Ombudsman;
  - (k) the Office of National Intelligence.

- (4) An entity accredited under section 74 as an:
- (a) accredited user (an ***accredited user***); or
  - (b) ADSP (short for accredited data service provider) (an ***ADSP***);

is an ***accredited entity***.

Note 1: Accredited users are able to collect and use shared data (including by creating output they can provide other entities with access to, or release) in accordance with an applicable data sharing agreement. ADSPs are expert intermediaries who can assist data custodians to prepare and share data appropriately.

Note 2: Excluded entities cannot be accredited (see subsection 74(1)).

- (5) A data scheme entity may do things under this Act in different capacities. In each of those capacities, the entity is taken to be a

## Section 11A

---

different data scheme entity. Among other things, this means that a data scheme entity may enter into a data sharing agreement to which it is party in more than one capacity.

Note: For 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.

### 11A The data sharing project

*Project, and output and ADSP-enhanced data of project*

- (1) A **project** involves at least both of the following elements:
  - (a) an entity (the **sharer**) shares data with another entity (the **user**), either directly or through another entity (the **intermediary**);
  - (b) the user collects the data and uses the **output** of the project, which is:
    - (i) the copy of the data collected by the user; and
    - (ii) any data that is the result or product of the user's use of the shared data.

Note 1: The sharer's authorisation to share data is in section 13. The user's authorisation to collect and use data is in section 13A.

Note 2: A project may involve sharing of data by multiple sharers, if multiple entities are data custodians of the data.
- (2) If, for the purposes of sharing data under section 13, data services are performed in relation to data, or data is created, by or on behalf of the sharer, the **project** also involves performing the services or creating the data.
- (3) If the sharer shares data with the user through an intermediary, the **project** also involves both of the following elements:
  - (a) the sharer shares the data with the intermediary;
  - (b) the intermediary collects the data and uses the **ADSP-enhanced data** of the project, which is:
    - (i) the copy of the data collected by the intermediary; and
    - (ii) any data that is the result or product of the intermediary's use of the shared data.

## Section 11A

---

Note: The sharer's authorisation to share data with the intermediary, and the intermediary's authorisation to share data with the user on behalf of the sharer, are in section 13. The intermediary's authorisation to collect data from the sharer and use it is in section 13B.

- (4) If the sharer is provided with access to output or ADSP-enhanced data of the project, the **project** also involves the sharer's collection and use of the output or ADSP-enhanced data.

Note: The sharer's authorisation to collect and use the output or ADSP-enhanced data of the project is in section 13C.

### *Combining projects*

- (5) A data sharing agreement may treat multiple projects as a single project, as long as they all have the same data sharing purpose or purposes and the same sharer and user and (if applicable) intermediary.

### *Successive projects*

- (6) If the user in a project shares data that is output of the project as part of a later project:
- (a) the copy retained by the user continues to be output of the earlier project; and
  - (b) the copy collected by the user in the later project is output of the later project in accordance with paragraph (1)(b); and
  - (c) if the sharing in the later project is done through an intermediary—the copy collected by the intermediary in the later project is ADSP-enhanced data of the later project in accordance with paragraph (3)(b).

Note: A data sharing agreement may allow the user to share output under section 13 as part of a later project (see section 20D).

## **Chapter 2—Authorisations**

### **Part 2.1—Introduction**

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

Under the data sharing scheme, Commonwealth bodies are authorised to share their public sector data with accredited users, and accredited users are authorised to collect and use the data, in a controlled way. Data may be shared with an accredited user directly, or through an intermediary accredited for the purpose (called an ADSP, short for accredited data service provider).

The sharing, collection and use of data must be part of a project that is for one or more of the defined data sharing purposes, and must be done consistently with the data sharing principles and a registered data sharing agreement that meets the requirements of this Act. Privacy protections apply to the sharing of personal information.

Commonwealth bodies must be the data custodian of public sector data they share (i.e. they must control the data, including by having the right to deal with it). Some Commonwealth bodies are excluded from the scheme.

Some sharing of data is barred (e.g. if the sharing would contravene a prescribed law or an agreement).

An accredited user's authorisation to use data may in some circumstances extend to providing access to output of the project to other entities, which may or may not be accredited. There are limits on the circumstances in which data sharing agreements may allow this.

If sharing, collection or use is authorised by this Chapter, the authorisation has effect despite any other law of the Commonwealth or a State or Territory.



## Section 12

---

Data custodians and accredited entities must comply with the rules made by the Minister and data codes made by the National Data Commissioner and meet other responsibilities under this Chapter.

This Act mainly relies for its constitutional basis on the matters set out in subsection 13(4) (constitutional requirements for authorisation for data custodian to share public sector data) (but see also subsections 42(2) and 61(2)).

## Part 2.2—Authorisations

### 13 Authorisation for data custodian to share public sector data

- (1) An entity (the *sharer*) is authorised to share data with another entity (the *user*), either directly or through another entity (the *intermediary*), if all of the following apply:
- (a) the constitutional requirements in subsection (4) are met;
  - (b) the data custodian requirements in subsection (2) are met;
  - (c) the project the sharing is part of is covered by a registered data sharing agreement that is in effect and that meets the requirements of this Act;
  - (d) the sharing is in accordance with the data sharing agreement;
  - (e) the sharer is satisfied that the project is consistent with the data sharing principles;
  - (f) the user is an accredited user and its accreditation is not suspended;
  - (g) if the data shared with the user includes personal information—the privacy coverage condition in section 16E is met in relation to the user;
  - (h) if the sharer shares through an intermediary—the intermediary is an ADSP and its accreditation is not suspended;
  - (i) if the data shared with the intermediary includes personal information—the privacy coverage condition in section 16E is met in relation to the intermediary.

Note: This section authorises the sharer to share its public sector data with the user and with the intermediary (if any). It also authorises the intermediary (if any) to share with the user, on behalf of the sharer, ADSP-enhanced data of which the sharer is the data custodian.

- (2) The data custodian requirements are the following:
- (a) the data is public sector data and the sharer is the data custodian of the data;

Section 13

---

- (b) if the sharer is not the only data custodian of the data—  
authority to share the data has been given by each other data  
custodian;
- (c) the sharing is not barred by section 17;
- (d) the sharing is consistent with the general privacy protections  
in section 16A and the purpose-specific privacy protections  
in section 16B;
- (e) if the data shared does not include personal information—  
only the minimum amount of data necessary for the project to  
proceed is shared;
- (f) if the requirement in subsection 16C(2) or 16D(2) applies—  
the requirement is met.

Note: If sharing is done through an intermediary, it is possible that authority to share as mentioned in paragraph (2)(b) will be needed from additional data custodians of ADSP-enhanced data of the project, before the ADSP-enhanced data can be shared with the user.

- (3) Authority given by a data custodian for the purposes of  
paragraph (2)(b) must be given by one of the following:
  - (a) an authorised officer of that data custodian;
  - (b) if another data custodian is authorised to act as the agent of  
that data custodian—an authorised officer of the agent data  
custodian.
- (4) The constitutional requirements are that any of the following  
apply:
  - (a) the data is shared with a Commonwealth body or Territory  
body, or the Commonwealth or a Territory;
  - (b) the data is shared with a State body or a State, as part of a  
project that:
    - (i) relates to a matter of national interest that requires  
national cooperation to achieve an identified national  
objective; or
    - (ii) addresses an immediate need to take coordinated action  
in an area that will have significant national and  
cross-jurisdictional effect; or
    - (iii) occurs in the context of the Commonwealth otherwise  
facilitating cooperation with or between the States;

## Section 13A

---

- (c) the data is shared as part of a project that is for a data sharing purpose set out in paragraph 15(1)(a) (delivery of government services) or (b) (informing government policy and programs), if the government concerned is or includes the Commonwealth;
- (d) the data is shared with a constitutional corporation as part of a project that is for the data sharing purpose set out in paragraph 15(1)(c) (research and development);
- (e) the data is shared by means of electronic communication;
- (f) the data is shared to enable analysis for statistical purposes;
- (g) the data is statistical information.

### 13A Authorisation for accredited user to collect and use data

An entity (the *user*) is authorised to collect data shared with the user under, or purportedly under, section 13 as part of a project, or to use output of the project, if all of the following apply:

- (a) the project is covered by a registered data sharing agreement that is in effect and that meets the requirements of this Act;
- (b) the collection or use is in accordance with the data sharing agreement;
- (c) the user is satisfied that the project is consistent with the data sharing principles;
- (d) the user is an accredited user and its accreditation is not suspended;
- (e) if the data shared with the user includes personal information—the privacy coverage condition in section 16E is met in relation to the user;
- (f) if the sharing by the sharer is not authorised by section 13—the user does not know and could not reasonably be expected to know that.

### 13B Authorisation for ADSP to act as intermediary

If an entity (the *sharer*) is sharing data with another entity (the *user*) under, or purportedly under, section 13 through another entity (the *intermediary*) as part of a project, the intermediary is

## Section 13C

---

authorised to collect data shared with it by the sharer, or to use ADSP-enhanced data of the project, if all of the following apply:

- (a) the project is covered by a registered data sharing agreement that is in effect and that meets the requirements of this Act;
- (b) the collection or use is in accordance with the data sharing agreement;
- (c) the intermediary is satisfied that the project is consistent with the data sharing principles;
- (d) the intermediary is an ADSP and its accreditation is not suspended;
- (e) if the data shared with the intermediary includes personal information—the privacy coverage condition in section 16E is met in relation to the intermediary;
- (f) if the sharing by the sharer is not authorised by section 13—the intermediary does not know and could not reasonably be expected to know that.

### **13C Authorisation for data custodian to collect and use submitted data**

If an entity (the *sharer*) has shared data with the user under section 13 as part of a project, either directly or through an intermediary, the sharer is authorised to collect output or ADSP-enhanced data of the project from the user or intermediary, or to use output or ADSP-enhanced data of the project collected from the user or intermediary, if both of the following apply:

- (a) the project is covered by a registered data sharing agreement that is in effect and that meets the requirements of this Act;
- (b) the collection or use by the sharer is in accordance with the data sharing agreement.

## **14 Penalties for unauthorised sharing**

### *Civil penalty provisions*

- (1) An entity contravenes this subsection if:
  - (a) the entity provides access to data; and
  - (b) the provision of access is purportedly under section 13; and

## Section 14

---

(c) the provision of access is not authorised by section 13.

Civil penalty: 300 penalty units.

- (2) An individual or a body corporate contravenes this subsection if:
- (a) the individual or body corporate uses data; and
  - (b) the use is a provision of access to the data by an entity under, or purportedly under, section 13; and
  - (c) the individual has a designated relationship with the entity, or the body corporate is party to an approved contract with the entity; and
  - (d) the individual or body corporate's use is not authorised by this Act.

Civil penalty: 300 penalty units.

### *Offences*

- (3) An entity commits an offence if:
- (a) the entity provides access to data; and
  - (b) the provision of access is purportedly under section 13; and
  - (c) the provision of access is not authorised by section 13 and the entity is reckless with respect to that circumstance.

Penalty: Imprisonment for 5 years or 300 penalty units, or both.

- (4) An individual or a body corporate commits an offence if:
- (a) the individual or body corporate uses data; and
  - (b) the use is a provision of access to the data by an entity under, or purportedly under, section 13; and
  - (c) the individual has a designated relationship with the entity, or the body corporate is party to an approved contract with the entity; and
  - (d) the individual or body corporate's use is not authorised by this Act and the individual is reckless with respect to that circumstance.

Penalty: Imprisonment for 5 years or 300 penalty units, or both.

## **14A Penalties for unauthorised collection or use**

### *Civil penalty provisions for user or intermediary*

- (1) An entity contravenes this subsection if:
- (a) the entity collects or uses data; and
  - (b) the data is ADSP-enhanced data, or output, of a project involving sharing data with the entity under, or purportedly under, section 13; and
  - (c) the collection or use is not authorised by this Act.

Civil penalty:

- (a) 300 penalty units; or
  - (b) if subsection (2) applies—600 penalty units.
- (2) This subsection applies if the entity concerned is or has been an accredited entity and the contravention is serious, having regard to any of the following matters:
- (a) the sensitivity of the data;
  - (b) the consequences of the contravention for entities, groups of entities or things to which the data involved in the contravention relates;
  - (c) the level of care taken by the contravening entity in relation to the entity's responsibilities under the data sharing scheme in relation to the collection or use.
- (3) An individual or a body corporate contravenes this subsection if:
- (a) the individual or body corporate uses data; and
  - (b) the data is ADSP-enhanced data, or output, of a project involving sharing data with an entity under, or purportedly under, section 13; and
  - (c) the individual has a designated relationship with the entity, or the body corporate is party to an approved contract with the entity; and
  - (d) the individual or body corporate's use of the data is not authorised by this Act.

Civil penalty: 300 penalty units.

## Section 14A

---

### *Offences for user or intermediary*

- (4) An entity commits an offence if:
- (a) the entity collects or uses data; and
  - (b) the data is ADSP-enhanced data, or output, of a project involving sharing data with the entity under, or purportedly under, section 13; and
  - (c) the collection or use is not authorised by this Act and the entity is reckless with respect to that circumstance.

Penalty: Imprisonment for 5 years or 300 penalty units, or both.

- (5) An individual or a body corporate commits an offence if:
- (a) the individual or body corporate uses data; and
  - (b) the data is ADSP-enhanced data, or output, of a project involving sharing data with an entity under, or purportedly under, section 13; and
  - (c) the individual has a designated relationship with the entity, or the body corporate is party to an approved contract with the entity; and
  - (d) the individual or body corporate's use of the data is not authorised by this Act and the individual or body corporate is reckless with respect to that circumstance.

Penalty: Imprisonment for 5 years or 300 penalty units, or both.

### *Defence*

- (6) Subsections (1), (3), (4) and (5) do not apply if the data collected or used is a copy of output, or ADSP-enhanced data, that has exited the data sharing scheme, or is derived from such a copy.

Note: A defendant bears an evidential burden in relation to the matter in subsection (6) (see subsection 13.3(3) of the *Criminal Code*).

### *Civil penalty provisions for sharer*

- (7) An entity contravenes this subsection if:
- (a) the entity collects or uses data submitted to the entity under, or purportedly under, section 13A or 13B; and
  - (b) the collection or use is not authorised by this Act.



Section 14A

---

Civil penalty: 300 penalty units.

- (8) An individual or a body corporate contravenes this subsection if:
- (a) the individual or body corporate uses data; and
  - (b) the data was submitted to an entity under, or purportedly under, section 13A or 13B; and
  - (c) the individual has a designated relationship with the entity, or the body corporate is party to an approved contract with the entity; and
  - (d) the individual or body corporate's use is not authorised by this Act.

Civil penalty: 300 penalty units.

*Offences for sharer*

- (9) An entity commits an offence if:
- (a) the entity collects or uses data submitted to the entity under, or purportedly under, section 13A or 13B; and
  - (b) the collection or use is not authorised by this Act and the entity is reckless with respect to that circumstance.

Penalty: Imprisonment for 5 years or 300 penalty units, or both.

- (10) An individual or a body corporate commits an offence if:
- (a) the individual or body corporate uses data; and
  - (b) the data was submitted to an entity under, or purportedly under, section 13A or 13B; and
  - (c) the individual has a designated relationship with the entity, or the body corporate is party to an approved contract with the entity; and
  - (d) the individual or body corporate's use is not authorised by this Act and the individual or body corporate is reckless with respect to that circumstance.

Penalty: Imprisonment for 5 years or 300 penalty units, or both.

Section 14A

---

*Relationship of collection and use civil penalty provisions and offences with other laws*

- (11) Subsections (1) to (10) have effect despite any other law of the Commonwealth or a State or Territory, whether enacted before or after the commencement of this Act.
- (12) To avoid doubt, subsections (1) to (10) have effect regardless of whether a permitted general situation, or a permitted health situation, exists within the meaning of the *Privacy Act 1988*.

## Part 2.3—Data sharing purposes and principles

### 15 Data sharing purposes

#### *Data sharing purposes*

- (1) The following are ***data sharing purposes***:

- (a) delivery of government services;
- (b) informing government policy and programs;
- (c) research and development.

Note: Data sharing agreements must specify the agreed data sharing purpose or purposes and agreed incidental purposes (if any), and prohibit collection or use of data for any other purpose, including any precluded purpose.

#### *Delivery of government services*

- (1A) For the purposes of paragraph (1)(a), ***delivery of government services*** means the delivery of any of the following services by the Commonwealth or a State or Territory:

- (a) providing information;
- (b) providing services, other than services relating to a payment, entitlement or benefit;
- (c) determining eligibility for a payment, entitlement or benefit;
- (d) paying a payment, entitlement or benefit.

Note: Making a decision under legislation about whether an individual is eligible to receive a payment, before any payment is made, is an example of delivery of government services. The purpose of making such a decision is not a precluded purpose.

#### *Precluded purposes*

- (2) The following are ***precluded purposes***:

- (a) an enforcement related purpose;
- (b) a purpose that relates to, or prejudices, national security within the meaning of the *National Security Information (Criminal and Civil Proceedings) Act 2004*;

## Section 15

---

(c) a purpose prescribed by the rules for the purposes of this paragraph.

(3) An ***enforcement related purpose*** means any of the following purposes:

(a) detecting, investigating, prosecuting or punishing:

(i) an offence; or

(ii) a contravention of a law punishable by a pecuniary penalty;

(b) detecting, investigating or addressing acts or practices detrimental to public revenue;

(c) detecting, investigating or remedying serious misconduct;

(d) conducting surveillance or monitoring, or intelligence-gathering activities;

(e) conducting protective or custodial activities;

(f) enforcing a law relating to the confiscation of proceeds of crime;

(g) preparing for, or conducting, proceedings before a court or tribunal or implementing a court/tribunal order.

Note: The purpose of verifying that a government payment previously made to a person was correctly made is an example of an enforcement related purpose. Other examples include the purpose of recovering overpayments, identifying individuals for compliance activity and identifying individuals for the purposes of exercising statutory investigation powers.

(4) A purpose is not a ***precluded purpose*** within the meaning of paragraph (2)(a) or (b) if the purpose is both:

(a) a data sharing purpose; and

(b) a purpose that:

(i) is with respect to matters that relate only in a general way to a purpose mentioned in paragraph (2)(a) or (b); and

(ii) does not involve any person undertaking an activity mentioned in a paragraph of subsection (3).

Section 16

---

*Preparing data for a later project*

- (5) A project that involves sharing, collecting and using data in order to prepare (including to create) data for sharing under section 13 as part of a later project that will be for one or more of the data sharing purposes is itself taken to be a project for that or those data sharing purposes.
- (6) Subsection (5) applies regardless of whether the entities sharing, collecting and using the data have a particular later project in mind and whether the data is actually shared under section 13 as part of any later project.

## **16 Data sharing principles**

*Project principle*

- (1) The project principle is that the project is an appropriate project or program of work.
- (2) The project principle includes (but is not limited to) the following elements:
  - (a) the project can reasonably be expected to serve the public interest;
  - (b) the parties observe processes relating to ethics, as appropriate in the circumstances.

*People principle*

- (3) The people principle is that data is made available only to appropriate persons.
- (4) The people principle includes (but is not limited to) the following elements:
  - (a) access to data is only provided to individuals who have attributes, qualifications, affiliations or expertise appropriate for the access;
  - (b) the entity sharing the data considers the following matters in relation to the entity collecting the data (the *collector*):

Section 16

---

- (i) the collector's experience with projects involving the sharing of public sector data, under this Act or otherwise;
- (ii) the collector's capacity to handle public sector data securely;
- (iii) any data breaches, or breaches of the law relating to data, by the collector;
- (iv) any other matters specified in a data code.

*Setting principle*

- (5) The setting principle is that data is shared, collected and used in an appropriately controlled environment.
- (6) The setting principle includes (but is not limited to) the following elements:
  - (a) the means by which the data is shared, collected and used are appropriate, having regard to the type and sensitivity of the data, to control the risks of unauthorised use;
  - (b) reasonable security standards are applied when sharing, collecting and using data.

*Data principle*

- (7) The data principle is that appropriate protections are applied to the data.
- (8) The data principle includes (but is not limited to) the element that only the data reasonably necessary to achieve the applicable data sharing purpose or purposes is shared, collected and used.

*Output principle*

- (9) The output principle is that the only output of the project is:
  - (a) the final output; and
  - (b) output the creation of which is reasonably necessary or incidental to creation of the final output.
- (10) The output principle includes (but is not limited to) the following elements:

Section 16

---

- (a) the data custodian of the data and the accredited user consider:
  - (i) the nature and intended use of the output of the project;  
and
  - (ii) requirements and procedures for use of the output of the project;
- (b) the final output contains only the data reasonably necessary to achieve the applicable data sharing purpose or data sharing purposes.

*Application of data sharing principles*

- (11) For a data scheme entity to be satisfied that the project is consistent with the data sharing principles, the entity must be satisfied that it has applied each principle to the sharing, collection or use of data in such a way that, when viewed as a whole, the risks associated with the sharing, collection or use are appropriately mitigated.

Note: Entities must also comply with the rules and any data codes (see section 26) and have regard to the guidelines (see section 27).

Section 16A

---

## Part 2.4—Privacy protections

### 16A General privacy protections

- (1) Data that includes biometric data must not be shared unless the individual to whom the biometric data relates expressly consents to the sharing of the biometric data.
- (2) If data that includes personal information is shared, the data sharing agreement that covers the sharing must prohibit any accredited entity with or through which it is shared from storing or accessing, or providing access to, the ADSP-enhanced data, or the output, of the project outside Australia.
- (3) If data that has been de-identified is shared, the data sharing agreement that covers the sharing must prohibit the accredited user from taking any action that may have the result that the data ceases to be de-identified.

### 16B Purpose-specific privacy protections

*If data sharing purpose is delivery of government services*

- (1) If the data sharing purpose of the project is delivery of government services, the data must not include personal information about an individual unless:
  - (a) one or more of the following apply:
    - (i) the service being delivered is a service mentioned in paragraph 15(1A)(a) or (b) and is delivered to the individual;
    - (ii) the individual consents to the sharing of their personal information;
    - (iii) the sharing would be a disclosure authorised under Part VIA of the *Privacy Act 1988* (dealing with personal information in emergencies and disasters); and
  - (b) the service being delivered is identified in the data sharing agreement for the project; and



Section 16B

---

- (c) only the minimum amount of personal information necessary to properly deliver the service is shared.
- (2) If data that includes personal information is to be shared with an accredited user in circumstances in which the shared data exits the data sharing scheme under subsection 20E(4), the data sharing agreement must specify this.

*If data sharing purpose is informing government policy and programs or research and development*

- (3) If the data sharing purpose of the project is informing government policy and programs, or research and development, the data must not include personal information about an individual unless:
  - (a) both of the following apply:
    - (i) the individual consents to the sharing of their personal information;
    - (ii) only the minimum amount of personal information necessary for the project to proceed is shared; or
  - (b) all of the following apply:
    - (i) the project cannot proceed without the personal information;
    - (ii) the public interest served by the project justifies the sharing of personal information about individuals without their consent;
    - (iii) only the minimum amount of personal information necessary for the project to proceed is shared;
    - (iv) a permitted circumstance for the project's data sharing purpose exists (see subsections (4) and (5)).
- (4) The permitted circumstances for the data sharing purpose of informing government policy and programs are the following:
  - (a) it is unreasonable or impracticable to seek the individual's consent;
  - (b) the data is to be collected and used in the course of medical research and in accordance with guidelines under subsection 95(1) of the *Privacy Act 1988*;

## Section 16B

---

- (c) the sharing is with an ADSP as an intermediary, to enable the ADSP to prepare ADSP-enhanced data that does not involve personal information about the individual;
- (d) the sharing is ADSP-controlled access (see subsection (6));
- (e) the accredited user is a Commonwealth body (other than a Commonwealth body excluded from this paragraph by the rules) and the final output of the project includes only de-identified information;
- (f) the sharing is a disclosure authorised under Part VIA of the *Privacy Act 1988* (dealing with personal information in emergencies and disasters).

Note: It is not unreasonable or impracticable to seek an individual's consent merely because the consent of a very large number of individuals needs to be sought. The Commissioner is also required to make a data code dealing with this matter.

- (5) The permitted circumstances for the data sharing purpose of research and development are the circumstances mentioned in paragraphs (4)(a) to (d).
- (6) Sharing is ***ADSP-controlled access*** if:
  - (a) an ADSP is sharing the data on behalf of the data custodian with an accredited user; and
  - (b) the data is shared by means of the ADSP providing access to the data:
    - (i) by use of systems controlled by the ADSP; and
    - (ii) to particular identified designated individuals for the entity, each of whom has appropriate experience, qualifications or training; and
  - (c) the ADSP has implemented controls to prevent or minimise the risk of the data being used to identify individuals.
- (7) If the data custodian of the data being shared concludes that, in relation to the sharing of personal information under the agreement for the purpose of informing government policy and programs, or research and development, the circumstance mentioned in paragraph (4)(a) exists (unreasonable or impracticable to seek individual's consent), the agreement must include:

## Section 16C

---

- (a) a statement that personal information is being shared without consent of individuals because it is unreasonable or impracticable to seek their consent; and
  - (b) an explanation of the data custodian's reasons for so concluding.
- (8) If personal information about an individual is to be shared without the consent of the individual for the data sharing purpose of informing government policy and programs, or research and development, the data sharing agreement must include a statement setting out why sharing the personal information is consistent with this section.

### **16C Project involving use of de-identification or secure access data services**

- (1) The requirement in subsection (2) applies if:
  - (a) the data sharing purpose of the project is informing government policy and programs or research and development; and
  - (b) the project involves performing a de-identification data service (see subsection (3)) or a secure access data service (see subsection (4)).
- (2) The data sharing agreement that covers the project must require the service to be performed by one of the following:
  - (a) the data custodian of the data, if the data custodian is not an ADSP but is satisfied that it has the appropriate skills and experience to perform the service;
  - (b) the data custodian of the data, if the data custodian is an ADSP able to perform such a service consistently with its conditions of accreditation;
  - (c) an ADSP able to perform such a service consistently with its conditions of accreditation.
- (3) A **de-identification data service** is 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.

## Section 16D

---

- (4) A **secure access data service** is:
- (a) the service of providing ADSP-controlled access; or
  - (b) any other service that enables an entity to access data under the control of another entity and that includes controls to prevent or minimise the risk of the data being misused.

### 16D Project involving complex data integration services

- (1) The requirement in subsection (2) applies if:
- (a) the data sharing purpose of the project is informing government policy and programs or research and development; and
  - (b) the project involves performing a complex data integration service (see subsection (3)); and
  - (c) a decision that subsection (4) applies to the service has not been made.
- (2) The data sharing agreement that covers the project must require the service to be performed by one of the following:
- (a) the data custodian of the data, if the data custodian is an ADSP able to perform such a service consistently with its conditions of accreditation;
  - (b) an ADSP able to perform such a service consistently with its conditions of accreditation.
- (3) A service to integrate data is a **complex data integration service** if:
- (a) 2 or more entities control the data being integrated; and
  - (b) the data is at the unit or micro level; and
  - (c) any of the following subparagraphs applies to any of the data to be integrated, or to the integrated data:
    - (i) the data includes personal information;
    - (ii) the data includes commercially sensitive information (including trade secrets) about the business, commercial, or financial affairs of an organisation;
    - (iii) the data includes information that is not publicly available about an industry or sector that forms part of the Australian economy;

Section 16D

---

- (iv) the data includes information about one or more persons or things the data custodian of the data considers to be vulnerable or sensitive;
    - (v) the data is to be used for more than one project;
    - (vi) the data meets conditions prescribed by the rules; and
  - (d) the data to be integrated, or the integrated data, has any of the characteristics prescribed by the rules (if any).
- (4) An individual covered by subsection (5) may decide that this subsection applies to the integration, if the individual is satisfied that, having regard to the following matters in relation to the data custodian's data and the other data proposed to be integrated, the risk that the integration could cause substantial harm is low:
- (a) the size of the data sets;
  - (b) whether the data relates to a significant proportion of the population of people or things to which the data relates;
  - (c) the detail of the individual records included in the data;
  - (d) how current the data is and whether it will be updated;
  - (e) the quality of the metadata and documentation for the data sets;
  - (f) whether entities that collected data to be integrated, or on whose behalf data to be integrated was collected, are aware of the proposed use of the data;
  - (g) if the data includes personal information—whether a person qualified to assess the ethics of the proposed use of the data has conducted such an assessment;
  - (h) whether the data custodian of the integrated data will control the technical environment in which the integrated data will be accessed;
  - (i) any other matters prescribed by the rules.
- (5) An individual is covered by this subsection if the individual is:
- (a) an authorised officer of a data custodian of data that is to be integrated; or
  - (b) an individual authorised under subsection 137(4) for the data custodian of data that is to be integrated.

## Section 16E

---

- (6) An individual who makes a decision that subsection (4) applies must make a written record of the decision and the reasons for the decision.

### 16E Privacy coverage condition

- (1) For the purposes of sections 13, 13A and 13B, the privacy coverage condition is met, in relation to an entity, if:
- (a) the entity is an APP entity; or
  - (b) the *Privacy Act 1988* applies to the entity, in relation to its collection and use of data as part of the project, as if the entity were an organisation within the meaning of that Act; or
  - (c) the entity is subject to an APP-equivalence term of the data sharing agreement in relation to its collection and use of data as part of the project; or
  - (d) a law of a State or Territory that provides for all of the following applies in relation to the entity's collection and use of data as part of the project:
    - (i) protection of personal information comparable to that provided by the Australian Privacy Principles;
    - (ii) monitoring of compliance with the law;
    - (iii) a means for an individual to seek recourse if the individual's personal information is dealt with in a way contrary to the law.
- (2) An **APP-equivalence term** is a term of a data sharing agreement prohibiting an entity from collecting or using personal information under the agreement in any way that would, if the entity were an organisation within the meaning of the *Privacy Act 1988*, breach an Australian Privacy Principle.
- (3) An act or practice engaged in by an entity that is an organisation referred to in paragraphs 7B(2)(a) and (b) of the *Privacy Act 1988* is not, despite subsection 7B(2) of that Act, **exempt** for the purposes of paragraph 7(1)(ee) of that Act if the act or practice is collecting or using personal information as part of a project.

Note: Paragraphs 7B(2)(a) and (b) of the *Privacy Act 1988* refer to an organisation that would be a small business operator if it were not a

## Section 16F

---

contracted service provider for a Commonwealth contract (within the meaning of the *Privacy Act 1988*).

- (4) Except as provided by subsection (3) and Part 3.3, nothing in this Act affects the operation of the *Privacy Act 1988* in relation to a data scheme entity that is an APP entity.

Note: Part 3.3 (data breach responsibilities) deals with the relationship between this Act and the requirements of Part IIIC of the *Privacy Act 1988* (notification of eligible data breaches).

### **16F Compliance with APP-equivalence term**

- (1) If an entity is subject to an APP-equivalence term of a data sharing agreement, an act or practice of the entity that contravenes the term in relation to an individual is taken to be:

- (a) an interference with the privacy of the individual for the purposes of the *Privacy Act 1988*; and
- (b) covered by sections 13 and 13G of that Act.

Note: An act or practice that is an interference with privacy may be the subject of a complaint under section 36 of the *Privacy Act 1988*.

- (2) The entity is taken, for the purposes of Part V of the *Privacy Act 1988* and any other provision of that Act that relates to that Part, to be an organisation (within the meaning of that Act) if:
- (a) an act or practice of the entity has contravened, or may have contravened, the APP-equivalence term in relation to an individual; and
  - (b) the act or practice is the subject of a complaint to, or an investigation by, the Information Commissioner under Part V of the *Privacy Act 1988*.
- (3) For the purposes of subsection (1), the reference in section 13G of the *Privacy Act 1988* to an entity includes a reference to any entity that is subject to an APP-equivalence term.
- (4) Paragraph 33C(1)(a) of the *Privacy Act 1988* applies in relation to an entity that is subject to an APP-equivalence term of a data sharing agreement as if the entity were an APP entity.

Section 16F

---

- (5) Sections 80V and 80W of the *Privacy Act 1988* apply in relation to an APP-equivalence term as if the term were a provision of that Act.



## Part 2.5—When sharing is barred

### 17 When sharing is barred

#### *When sharing is barred*

- (1) For the purposes of paragraph 13(2)(c), sharing data is barred if the sharing is barred by any of the following subsections.

Note: If a sharing of data is barred, it is not authorised by section 13.

#### *National security and law enforcement etc.*

- (2) Sharing data is barred if:
- (a) the data is held by, or originated with or was received from, an excluded entity; or
  - (b) the data is operational data that is held by, or originated with or was received from, any of the following:
    - (i) AUSTRAC (within the meaning of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*);
    - (ii) the Australian Federal Police;
    - (iii) the Department administered by the Minister administering the *Australian Border Force Act 2015*; or
  - (c) an excluded entity would be a data custodian of the data, if paragraph 11(2)(b) were disregarded.

#### *Contravention or infringement of rights etc.*

- (3) Sharing data is barred if:
- (a) sharing the data contravenes or infringes:
    - (i) copyright or other intellectual property rights to which the data is subject; or
    - (ii) a contract or agreement to which a data custodian of the data is party; or
    - (iii) a common law duty or privilege; or

## Section 17

---

- (iv) a privilege or immunity of a House of the Parliament, a member of a House of the Parliament, or a committee within the meaning of the *Parliamentary Privileges Act 1987*; or
- (b) the data is commercial information and sharing it founds an action by a person (other than the Commonwealth or a Commonwealth body) for breach of confidence.

### *Prescribed by the regulations*

- (4) Sharing data is barred if:
  - (a) any of the following prohibits the data custodian, or any of the individuals to whom the data custodian's authorisation would extend under section 124, from disclosing the data in the circumstances in which the sharing is done:
    - (i) a provision of a law prescribed by the regulations for the purposes of this subparagraph;
    - (ii) an order, direction, certificate or other instrument made by an officer of the Commonwealth (including a Minister) under a provision of a law prescribed by the regulations for the purposes of this subparagraph; or
  - (b) the data custodian of the data is prescribed by the regulations as an entity that must not share data in the capacity of data custodian; or
  - (c) any other circumstances prescribed by the regulations for the purposes of this paragraph exist.

### *International matters*

- (5) Sharing data is barred if:
  - (a) sharing the data is inconsistent with:
    - (i) the obligations of Australia under international law, including obligations under any international agreement binding on Australia; or
    - (ii) any law of the Commonwealth giving effect to such an agreement; or
  - (b) unless the foreign government, or agency of the foreign government, has agreed to the sharing—the data was

Section 17

---

collected from a foreign government, or an agency of a foreign government.

Note: The *Privacy Act 1988* and legislative instruments made under that Act are examples of laws of the Commonwealth giving effect to an international agreement binding on Australia (the International Covenant on Civil and Political Rights done at New York on 16 December 1966 ([1980] ATS 23)).

*Evidence and court/tribunal orders*

- (6) Sharing data is barred if:
- (a) the copy of the data to be shared is being held as evidence before a court; or
  - (b) the copy was obtained by a tribunal, authority or other person using a power to require the answering of questions or the production of documents and is being held as evidence before the tribunal, authority or other person; or
  - (c) the data:
    - (i) is subject to a court/tribunal order that manages, prohibits or restricts publication or other disclosure of the data; or
    - (ii) relates to the existence or content of such a court/tribunal order and a law of the Commonwealth prohibits or restricts disclosure of that existence or content.

Section 18

---

## Part 2.6—Data sharing agreements

### 18 Data sharing agreement

- (1) An agreement is a *data sharing agreement* if:
- (a) the agreement relates to the sharing of public sector data; and
  - (b) the parties to the agreement include a data custodian of public sector data and an accredited user; and
  - (c) the agreement is in the approved form (if any) or in writing (if there is no approved form); and
  - (d) any requirements specified in a data code are met in relation to the agreement.

Note 1: All data sharing agreements must also meet the requirements in section 19. Other provisions also impose requirements in certain circumstances (see for example sections 16B and 16C).

Note 2: Data scheme entities must also have regard to the guidelines (see section 27) in entering a data sharing agreement.

Note 3: Copies of data sharing agreements, including variations, must be given to the Commissioner (see section 33) for inclusion on the register of data sharing agreements under section 130. Certain details of the agreements must be made publicly available.

- (2) A data sharing agreement must not be entered into by an individual on behalf of a data scheme entity unless the individual is an authorised officer of the entity or authorised under subsection 137(4) for the entity.
- (3) A variation of a data sharing agreement must not be entered into by an individual on behalf of a data scheme entity unless the individual is an authorised officer of the entity or authorised under subsection 137(3) or (4) for the entity.
- (4) A data sharing agreement has no effect until the agreement is registered.
- (5) A variation of a data sharing agreement has no effect (and the agreement as in effect before the variation continues in effect) until the variation, or the agreement as varied, is registered.

---

Section 19

---

- (6) A data sharing agreement may deal with matters not required to be dealt with by this Act, but must not do so in a way that is inconsistent with the data sharing scheme.

**19 Requirements to be met by all data sharing agreements**

- (1A) The requirements in this section must be met by all data sharing agreements.

Note: There are other requirements that, depending on the nature of the project, must be met by some data sharing agreements. See sections 16A and 16B.

- (1) The parties to the agreement must be identified in the agreement.
- (2) The agreement must describe the project and specify that this Act applies to the project.
- (3) The agreement must specify:
- (a) the public sector data that the data custodian is to share (including any ADSP-enhanced data an ADSP is to share on behalf of the data custodian) (the *source data*); and
  - (b) the output of the project that the data custodian and accredited user agree is to be the final output.
- (4) The agreement must:
- (a) specify the data custodian of the source data; and
  - (b) if the agreement appoints a Commonwealth body as data custodian of output of the project in accordance with section 20F—specify the output and explain why the appointment has been made.
- Note: If the accredited user is a Commonwealth body, the agreement may appoint the accredited user as the Commonwealth body that is to be data custodian of the output.
- (5) The agreement must specify the title of any law that the sharing would contravene but for section 23 (authorisation to share overrides other laws).
- (6) The agreement must:
- (a) specify:

Section 19

---

- (i) the data sharing purpose, or data sharing purposes, of the project; and
    - (ii) if, under the agreement, the accredited user is to be allowed to use output of the project for any purpose incidental to that purpose or those purposes—any such incidental purpose; and
  - (b) except in relation to any use of the output allowed in accordance with section 20D—prohibit the accredited user from collecting and using output of the project for any of the following:
    - (i) any purpose not specified;
    - (ii) any precluded purpose.
- (6A) The agreement must prohibit the accredited user from creating output of the project, other than:
- (a) the final output; and
  - (b) output the creation of which is reasonably necessary or incidental to creation of the final output.
- (7) The agreement must specify how the project will be consistent with the data sharing principles, including by:
- (a) describing how the public interest is served by the project; and
  - (b) specifying the actions the party will take to give effect to the principles.
- (8) If the sharing is being done through an ADSP, the agreement must:
- (a) specify any data services the ADSP is to perform in relation to public sector data shared with the ADSP by the data custodian; and
  - (b) specify the circumstances in which the ADSP is to share, with the accredited user on behalf of the data custodian, ADSP-enhanced data of the project; and
  - (c) prohibit the ADSP from providing access to, or releasing, the ADSP-enhanced data in any other circumstances other than circumstances (if any) specified in the agreement.

Section 19

---

- (8A) For the purposes of paragraph (8)(c), the only other circumstances that may be specified in the agreement are those allowed by section 20A.
- (9) The agreement must:
  - (a) describe in general terms the use to be made by the accredited user of the output of the project; and
  - (b) prohibit the accredited user from using the output in a way that is inconsistent with the description; and
  - (c) prohibit the accredited user from providing access to, or releasing, the output in any circumstances other than circumstances (if any) specified in the agreement.
- (10) For the purposes of paragraph (9)(c), the only circumstances that may be specified in the agreement are those allowed by section 20A, 20B, 20C or 20D.
- (11) The agreement must prohibit the accredited entities that are party to the agreement from doing anything inconsistent with the conditions of accreditation imposed on or applicable to the entity from time to time.
- (12) If section 37 applies in relation to sharing under the agreement and the agreement does not provide that subsections 37(2) and (3) are not to apply, the agreement must specify that those subsections apply.
- (12A) If the parties agree to responsibilities in relation to data breaches additional to those under Part 3.3, the agreement must set out those responsibilities.
- (13) The agreement must specify the circumstances in which it may be varied or terminated and how a variation or termination is to be done.
- (14) The agreement must specify either or both of the following:
  - (a) its duration;
  - (b) the intervals at which the parties must review it.
- (15) The agreement must provide for how scheme data covered by the agreement is to be dealt with when the agreement ends.

Section 19

---

- (16) The agreement must meet any other requirements prescribed by a data code for the purposes of this subsection.
- (17) The agreement must require the data custodian of the source data to give the Commissioner written notice of the cessation of the agreement, as soon as practicable after the agreement ceases to be in effect.



## **Part 2.7—Allowed access to output of project**

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

- (1) The data sharing agreement may allow the ADSP to provide access to specified ADSP-enhanced data of the project under the agreement to the data custodian of the source data, for the purpose of the data custodian ensuring that the ADSP-enhanced data is as agreed.
- (2) The data sharing agreement may allow the accredited user to provide access to specified output of the project under the agreement to the data custodian of the source data, for the purpose of the data custodian ensuring that the output is as agreed.
- (3) If the ADSP or accredited user provides access to data that is ADSP-enhanced data or output in accordance with subsection (1) or (2), the ADSP or accredited user *submits* the data.
- (4) Providing access to output or ADSP-enhanced data as allowed by this section is taken to be for the data sharing purpose, or data sharing purposes, of the project.

### **20B Allowed access: providing access to output for validation or correction**

- (1) The data sharing agreement may allow the accredited user to provide another entity with access to specified output of the project, if the agreement:
  - (a) allows the access to be provided to:
    - (i) an entity that carries on a business, or is a not-for-profit entity, to which the output relates, for the purpose of validating or correcting the output; or
    - (ii) an individual to whom the output relates, or a responsible person (within the meaning of the *Privacy Act 1988*) for such an individual, for the purpose of validating or correcting the output; or

## Section 20C

---

- (iii) another person in circumstances prescribed by the rules that relate to validating or correcting the output; and
  - (b) requires the data custodian of the source data to be satisfied, before access is provided, that the access will be an authorised use of the output under section 13A.
- (2) If data exits the data sharing scheme under subsection 20E(2) as a result of the accredited user providing an entity, individual or other person with access to the data as allowed by subsection (1), the accredited user is taken to have collected a copy of the data from the entity, individual or person concerned, at the time the entity, individual or person validates or corrects the data.
- (3) Providing access to output in accordance with a term of a data sharing agreement allowed by this section is taken to be for the data sharing purpose, or data sharing purposes, of the project.

### **20C Allowed access: providing access to or releasing output in other circumstances**

- (1) The data sharing agreement may allow the accredited user to provide another entity with access to, or to release, specified output of the project, if the agreement:
  - (a) allows the provision of access, or release, in specified circumstances that do not contravene any other law of the Commonwealth or a law of a State or Territory (disregarding section 23 of this Act); and
  - (b) if the output includes personal information about an individual—prohibits provision of access or release unless the individual consents; and
  - (c) requires the data custodian of the source data to be satisfied, before the access is provided or the release occurs, that the access or release will be an authorised use of the output under section 13A.
- (2) Providing access to output in accordance with a term of a data sharing agreement allowed by this section is taken to be for the data sharing purpose, or data sharing purposes, of the project.

## **20D Allowed access: sharing under section 13**

The data sharing agreement may allow the accredited user to share output of the project under section 13, if:

- (a) the accredited user is appointed as the data custodian of the output in accordance with subsection 20F(2); and
- (b) the agreement requires the data custodian of the source data to be satisfied, before the sharing occurs, that the sharing will be an authorised use of the output under section 13A.

## **20E Exit of ADSP-enhanced data or output of project**

### *Overview of this section*

- (1) If the user or intermediary in a project uses output, or ADSP-enhanced data, of the project in ways other than those authorised by this Act, it is a defence to an offence under section 14A if the copy being used has exited the data sharing scheme under this section (see subsection 14A(6)).

### *Exit on provision of authorised or required access*

- (2) If a person obtains a copy of output of the project as a result of the user providing the person with access to the output, the copy *exits* the data sharing scheme at the time it is collected by the person, as long as the user's provision of access is:
  - (a) a use of the output authorised by section 13A or 135 or required by a direction under section 112; and
  - (b) not a submission of the output; and
  - (c) not a sharing of data under section 13 allowed as mentioned in section 20D.

Note: See the definition of *submit* in subsection 20A(3).

- (3) If a person obtains a copy of ADSP-enhanced data of the project as a result of the intermediary providing the person with access to the ADSP-enhanced data, the copy *exits* the data sharing scheme at the time it is collected by the person, as long as the intermediary's provision of access is:
  - (a) required by a direction under section 112; or

Section 20E

---

(b) authorised by section 135.

*Exit on collection etc. if sharing is for purpose of delivery of government services*

- (4) A copy of output of the project held by the user ***exits*** the data sharing scheme at the time applicable under subsection (5) if:
- (a) the data is personal information about an individual; and
  - (b) the data sharing purpose of the project is delivery of government services; and
  - (c) before the data was shared with the accredited user, the individual expressly consented to their personal information:
    - (i) being shared by the data custodian with the accredited user; and
    - (ii) being used by the accredited user without the requirements of this Act applying to the use.
- (5) For the purposes of subsection (4), the applicable time is:
- (a) the time the user collected the copy of the shared data; or
  - (b) if the individual's consent as mentioned in paragraph (4)(c) specified a later time—that later time.
- (6) The user is taken to collect a copy of data that exits the data sharing scheme under subsection (4) from the individual concerned, at the time the data exits.

*Exit for accredited user that is appointed data custodian of output*

- (7) The user in a project is taken to hold a copy of output of the project that has ***exited*** the data sharing scheme, from the time specified for exit of the output in the data sharing agreement that covers the project, if:
- (a) the agreement appoints the user as data custodian of the output under subsection 20F(2); and
  - (b) subparagraph 20F(2)(c)(i) does not apply; and
  - (c) the conditions in subsection 20F(3) for exit of the output are met.

---

Section 20F

---

**20F Data custodian of output of project**

- (1) An entity appointed as the data custodian of output of a project in accordance with subsection (2) or (5) becomes the data custodian of the output:
  - (a) if subparagraph (2)(c)(i) applies—at the time the output is created; or
  - (b) if subparagraph (2)(c)(ii) applies—at the time the output exits the data sharing scheme under subsection 20E(7); or
  - (c) if subsection (5) applies—at the time the entity is provided with access to the output in accordance with section 13A.
- (2) A data sharing agreement that covers a project may appoint the user in the project as the data custodian of specified output of the project, if:
  - (a) the user is a Commonwealth body; and
  - (b) the output is public sector data and not a copy of the shared data collected by the user; and
  - (c) either:
    - (i) the agreement allows the user to provide access to the data in circumstances allowed by section 20C or 20D; or
    - (ii) if subparagraph (i) does not apply—the conditions in subsection (3) for exit of the output are met.
- (3) The conditions for exit of the output are that:
  - (a) provision of access to, or release of, the output by the user would not contravene any other law of the Commonwealth or a law of a State or Territory (disregarding section 23 of this Act); and
  - (b) if the output includes personal information about an individual—the individual has expressly consented to their personal information being used by the user without the requirements of this Act applying to the use; and
  - (c) the agreement requires the data custodian of the source data to be satisfied that all requirements in the agreement relating to exit of the output are met before the time specified in the agreement for the exit.

Section 20F

---

- (4) Unless appointed as mentioned in subsection (2), the user in the project is not the data custodian of output of the project. This subsection has effect despite subparagraph 11(2)(c)(i).
- (5) A data sharing agreement that covers a project may appoint an entity that is party to the agreement, other than in the capacity of user, as the data custodian of specified output of the project, if:
  - (a) the entity is a Commonwealth body; and
  - (b) the entity is not an excluded entity; and
  - (c) the output is public sector data and not a copy of the shared data collected by the user; and
  - (d) the agreement allows the user to provide the entity with access to the output in circumstances allowed by section 20C.

## **Part 2.8—Relationship with other laws**

### **22 Other authorisations for data custodians not limited**

The authorisation in section 13 for a data custodian to share particular data does not limit any other law of the Commonwealth or a State or Territory that authorises the data custodian to share or disclose the data.

### **23 Authorisations override other laws**

- (1) The authorisations in sections 13, 13A, 13B and 13C have effect despite anything in another law of the Commonwealth, or a law of a State or Territory.

Note: These authorisations extend to individuals (see section 124).

- (2) Subsection (1) applies in relation to a law enacted before or after the commencement of this Act.

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

### **Part 3.1—Introduction**

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

The responsibilities imposed on data scheme entities are mainly set out in this Chapter, although some important responsibilities are set out elsewhere (see especially sections 14 and 14A in Chapter 2).

Civil penalties apply in some cases if responsibilities in this Chapter are not met. In any case, the responsibilities may be enforced by use of the Commissioner’s other regulatory powers under Part 5.5.



## **Part 3.2—General responsibilities**

### **25 No duty to share but reasons required for not sharing**

- (1) This Act does not require, or authorise any person to require, a data custodian to share public sector data.
- (2) However, a data custodian of public sector data must, within a reasonable period, consider a request for it to share the data, if the request is made:
  - (a) by an accredited user; and
  - (b) in the approved form (if any) or in writing (if there is no approved form).
- (3) The data custodian may refuse the request for any reason (including that the request is unreasonable), but must give the accredited user written notice of the reasons no later than 28 days after the day the decision to refuse is made.

### **26 Comply with rules and data codes**

A data scheme entity must comply with:

- (a) the rules; and
- (b) data codes.

### **27 Have regard to guidelines**

Data scheme entities must have regard to the guidelines when engaging in conduct for the purposes of this Act.

### **30 Comply with conditions of accreditation**

An accredited entity must comply with the conditions of the entity's accreditation.

Civil penalty:        300 penalty units.

## Section 31

---

### **31 Report events and changes in circumstances affecting accreditation to Commissioner**

- (1) An accredited entity must give the Commissioner written notice, in the approved form (if any) of any event, or change in circumstance, relevant to either of the following:
- (a) the exercise of the Commissioner's regulatory functions or the Minister's functions as the accreditation authority for the entity;
  - (b) the entity's accreditation or conditions of accreditation.

Civil penalty: 300 penalty units.

- (2) Subsection (1) does not apply in relation to an event or change in circumstances prescribed by the rules for the purposes of this subsection.

### **32 Not provide false or misleading information**

- (1) A data scheme entity must not, in giving information or a document in compliance or purported compliance with this Act, the rules or a data code, give the Minister or Commissioner:
- (a) information or a document that is false or misleading; or
  - (b) information that omits any matter or thing without which the information is false or misleading.

Note: A data scheme entity that contravenes this subsection might also commit an offence under Division 136 or 137 of the *Criminal Code*.

Civil penalty: 300 penalty units.

- (2) A data scheme entity must not, in giving information or a document for the purposes of entering into or giving effect to a data sharing agreement, give another data scheme entity:
- (a) information or a document that is false or misleading; or
  - (b) information that omits any matter or thing without which the information is false or misleading.

Civil penalty: 300 penalty units.

### **33 Registration of data sharing agreements**

- (1) If an entity is party to a data sharing agreement in the capacity of data custodian, the entity must give the Commissioner, in the approved form (if any):
  - (a) an electronic copy of the agreement; and
  - (b) if the agreement is varied—an electronic copy of the variation, or the agreement as varied;no later than 30 days after the day the agreement or variation is made.
- (2) The entity must also give the Commissioner any other information or documents required by a data code to be given to the Commissioner at the time the entity gives the Commissioner a document mentioned in subsection (1).

### **34 Assist Commissioner in relation to annual report**

- (1) A data custodian must, within the period applicable under subsection (5) after the end of a financial year, notify the Commissioner, in the approved form (if any), of the following in relation to the financial year:
  - (a) whether it received requests from accredited users to share data under this Act;
  - (b) if it received any such requests—the number of requests and the reasons it agreed to or refused them;
  - (c) if it refused any such requests—the number of requests that were refused where reasons for the refusal were not given within the time required by subsection 25(3);
  - (d) whether it received complaints relating to the data sharing scheme or its conduct in relation to it, and if it did, the number of complaints and information about the subject matter of the complaints;
  - (e) whether it entered into any data sharing agreements and if it did, the number entered into.
- (2) A data custodian must give the Commissioner any other information and assistance the Commissioner reasonably requires

## Section 34

---

in relation to the preparation of the annual report mentioned in section 138.

- (3) An entity that was an accredited entity at any time during a financial year must give the Commissioner any information and assistance the Commissioner reasonably requires in relation to the preparation of the annual report for the financial year mentioned in section 138.
- (4) The period for notifying the Commissioner is:
  - (a) the period applicable under a data code; or
  - (b) if there is no period applicable under a data code—as soon as practicable.

## Part 3.3—Data breach responsibilities

### 35 Definition of *data breach*

If:

- (a) a data scheme entity holds scheme data; and
- (b) any of the following apply:
  - (i) there is unauthorised access to or disclosure of the data;
  - (ii) the data is lost in circumstances where there is likely to be unauthorised access to or disclosure of the data;
  - (iii) an event prescribed by a data code occurs in relation to the data;

the access, disclosure, loss or event is a ***data breach*** of the data scheme entity.

### 36 Take steps to mitigate data breach

- (1) If a data scheme entity reasonably suspects or becomes aware that a data breach of the entity has occurred, the entity must, within the period applicable under subsection (3), take reasonable steps 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.

Civil penalty:            300 penalty units.

- (2) If:

- (a) a data custodian reasonably suspects or becomes aware that a data breach of an accredited entity has occurred; and
- (b) the data breach involves scheme data that is output, or ADSP-enhanced data, of a project in which the data custodian shared public sector data with or through the accredited entity;

the data custodian must, within the period applicable under subsection (3), take reasonable steps 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.

## Section 37

---

Civil penalty: 300 penalty units.

- (3) The period for taking the steps is:
- (a) the period applicable under a data code; or
  - (b) if there is no period applicable under a data code—as soon as practicable after the breach occurs.

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

#### *Scope*

- (1) This section applies if:
- (a) a data custodian of public sector data that is personal information about one or more individuals has shared the personal information with or through an accredited entity under section 13; and
  - (b) the accredited entity holds the personal information.

#### *Deemed holding of personal information by data custodian*

- (2) Part IIIC of the *Privacy Act 1988* (notification of eligible data breaches) has effect as if:
- (a) the personal information were held by the data custodian; and
  - (b) the data custodian were required under section 15 of that Act not to do an act, or engage in a practice, that breaches Australian Privacy Principle 11.1 in relation to the personal information.

Note: This has the effect that the data custodian has responsibilities under Part IIIC of the *Privacy Act 1988* (notification of eligible data breaches) in relation to the personal information held by the accredited entity.

- (3) If the accredited entity reasonably suspects or becomes aware that a data breach of the entity has occurred (within the meaning of section 35), the accredited entity must give the data custodian written notice of the suspected or actual data breach:
- (a) in sufficient time; and
  - (b) containing sufficient detail;

Section 37

---

to enable the data custodian to comply with its obligations under Part IIIC of the *Privacy Act 1988* as that Part applies because of subsection (2) of this section.

- (4) Subsections (2) and (3) do not apply if:
- (a) the accredited entity is an APP entity that is required under section 15 of the *Privacy Act 1988* not to do an act, or engage in a practice, that breaches Australian Privacy Principle 11.1 in relation to the personal information; and
  - (b) the data sharing agreement under which the personal information was shared with the entity provides that subsections (2) and (3) are not to apply in relation to the personal information.

Note: This has the effect that only the entity with which the personal information was shared, and not the data custodian, has responsibilities under Part IIIC of the *Privacy Act 1988* (notification of eligible data breaches) in relation to the personal information held by the entity.

*Copy of eligible data breach statements given to Information Commissioner*

- (5) A data scheme entity must, as soon as practicable, give the National Data Commissioner a copy of any statement the entity is required to give the Information Commissioner under section 26WK of the *Privacy Act 1988* (statement about eligible data breach), if the eligible data breach to which the statement relates involves scheme data.
- (5A) The Information Commissioner may give the National Data Commissioner a copy of any statement given to the Commissioner under section 26WK of the *Privacy Act 1988*, if the Information Commissioner is satisfied that the matters dealt with in the statement are relevant to the National Data Commissioner's functions.

*Meaning of hold*

- (6) A reference in this section to an entity holding personal information is a reference to the entity holding the information within the meaning of the *Privacy Act 1988*.

## Section 38

---

### **38 Notify Commissioner of non-personal data breach**

- (1) A data scheme entity must notify the Commissioner, in an approved form (if any), within the period applicable under subsection (1A) and in accordance with any requirements prescribed by a data code, if:
- (a) the entity reasonably suspects or becomes aware that a data breach of the entity has occurred; and
  - (b) data involved in the breach is not personal information about one or more individuals.

Note: Breaches involving personal information are dealt with under Part IIIC of the *Privacy Act 1988* (see section 37).

Civil penalty: 300 penalty units.

- (1A) The period for notifying the Commissioner is:
- (a) the period applicable under a data code; or
  - (b) if there is no period applicable under a data code—as soon as practicable after the end of the financial year in which the breach occurs.
- (2) A data code may prescribe different periods for the purposes of paragraph (1A)(a), according to whether the breach is, or is not, a breach that a reasonable person would conclude would be likely to result in serious harm to an entity, a group of entities or a thing to which the data relates.
- (3) In determining whether a reasonable person would conclude that the breach would, or would not, be likely to result in serious harm to an entity, a group of entities or a thing to which the data involved in the breach relates, have regard to the following:
- (a) the kind or kinds of data;
  - (b) the sensitivity of the data;
  - (c) whether the data is protected by one or more security measures and, if so, the nature of those measures;
  - (d) the persons, or the kinds of persons, who have obtained, or who could obtain, the data;
  - (e) the nature of the harm;
  - (f) any other relevant matters.



## **Chapter 4—National Data Commissioner and National Data Advisory Council**

### **Part 4.1—Introduction**

#### **39 Simplified outline of this Chapter**

There is to be a National Data Commissioner.

The Commissioner is the regulator for the data sharing scheme, and provides advice and guidance about it. The Commissioner also has the function of regulating and enforcing the scheme, which includes dealing with complaints that data scheme entities make about each other, and other complaints relating to the scheme's administration or operation.

In addition, the Commissioner's functions include educating and supporting Commonwealth bodies more generally in relation to sharing and safely handling public sector data.

The Commissioner is assisted in the performance of these functions by APS employees in the Department who are made available by the Secretary. The Commissioner may also engage contractors and consultants.

The Commissioner is also assisted by the advice of the National Data Advisory Council.

The constitutional basis for the roles of the Commissioner and Council is set out in subsections 42(2) and 61(2).

#### **40 Commissioner to have regard to objects of Act**

In performing functions, the Commissioner must have regard to the objects of this Act (see section 3).

## **Part 4.2—National Data Commissioner**

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

#### **41 National Data Commissioner**

There is to be a National Data Commissioner.

#### **42 Functions**

- (1) The Commissioner has the following functions:
  - (a) the advice related functions set out in section 43;
  - (b) the guidance related functions set out in section 44;
  - (c) the regulatory functions set out in section 45;
  - (d) the education related functions set out in section 45A;
  - (e) any other functions conferred on the Commissioner by this Act or an instrument under this Act or by any other law of the Commonwealth;
  - (f) to do anything incidental or conducive to the performance of any of the above functions.
- (2) The Commissioner may perform the Commissioner's functions only with respect to the following:
  - (a) sharing of data under, or purportedly under, section 13 and the collection and use of data in relation to such sharing;
  - (b) matters incidental to the execution of any of the legislative powers of the Parliament or the executive power of the Commonwealth.

#### **43 Advice related functions**

For the purposes of paragraph 42(1)(a), the Commissioner's advice related functions are to do the following, on request by the Minister or on the Commissioner's own initiative:

- (a) advise on matters relating to the operation of this Act, including Commonwealth laws and changes to Commonwealth laws relating to this Act;

- (aa) advise a data scheme entity about how, in the Commissioner's opinion, the data sharing scheme applies, or would apply in particular circumstances, in relation to the entity;
- (ab) advise the Minister in relation to the exercise of the Minister's powers under Part 5.2 (accreditation framework);
- (b) inform the Minister about actions to be taken by data scheme entities in order to comply with this Act;
- (c) report and make recommendations to the Minister in relation to this Act, or the need for or desirability of legislative or administrative action in relation to this Act.

#### **44 Guidance related functions**

For the purposes of paragraph 42(1)(b), the Commissioner's guidance related functions are to make:

- (a) data codes under section 126; and
- (b) guidelines under section 127.

#### **45 Regulatory functions**

- (1) For the purposes of paragraph 42(1)(c), the Commissioner's regulatory functions are to regulate and enforce the data sharing scheme by performing the functions and exercising the powers conferred by Chapter 5 (regulation and enforcement), and the Regulatory Powers Act as it applies in relation to this Act.

Note: The Commissioner and members of staff mentioned in section 47 cannot participate in sharing under this Act (see subsection 17(8)).

- (2) A person assisting the Commissioner in the performance of any of the Commissioner's regulatory functions must be a person who, in the Commissioner's opinion, has the skills, qualifications or experience necessary to assist the Commissioner to perform that regulatory function.

#### **45A Education and support related functions**

For the purposes of paragraph 42(1)(d), the Commissioner's education and support related functions are the following:

---

## Section 46

---

- (a) to foster best practice by data custodians when responding to requests to share, and sharing, public sector data;
- (b) to foster safe data handling practices by Commonwealth bodies;
- (c) to make available to Commonwealth bodies information, educational material and support relating to using public sector data and providing other entities with access to it in a controlled manner.

### **46 Application of finance law**

For the purposes of the finance law (within the meaning of the *Public Governance, Performance and Accountability Act 2013*), the Commissioner is an official of the Department.

### **47 Staff**

- (1) The Secretary of the Department must:
  - (a) make available to the Commissioner APS employees in the Department who, in the Commissioner's opinion, have the skills, qualifications or experience necessary to assist the Commissioner to perform the Commissioner's functions and exercise the Commissioner's powers; and
  - (b) do so to the extent the Commissioner reasonably requires.
- (2) An APS employee made available to assist the Commissioner is subject to the directions of the Commissioner in relation to that assistance. The APS employee remains subject to the directions of the Secretary in relation to other matters.

### **48 Contractors**

The Commissioner may, on behalf of the Commonwealth, engage persons under a written agreement to assist the Commissioner to perform or exercise the functions or powers of the Commissioner.

## **49 Consultants**

The Commissioner may, on behalf of the Commonwealth, engage consultants to advise in relation to the performance of the Commissioner's functions.

## **50 Delegation by Commissioner**

- (1) The Commissioner may, in writing, delegate to a member of the staff mentioned in section 47 any or all of the Commissioner's functions or powers under:
  - (a) this Act; or
  - (b) the rules; or
  - (c) the Regulatory Powers Act as it applies in relation to this Act.

Note: Sections 34AA to 34A of the *Acts Interpretation Act 1901* contain provisions relating to delegations.

- (2) Despite subsection (1), the Commissioner must not delegate:
  - (a) functions or powers under the following provisions:
    - (i) section 112 (directions);
    - (ii) section 126 (data codes);
    - (iii) section 127 (guidelines); or
  - (b) a regulatory function, or a power in relation to a regulatory function, 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; or
  - (c) functions or powers under Part 4.3 (National Data Advisory Council).
- (3) In performing functions or exercising powers under the delegation, the delegate must comply with any written directions of the Commissioner.
- (4) If the Commissioner delegates functions or powers under this section, the Commissioner must make publicly available information about the persons or class of persons to whom the functions or powers are delegated.

Section 51

---

**51 Independence of Commissioner**

Subject to this Act and other laws of the Commonwealth, the Commissioner has discretion in the performance or exercise of the Commissioner's functions or powers and is not subject to direction by any person in relation to the performance or exercise of those functions or powers.

**52 Commissioner not to be sued**

The Commissioner, and any person acting under the direction or authority of the Commissioner, is not liable to an action, suit or proceeding in relation to an act done or omitted to be done in good faith in the performance or purported performance, or exercise or purported exercise, of a function or power conferred by this Act, the rules or a data code.

## **Division 2—Terms and conditions etc.**

### **53 Appointment**

- (1) The Commissioner is to be appointed by the Governor-General by written instrument.

Note: The Commissioner may be reappointed: see section 33AA of the *Acts Interpretation Act 1901*.

- (2) A person may be appointed as the Commissioner only if the person has appropriate qualifications, skills or experience to perform the functions of the position.

### **54 General terms and conditions of appointment**

- (1) The Commissioner holds office for the period specified in the instrument of appointment. The period must not exceed 5 years.
- (2) The Commissioner holds office on a full-time basis.
- (3) The Commissioner holds office on the terms and conditions (if any), in relation to matters not covered by this Act, that are determined by the Governor-General.

### **55 Other paid work**

The Commissioner must not engage in paid work outside the duties of the office without the Minister's approval.

### **56 Remuneration**

- (1) The Commissioner is to be paid the remuneration that is determined by the Remuneration Tribunal. If no determination of that remuneration by the Tribunal is in operation, the Commissioner is to be paid the remuneration that is prescribed by the rules.
- (2) The Commissioner is to be paid the allowances that are prescribed by the rules.

## Section 57

---

- (3) This section has effect subject to the *Remuneration Tribunal Act 1973*.

### **57 Leave of absence**

- (1) The Commissioner has the recreation leave entitlements that are determined by the Remuneration Tribunal.
- (2) The Minister may grant the Commissioner leave of absence, other than recreation leave, on the terms and conditions as to remuneration or otherwise that the Minister determines.

### **58 Resignation**

- (1) The Commissioner may resign the Commissioner's appointment by giving the Governor-General a written resignation.
- (2) The resignation takes effect on the day it is received by the Governor-General or, if a later day is specified in the resignation, on that later day.

### **58A Disclosure of interests to Minister**

The Commissioner must give written notice to the Minister of any interests, pecuniary or otherwise, that the Commissioner has or acquires and that conflict or could conflict with the proper performance of the Commissioner's functions.

Note: See also section 67 in relation to disclosure obligations in connection with the Commissioner's role on the National Data Advisory Council.

### **59 Termination of appointment**

The Governor-General may terminate the appointment of the Commissioner:

- (a) for misbehaviour; or
- (b) if the Commissioner is unable to perform the duties of the office because of physical or mental incapacity; or
- (c) if the Commissioner:
- (i) becomes bankrupt; or



- (ii) applies to take the benefit of any law for the relief of bankrupt or insolvent debtors; or
- (iii) compounds with the Commissioner's creditors; or
- (iv) makes an assignment of the Commissioner's remuneration for the benefit of the Commissioner's creditors; or
- (d) if the Commissioner is absent, except on leave of absence, for 14 consecutive days or for 28 days in any 12 months; or
- (e) if the Commissioner fails, without reasonable excuse, to comply with:
  - (i) section 58A (disclosure of interests to Minister); or
  - (ii) section 67 (disclosure of interests to Minister or Commissioner); or
  - (iii) section 29 of the *Public Governance, Performance and Accountability Act 2013* (which deals with the duty to disclose interests) or rules made for the purposes of that section; or
- (f) if the Commissioner engages, except with the Minister's approval, in paid work outside the duties of the office (see section 55).

## 60 Acting appointments

- (1) The Minister may, by written instrument, appoint a person to act as the Commissioner:
  - (a) during a vacancy in the office of the Commissioner (whether or not an appointment has previously been made to the office); or
  - (b) during any period, or during all periods, when the Commissioner:
    - (i) is absent from duty or from Australia; or
    - (ii) is, for any reason, unable to perform the duties of the office.

Note: For rules that apply to acting appointments, see sections 33AB and 33A of the *Acts Interpretation Act 1901*.

- (2) A person must not be appointed to act as the Commissioner unless the person has appropriate qualifications, skills or experience, as

Section 60

---

mentioned in subsection 53(2), to be appointed as the Commissioner.

## Part 4.3—National Data Advisory Council

### 61 Establishment and function of Council

- (1) The National Data Advisory Council is established by this section, and has the function of advising the Commissioner on the following matters relating to use of public sector data and provision of access to it in a controlled manner:
  - (a) ethics;
  - (b) balancing data availability with privacy protection;
  - (c) trust and transparency;
  - (d) technical best practice;
  - (e) industry and international developments;
  - (f) any other matters.
- (2) The Council may perform the Council's functions only with respect to the following:
  - (a) sharing of data under, or purportedly under, section 13 and the use of data in relation to such sharing;
  - (b) matters incidental to the execution of any of the legislative powers of the Parliament or the executive power of the Commonwealth.

### 62 Membership of Council

#### *Membership*

- (1) The Council consists of the following members:
  - (a) the Commissioner;
  - (b) the Australian Statistician;
  - (c) the Information Commissioner;
  - (d) the Chief Scientist;
  - (e) at least 5, and no more than 8, other members appointed by the Commissioner (the ***appointed members***).

## Section 63

---

### *Chair*

- (2) The Commissioner may:
  - (a) designate himself or herself as the Chair of the Council; or
  - (b) by written instrument, designate an appointed member to be the Chair for the period specified in the instrument.
- (3) At any time when a Chair is not designated under subsection (2), the Council may, by written instrument, designate a Chair itself from among the appointed members for the period specified in the instrument.
- (4) A Chair may be designated or appointed for a maximum period of 3 years, but may be designated again or appointed again.

## **63 Appointment of members**

- (1) The appointed members are to be appointed by the Commissioner by written instrument, on a part-time basis.
- (2) The Commissioner must ensure that appointed members are persons with qualifications, skills or experience that will help the Council perform its function.

## **64 Term of appointment**

An appointed member holds office for the period specified in the instrument of appointment. The period must not exceed 3 years.

## **65 Remuneration and allowances**

- (1) An appointed member is to be paid the remuneration that is determined by the Remuneration Tribunal. If no determination of that remuneration by the Tribunal is in operation, the member is to be paid the remuneration that is prescribed by the rules.
- (2) An appointed member is to be paid the allowances as are prescribed by the rules.
- (3) This section has effect subject to the *Remuneration Tribunal Act 1973*.

## **66 Leave of absence**

The Commissioner may grant leave of absence to an appointed member on the terms and conditions that the Commissioner determines.

## **67 Disclosure of interests to Minister or Commissioner**

- (1) The Commissioner must give written notice to the Minister of all interests, pecuniary or otherwise, that the Commissioner has or acquires and that conflict or could conflict with the proper performance of the Commissioner's role as a member of the Council.
- (2) A member of the Council other than the Commissioner must give written notice to the Commissioner of all 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.

## **68 Disclosure of interests to Council**

- (1) A member of the Council who has an interest, pecuniary or otherwise, in a matter being considered or about to be considered by the Council must disclose the nature of the interest to a meeting of the Council.
- (2) The disclosure must be made as soon as possible after the relevant facts have come to the member's knowledge.
- (3) The disclosure must be recorded in the minutes of the meeting.

## **69 Resignation of members**

- (1) An appointed member may resign as a member by giving the Commissioner a written resignation.
- (2) The resignation takes effect on the day it is received by the Commissioner or, if a later day is specified in the resignation, on that later day.

## Section 70

---

### **70 Termination of appointment of members**

The Commissioner may terminate the appointment of an appointed member:

- (a) for misbehaviour; or
- (b) if the member is unable to perform the duties of office because of physical or mental incapacity; or
- (c) if the member:
  - (i) becomes bankrupt; or
  - (ii) applies to take the benefit of any law for the relief of bankrupt or insolvent debtors; or
  - (iii) compounds with the member's creditors; or
  - (iv) makes an assignment of the member's remuneration for the benefit of the member's creditors; or
- (d) if the member is repeatedly absent, except on leave of absence; or
- (da) if the member fails, without reasonable excuse, to comply with section 67 (disclosure of interests to Minister or Commissioner); or
- (e) if the member's qualifications, skills or experience are no longer relevant to the Council function or the member has ceased to hold a professional role that was relevant to the member's appointment.

### **71 Other terms and conditions of members**

An appointed member holds office on the terms and conditions (if any), in relation to matters not covered by this Act, that are determined by the Commissioner.

### **72 Procedures**

- (1) The Council is to hold any meetings necessary for the performance of its functions, and must meet at least twice every calendar year.
- (2) Meetings of the Council may be convened by the Commissioner or by the Chair.

Section 72

---

- (3) Except as mentioned above, the Council is to determine its own procedures.

## **Chapter 5—Regulation and enforcement**

### **Part 5.1—Introduction**

#### **73 Simplified outline of this Chapter**

The Minister and the Commissioner may accredit entities, impose and vary conditions of accreditation, and suspend or cancel accreditation, in accordance with the accreditation framework.

If a data scheme entity breaches this Act or a data sharing agreement, another data scheme entity may complain to the Commissioner. A complaint will ordinarily result in an investigation by the Commissioner, which may in turn lead to enforcement action being taken by the Commissioner against the breaching data scheme entity.

The Commissioner may also conduct assessments from time to time to ensure data scheme entities are operating in accordance with the Act. If the Commissioner reasonably suspects a data scheme entity has breached the Act or a data sharing agreement, the Commissioner may investigate the entity regardless of whether a complaint has been made.

The Minister may also direct the Commissioner to investigate a data scheme entity.

The Commissioner has power to require persons to give information, and has monitoring and investigation powers in relation to certain provisions of this Act. The Commissioner may transfer matters to a more appropriate agency, which could include the police if an offence is involved.

There are a range of enforcement options available to the Commissioner, as follows:

- (a) making recommendations to a data scheme entity;
- (b) giving directions in specified circumstances;



Section 73

---

- (c) issuing an infringement notice, or applying to a court for a pecuniary penalty order, if a data scheme entity contravenes a civil penalty provision;
- (d) accepting an enforceable undertaking in relation to any aspect of this Act;
- (e) applying to a court for an injunction if a data scheme entity has contravened, or is contravening or proposing to contravene, a civil penalty provision or a provision of Chapter 3 (responsibilities of data scheme entities).

The provisions continue to apply in relation to former data scheme entities as set out in the Chapter.

## Part 5.2—Accreditation framework

### Division 1—Accreditation

#### 74 Accreditation

- (1) If an entity applies for accreditation as an ADSP or an accredited user under section 76, the accreditation authority for the entity may grant the entity the accreditation applied for if:
    - (a) the entity is an Australian entity and not an excluded entity; and
    - (b) the authority is satisfied that the entity meets the criteria for accreditation under section 77, to a standard appropriate for the accreditation; and
    - (c) the authority considers it appropriate, in all the circumstances, to grant the accreditation.
  - (2) If the accreditation authority grants the entity the accreditation applied for, the authority may accredit the entity:
    - (a) without imposing conditions of accreditation; or
    - (b) with conditions of accreditation imposed by the authority, if the authority is satisfied that imposing the conditions is:
      - (i) appropriate for reasons of security, including on the basis of an adverse or qualified security assessment in respect of a person; or
      - (ii) otherwise reasonable and appropriate in the circumstances to ensure that scheme data is collected and used in accordance with this Act.
- Note 1: The accreditation authority must give the entity notice before making a decision to grant accreditation with conditions (see section 79).
- Note 2: Even if the accreditation authority does not impose conditions of accreditation, conditions of accreditation prescribed by the rules may still be applicable to the entity.
- (3) Without limiting paragraph (1)(b), the accreditation authority may be satisfied that the entity meets the criteria for accreditation under section 77 to the appropriate standard on the basis that:

- (a) the entity will comply with conditions of accreditation imposed on the entity; or
  - (b) because the entity will comply with conditions of accreditation imposed on the entity, the entity does not need to meet one or more of the criteria.
- (4) For the purposes of paragraph (1)(c), an example of when the accreditation authority for an entity may consider it not appropriate to accredit the entity is if the authority considers that the entity's participation in the data sharing scheme would pose concerns for reasons of security.

## **75 Notice of accreditation decision**

- (1) The accreditation authority must give the entity written notice of the authority's decision under section 74, as soon as practicable after making the decision.
- (2) If the accreditation authority grants the entity the accreditation applied for, the notice must set out the following:
  - (a) whether the entity is accredited as an ADSP or accredited user, or both;
  - (b) the day the accreditation comes into force;
  - (c) if the entity is accredited as an ADSP—that the accreditation must be renewed every 5 years (see paragraph 81(8)(a));
  - (d) if the authority decides to grant the accreditation with conditions of accreditation imposed by the authority:
    - (i) those conditions; and
    - (ii) the reasons for the decision; and
    - (iii) the entity's review rights under Part 6.2.
- (3) If the accreditation authority refuses to accredit the entity, the notice must set out the following:
  - (a) the reasons for the refusal;
  - (b) the entity's review rights under Part 6.2.

Section 76

---

**76 Application for accreditation**

- (1) An entity may apply for accreditation, as an ADSP or an accredited user, to the accreditation authority for the entity.
- (2) The application must:
  - (a) be made by an authorised officer on behalf of the entity; and
  - (b) be in the form approved by the Commissioner (if any); and
  - (c) include the evidence prescribed by the rules to support the criteria for accreditation and the entity's ability to meet the criteria to the appropriate standard; and
  - (d) include consent for the Commissioner to:
    - (i) obtain information relevant to the entity's application for accreditation from third parties; and
    - (ii) verify information provided by the entity with third parties.

**77 Criteria for accreditation**

- (1) The criteria for accreditation are the following:
  - (a) the entity has appropriate data management and governance policies and practices and an appropriately qualified individual in a position that has responsibility for data management and data governance for the entity;
  - (b) the entity is able to minimise the risk of unauthorised access, sharing or loss of data;
  - (c) the entity has the necessary skills and capability to ensure the privacy, protection and appropriate use of data, including the ability to manage risks in relation to those matters;
  - (d) any additional criteria prescribed under subsection (2).
- (1A) In addition to the criteria set out in subsection (1), it is a criterion for accreditation as an ADSP that the entity has the necessary policies, practices, skills and capability to perform the following data services:
  - (a) de-identification data services;
  - (b) secure access data services;
  - (c) complex data integration services.

---

Section 77A

---

- (2) The rules may provide for additional criteria for accreditation covering any other matters the Minister considers appropriate.

**77A General provisions relating to accreditation**

- (1) An entity accredited as an ADSP continues to be an ADSP (including while its accreditation as an ADSP is suspended) until the accreditation is cancelled.
- (2) An entity accredited as an accredited user continues to be an accredited user (including while its accreditation as an accredited user is suspended) until the accreditation is cancelled.
- (3) Accreditation is granted on the basis that:
- (a) under Part 5.2, the entity may be accredited with conditions of accreditation and conditions of accreditation may be imposed, varied or removed while the entity is accredited; and
  - (b) the accreditation may be suspended or cancelled under section 81; and
  - (c) the accreditation may be cancelled, revoked, terminated or varied, and conditions of accreditation may be imposed, varied or removed, by or under later legislation; and
  - (d) no compensation is payable in any of those events.

## **Division 2—Conditions of accreditation**

### **77B Conditions of accreditation**

- (1) The rules may prescribe conditions of accreditation applicable to all entities, or to classes of entities, as prescribed.
- (2) Conditions of accreditation, whether prescribed by the rules or imposed by an accreditation authority under section 74, 78 or 84, may require or permit an entity to do something, or prevent it from doing something.
- (3) Examples of conditions that may be prescribed or imposed are conditions to do any of the following:
  - (a) limit the individuals who may collect and use data;
  - (b) require the entity to provide, at a specified time or specified intervals, evidence of specified matters, or specified information, relating to the entity's accreditation;
  - (c) prohibit collection or use of personal information;
  - (d) prohibit collection and use of data other than by means of a secure access data service;
  - (e) prohibit the entity from storing or accessing, or providing access to, scheme data outside Australia;
  - (f) if the entity is, or is applying for accreditation as, an ADSP—limit the kinds of data services the entity may provide.

### **78 Imposition, variation or removal of conditions of accreditation by accreditation authority**

- (1) The accreditation authority for an entity may, while the entity is an accredited entity, impose conditions of accreditation on the entity if the authority considers that doing so is:
  - (a) appropriate for reasons of security, including on the basis of an adverse or qualified security assessment in respect of a person; or
  - (b) otherwise reasonable and appropriate in the circumstances to ensure that scheme data is collected and used in accordance with this Act.

---

Section 79

---

- (2) If a court finds that an accredited entity has committed an offence against this Act, or a civil penalty order is made against an accredited entity for a contravention of subsection 14A(1) to which subsection 14A(2) applies, the accreditation authority for the entity must consider whether it is appropriate to:
  - (a) cancel or suspend the entity's accreditation; or
  - (b) impose one or more conditions on the entity:
    - (i) to mitigate the risks of the entity contravening subsection 14A(1) again or otherwise breaching this Act; or
    - (ii) to prevent one or more individuals engaging in conduct in relation to scheme data held by the entity.
- (3) If a civil penalty order is made against an entity that is accredited as both an ADSP and an accredited user, subsection (2) applies in relation to the entity in both capacities.
- (4) The accreditation authority may vary or remove a condition of accreditation imposed on the entity by the authority at any time if the authority considers that doing so is:
  - (a) appropriate for reasons of security, including on the basis of an adverse or qualified security assessment in respect of a person; or
  - (b) otherwise appropriate in the circumstances.
- (5) If the Minister decides to impose a condition of accreditation on an entity, or vary or remove such a condition, the Minister must notify the Commissioner of the decision.

**79 Notice before decision relating to conditions of accreditation**

- (1) Subject to subsection (4), the accreditation authority for an entity must not make any of the following decisions in relation to an entity unless the authority has given the entity written notice of the proposed decision in accordance with subsection (2):
  - (a) a decision under section 74 to accredit the entity with conditions of accreditation imposed by the authority;
  - (b) a decision under section 78 to impose conditions of accreditation on the entity or vary or remove such conditions;

**Section 80**

---

- (c) a decision under section 84 to renew the entity's accreditation with conditions of accreditation imposed by the authority (including conditions of accreditation imposed before the renewal that continue to be imposed on the entity).

Note: The Commissioner is the accreditation authority under section 84.

- (2) The notice must:
  - (a) state the proposed decision; and
  - (b) request the entity to give the accreditation authority, within the period specified in the notice, a written statement relating to the proposed decision.
- (3) The accreditation authority must consider any written statement given to the authority within the period specified in the notice before making the decision.
- (4) If the reasons for the decision relate to security, or the accreditation authority reasonably believes the reasons to be serious and urgent, the accreditation authority may decide:
  - (a) to give the entity a notice under subsection (2) that does not include the request referred to in paragraph (2)(b); or
  - (b) not to give the entity a notice under subsection (2).

**80 Notice of conditions**

- (1) The accreditation authority for an accredited entity must give the entity written notice of a decision made under section 78, as soon as practicable after making the decision.
- (2) The notice must:
  - (a) state the condition or the variation, or state that the condition is removed; and
  - (b) state the day on which the condition, variation or removal takes effect; and
  - (c) include a statement setting out the entity's review rights under Part 6.2.



## **Division 3—Suspension and cancellation of accreditation**

### **81 Suspension or cancellation of accreditation**

#### *When accreditation may be suspended or cancelled*

- (1) The accreditation authority for an entity may suspend or cancel the accreditation of the entity if any of the following circumstances exist:
  - (a) the accreditation authority is reasonably satisfied that the entity does not meet the criteria for accreditation under section 77 to the appropriate standard;
  - (b) the entity becomes a Chapter 5 body corporate within the meaning of the *Corporations Act 2001*;
  - (c) for accreditation as an ADSP if the entity is a Commonwealth body, State body or Territory body, or the Commonwealth, a State or Territory—the Minister:
    - (i) refuses to accredit the entity as an accredited user; or
    - (ii) suspends or cancels the entity's accreditation as an accredited user;
  - (d) for accreditation as an accredited user—the Commissioner suspends or cancels the entity's accreditation as an ADSP;
  - (e) the accreditation authority determines it is in the national interest;
  - (f) for reasons of security, including on the basis of an adverse or qualified security assessment in respect of a person.
- Note: An accredited entity continues to be an accredited entity (including while its accreditation is suspended) until its accreditation is cancelled (see subsections 77A(1) and (2)).
- (2) The accreditation authority for an entity may suspend the accreditation of the entity if the accreditation authority reasonably suspects that the entity has breached this Act or a data sharing agreement.
- (3) The accreditation authority for an entity may cancel the entity's accreditation if the Commissioner determines under

**Section 81**

---

subsection 102(1) that the entity has breached this Act or a data sharing agreement.

- (4) The Minister may cancel the accreditation of an entity for which the Minister is the accreditation authority if the Minister reasonably believes that the entity has breached this Act or a data sharing agreement.
- (5) If an entity is a data scheme entity in more than one capacity, the accreditation authority may have regard to the entity's conduct in any of those capacities for the purposes of subsections (1), (2), (3) and (4).
- (6) If, under paragraph (1)(c), there is a ground for suspending or cancelling an entity's accreditation as an ADSP, the Commissioner must consider whether to do any of the following:
  - (a) suspend or cancel the entity's accreditation as an ADSP on that ground;
  - (b) impose conditions of accreditation on the entity in its capacity as an ADSP, or vary any such conditions.
- (7) If, under paragraph (1)(d), there is a ground for suspending or cancelling an entity's accreditation as an accredited user, the accreditation authority for the accredited user must consider whether to do any of the following:
  - (a) suspend or cancel the entity's accreditation as an accredited user on that ground;
  - (b) impose conditions of accreditation on the entity in its capacity as an accredited user, or vary any such conditions.

*When accreditation must be suspended or cancelled*

- (8) The Commissioner:
  - (a) must suspend an entity's accreditation as an ADSP if the entity fails to apply for renewal under section 85A within 5 years of the grant of accreditation under section 74 or its renewal under section 84, as applicable; and
  - (b) must suspend or cancel an entity's accreditation as an ADSP after having refused to renew the entity's accreditation under section 84.

---

Section 82

---

Note: An accredited entity continues to be an accredited entity (including while its accreditation is suspended) until its accreditation is cancelled (see subsections 77A(1) and (2)).

*Cancellation on request*

- (9) The accreditation authority for an entity may cancel the entity's accreditation upon request by an authorised officer of the entity. The request must be in the approved form (if any).

*Circumstances in which cancellation does not take effect*

- (10) Unless the accreditation authority for an entity otherwise determines, a decision to cancel the entity's accreditation does not take effect if the entity has not complied with a direction given by the Commissioner under subsection 112(3) (direction for purposes of ensuring that entity does not hold scheme data after the cancellation).

**82 Notice before decision about suspension or cancellation**

- (1) Subject to subsection (4), the accreditation authority for an entity must not suspend or cancel the entity's accreditation under subsection 81(1), (2), (3) or (4) unless the authority has given the entity a written notice in accordance with subsection (2) of this section.
- (2) The notice must:
- (a) state the circumstance that exists for the proposed suspension or cancellation under section 81; and
  - (b) state:
    - (i) if suspension is proposed—the period of suspension, or that the proposed suspension is indefinite; or
    - (ii) if cancellation is proposed—the date proposed for the cancellation to take effect; and
  - (c) for proposed suspension or cancellation under subsection 81(1), (2), (3) or (4)—request the accredited entity to give the accreditation authority, within the period specified in the notice, a written statement showing cause why the accreditation should not be suspended or cancelled.

## Section 83

---

- (3) The accreditation authority must consider any written statement given to the accreditation authority within the period specified in the notice before making a decision under section 81.
- (4) If the reasons for making a decision under section 81 relate to security, or the accreditation authority reasonably believes the reasons to be serious and urgent, the accreditation authority may decide:
  - (a) for a decision made under subsection 81(1), (2), (3) or (4)—to give the entity a notice under subsection (2) of this section that does not include the request referred to in paragraph (2)(c) of this section; or
  - (b) not to give the entity a notice under subsection (2) of this section.

### **83 Notice of suspension or cancellation**

- (1) The accreditation authority for an entity must give the entity written notice of a decision under section 81 to suspend or cancel the entity's accreditation in accordance with subsection (3) of this section.
- (2) The accreditation authority must give the notice as soon as practicable after making the decision.
- (3) The notice must state the following:
  - (a) if accreditation is suspended or cancelled—the circumstance that exists for the suspension or cancellation;
  - (c) if accreditation is suspended—the period of suspension or that the suspension is indefinite;
  - (d) if accreditation is cancelled—the date the cancellation takes effect;
  - (e) the entity's review rights under Part 6.2.

### **83A Lifting of suspension**

If an entity's accreditation is suspended under section 81, the accreditation authority for the entity may lift the suspension by written notice to the entity if satisfied that:

Section 83A

---

- (a) there are no longer any grounds for the suspension; or
- (b) it is otherwise no longer appropriate for the accreditation to be suspended.

## **Division 4—Renewal of accreditation of ADSPs**

### **84 Renewal**

- (1) If an entity applies for the renewal of the entity's accreditation as an ADSP under section 85A, the Commissioner may grant the renewal if:
  - (a) the entity is an Australian entity and not an excluded entity; and
  - (b) the Commissioner is satisfied that the entity meets the criteria for accreditation under section 77, to a standard appropriate for accreditation as an ADSP; and
  - (c) the Commissioner considers it appropriate, in all the circumstances, to grant the renewal.
- (2) If the Commissioner grants the renewal, the Commissioner may renew the accreditation:
  - (a) without imposing conditions of accreditation on the entity; or
  - (b) with conditions of accreditation imposed by the Commissioner (including conditions of accreditation imposed before the renewal that continue to be imposed on the entity), if the Commissioner is satisfied that imposing the conditions is:
    - (i) appropriate for reasons of security, including on the basis of an adverse or qualified security assessment in respect of a person; or
    - (ii) otherwise reasonable and appropriate in the circumstances to ensure that scheme data is collected and used in accordance with this Act.

Note 1: The Commissioner must give the entity notice before making a decision to renew the entity's accreditation with conditions (see section 79).

Note 2: Even if the Commissioner does not impose conditions of accreditation, conditions of accreditation prescribed by the rules may still be applicable to the entity.

- (3) Without limiting paragraph (1)(b), the Commissioner may be satisfied that the entity meets the criteria for accreditation under section 77 to the appropriate standard on the basis that:
  - (a) the entity will comply with conditions of accreditation imposed on the entity; or
  - (b) because the entity will comply with conditions of accreditation imposed on the entity, the entity does not need to meet one or more of the criteria.
- (4) For the purposes of paragraph (1)(c), an example of when the Commissioner may consider it not appropriate to grant the renewal is if the Commissioner considers that the entity's continued participation in the data sharing scheme would pose concerns for reasons of security.

## **85 Notice of renewal decision**

- (1) The Commissioner must give the entity written notice of the Commissioner's decision under section 84, as soon as practicable after making the decision.
- (2) If the Commissioner grants the entity the renewal, the notice must set out the following:
  - (a) the 5-year period for which the renewed accreditation is in effect (see paragraph 81(8)(a));
  - (b) if the Commissioner decides to grant the renewal with conditions of accreditation imposed by the Commissioner (including conditions of accreditation imposed before the renewal that continue to be imposed on the entity):
    - (i) those conditions; and
    - (ii) the reasons for the decision; and
    - (iii) the entity's review rights under Part 6.2.
- (3) If the Commissioner refuses to renew the entity's accreditation, the notice must set out the following:
  - (a) the reason for the refusal;
  - (b) that the entity's accreditation will be suspended or cancelled under section 81; and
  - (c) the entity's review rights under Part 6.2.

Section 85A

---

**85A Application for renewal**

- (1) An entity that is accredited as an ADSP may apply to the Commissioner for renewal of its accreditation.

Note: For the consequences of failure to apply for renewal, see subsection 81(8). An entity may apply for renewal under this section before or after its accreditation has been suspended under that subsection.

- (2) The application must:
- (a) be made by an authorised officer of the entity; and
  - (b) be in the approved form (if any); and
  - (c) include the evidence prescribed by the rules to support the criteria for accreditation and the entity's ability to meet the criteria to the appropriate standard; and
  - (d) include consent for the Commissioner to:
    - (i) obtain information relevant to the entity's application for renewal from third parties; and
    - (ii) verify information provided by the entity with third parties.



## **Division 5—Rules and further information**

### **86 Rules relating to the accreditation framework**

The rules may provide for procedures, requirements and any other matters relating to the accreditation of entities for the purposes of the data sharing scheme.

Note: The rules may prescribe fees in relation to services provided under the accreditation framework (see section 139).

### **87 Further information or evidence**

- (1) The accreditation authority for an entity may, by notice in writing, request further information or evidence from the entity for the purpose of making a decision under this Part, including information or evidence prescribed by the rules.
- (2) If the accreditation authority requests information or evidence under subsection (1), the accreditation authority need not make the decision under this Part until the entity provides the information or evidence.

## **Part 5.3—Complaints**

### **Division 1—Scheme Complaints**

#### **88 Making scheme complaints**

- (1) A data scheme entity may complain to the Commissioner if the complainant reasonably suspects that another entity, while the other entity was a data scheme entity, breached:
  - (a) this Act; or
  - (b) a data sharing agreement to which both entities were party when the alleged breach occurred.
- (2) An entity that ceased to be a data scheme entity no more than 12 months earlier may also complain to the Commissioner if the complainant has the reasonable suspicion mentioned in subsection (1).
- (3) A complaint must:
  - (a) specify the respondent (see section 89); and
  - (b) be made in an approved form (if any); and
  - (c) meet any requirements prescribed by a data code.

#### **89 Respondents**

- (1) If the complaint is about an entity that is a Commonwealth body, the respondent is whichever of the following applies:
  - (a) if the Commonwealth body is a body corporate or an individual—the Commonwealth body;
  - (b) if the Commonwealth body is unincorporated—the principal executive of the Commonwealth body within the meaning of section 37 of the *Privacy Act 1988*.
- (2) If the complaint is about an entity that is not a Commonwealth body, the respondent is the entity.

**90 Communicating with complainant**

- (1) The Commissioner must, no later than 30 days after receiving a complaint under section 88, give the complainant written notice setting out how the Commissioner is dealing with, or intends to deal with, the complaint.
- (2) The Commissioner may, by written notice given to the complainant, request the complainant to give the Commissioner, within the period specified in the notice, further information in connection with the complaint.
- (3) If the Commissioner makes a request under subsection (2):
  - (a) the Commissioner need not take any further action in relation to the complaint until the complainant complies with the request; and
  - (b) if the request is made before the end of the 30 day period mentioned in subsection (1)—the 30 day period mentioned in that subsection is taken to start on the day the complainant complies with the request.
- (4) The Commissioner does not need to comply with subsection (1) of this section if the Commissioner gives the complainant a notice under subsection 92(2) (grounds for not dealing with complaints) on or before the last day for complying with subsection (1).

**91 Dealing with complaints**

- (1) If the Commissioner receives a complaint under section 88, the Commissioner must:
  - (a) make any preliminary inquiries, of the complainant, respondent or any other person, that the Commissioner considers necessary for the purposes of determining whether and how to deal with the complaint; and
  - (b) consider whether it would be appropriate to seek to resolve the complaint by conciliation, or an external dispute resolution scheme recognised under section 131, and, if so, make the necessary arrangements.

## Section 92

---

- (2) Paragraph (1)(b) does not apply if the Commissioner is satisfied that a ground exists for not dealing with the complaint (see section 92).

### **92 Grounds for not dealing with complaints**

- (1) If a complaint is made under section 88 in relation to an entity's alleged breach of this Act or a data sharing agreement, a ground exists for not dealing with the complaint if any of the following applies:
- (a) the Commissioner is satisfied that the alleged breach:
    - (i) did not occur; or
    - (ii) is not material;
  - (b) the complainant fails to satisfy the Commissioner that:
    - (i) the complainant has complained about the alleged breach to the entity; or
    - (ii) it would not be appropriate for the complainant to do so;
  - (c) the complainant has complained about the alleged breach to the entity before complaining to the Commissioner and the Commissioner is satisfied that:
    - (i) the entity has dealt, or is dealing, adequately with the complaint; or
    - (ii) the entity has not had an adequate opportunity to deal with the complaint;
  - (d) the complaint was made more than 12 months after the complainant first reasonably suspected the entity breached this Act or the relevant data sharing agreement;
  - (e) the complaint is frivolous, vexatious, misconceived, lacking in substance or not made in good faith;
  - (f) an investigation, or further investigation, of the alleged breach is impracticable or otherwise unwarranted, having regard to all the circumstances;
  - (g) the complainant has not responded, within the period specified by the Commissioner, to a request for information in relation to the complaint;
  - (h) the Commissioner considers that it would be appropriate to seek to resolve the complaint by conciliation or an external

dispute resolution scheme recognised under section 131 (whether or not the entity and the complainant agree to do so);

- (i) the complaint is being resolved as mentioned in paragraph (h);
  - (j) the conduct giving rise to the complaint is the subject of an application under another Commonwealth law, or a State or Territory law, and the subject matter of the complaint has been, or is being, dealt with adequately under that law;
  - (k) another Commonwealth law, or a State or Territory law, provides a more appropriate remedy for the conduct giving rise to the complaint (including where the Commissioner has formed the opinion mentioned in section 107 (transfer of matters to appropriate authority));
  - (l) the complainant has withdrawn the complaint.
- (2) If the Commissioner decides under subsection 91(2) or paragraph 101(4)(a) to cease dealing with a complaint because a ground exists for not dealing with the complaint, the Commissioner must give the complainant written notice of:
- (a) the Commissioner's decision and the reasons for it; and
  - (b) the complainant's review rights under Part 6.2.
- (3) If the Commissioner notified the respondent of the complaint, the Commissioner must give the respondent a copy of any notice given to the complainant.

### **93 Admissibility of things said or done in conciliation**

If a complaint is dealt with by conciliation, evidence of anything said or done in the course of the conciliation is not admissible in any legal proceedings under this Act or any other law, unless:

- (a) the complainant and respondent otherwise agree; or
- (b) the thing was said or done in the course of committing an offence or contravening a civil penalty provision.

## Division 2—General complaints

### 94 Making general complaints

A person may complain to the Commissioner about any matter relating to the administration or operation of the data sharing scheme.

### 95 Dealing with complaints

The Commissioner may deal with a complaint made under section 94 by doing any of the following:

- (a) making any preliminary inquiries, of the complainant or any other person, that the Commissioner considers necessary for the purposes of determining whether and how to deal with the complaint;
- (b) requesting the complainant to give the Commissioner further information in connection with the complaint;
- (c) if the complaint causes the Commissioner to reasonably suspect that an entity has breached this Act, or a data sharing agreement, while the entity is or was a data scheme entity—investigating the entity’s conduct under subsection 101(2);
- (d) considering whether it would be appropriate to deal with the complaint by conciliation and, if so, dealing with it or arranging for it to be dealt with in that way;
- (e) if the Commissioner is satisfied no action is required in relation to the complaint—deciding to take no action;
- (f) exercising any other powers of the Commissioner under this Act that the Commissioner considers appropriate in relation to the complaint, including:
  - (i) the power to conduct assessments under section 99; and
  - (ii) the power to transfer matters to other agencies or bodies under section 107.

### 96 Admissibility of things said or done in conciliation

If a complaint under section 94 is dealt with by conciliation, evidence of anything said or done in the course of the conciliation

is not admissible in any legal proceedings under this Act or any other law, unless:

- (a) the complainant and respondent otherwise agree; or
- (b) the thing was said or done in the course of committing an offence or contravening a civil penalty provision.

Section 99

---

## **Part 5.4—Assessments and investigations**

### **99 Assessments**

- (1) The Commissioner may, from time to time, assess whether conduct that an entity engages or engaged in while it is or was a data scheme entity is consistent with the requirements of this Act.
- (2) The Commissioner may conduct an assessment in any manner the Commissioner considers appropriate.
- (3) The Commissioner may, for the purposes of an assessment, obtain information from any person, and make any inquiries, the Commissioner considers appropriate.

Note: The Commissioner may require a person to give information or documents for the purposes of the Commissioner's functions under this Part (see section 104), and may exercise powers under the Regulatory Powers Act to monitor compliance with certain provisions of this Act (see section 109).

- (4) If the Commissioner invites submissions in relation to an assessment, the Commissioner must have regard to any submissions made in response to the invitation.

### **100 Notices of assessment**

- (1) The Commissioner must give an entity written notice before starting, and on completion of, an assessment of the operations of the entity.
- (2) The notice given before starting the assessment must specify the intended scope of the assessment.

### **101 Investigations**

- (1) The Commissioner must investigate conduct engaged in by an entity, so far as it relates to a complaint made about the entity under section 88, unless the Commissioner is satisfied that a ground exists for not dealing with the complaint (see section 92).



Section 101

---

- (1A) The Commissioner must investigate conduct engaged in by an entity while it is or was a data scheme entity if the Minister directs the Commissioner to do so under subsection (1B).
- (1B) The Minister may, by notifiable instrument, direct the Commissioner to investigate conduct engaged in by an entity while it is or was a data scheme entity, if the Minister:
  - (a) is or was the accreditation authority for the entity; and
  - (b) reasonably suspects that the entity has breached, is breaching or is proposing to breach this Act or a data sharing agreement.
- (2) The Commissioner may, on the Commissioner's own initiative, investigate conduct engaged in by an entity while the entity is or was a data scheme entity if the Commissioner reasonably suspects that the entity has breached, is breaching or is proposing to breach this Act or a data sharing agreement.
- (3) An investigation may be conducted while the entity is, or after it has ceased to be, a data scheme entity.
- (4) The Commissioner may cease an investigation at any time if:
  - (a) for an investigation under subsection (1)—the Commissioner is satisfied that a ground exists for not dealing with the complaint to which the investigation relates (see section 92); or
  - (b) for an investigation under subsection (1A):
    - (i) the Minister no longer reasonably suspects that the entity has breached, is breaching or is proposing to breach this Act or a data sharing agreement (as the case requires), and informs the Commissioner of that fact; or
    - (ii) the Commissioner otherwise considers it appropriate to cease the investigation; or
  - (c) for an investigation under subsection (2)—the Commissioner:
    - (i) no longer reasonably suspects that the entity has breached this Act or a data sharing agreement; or
    - (ii) otherwise considers it appropriate to cease the investigation.

## Section 102

---

- (5) The Commissioner may conduct an investigation in any manner the Commissioner considers appropriate.
- (6) The Commissioner may, for the purposes of an investigation, obtain information from any person, and make any inquiries, the Commissioner considers appropriate.

**Note:** The Commissioner may require a person to give information or documents for the purposes of an investigation (see section 104), and may exercise powers under the Regulatory Powers Act to investigate breaches of certain provisions of this Act (see section 110).

- (7) If the Commissioner invites submissions in relation to an investigation, the Commissioner must have regard to any submissions made in response to the invitation.

### **102 Determination on completion of investigation**

- (1) If the Commissioner completes an investigation of the operations of an entity under this Part, the Commissioner must make a written determination setting out:
  - (a) the Commissioner's opinion as to whether the entity has breached this Act or a data sharing agreement, or is breaching or proposing to breach this Act or a data sharing agreement, and the reasons for that opinion; and
  - (b) if the Commissioner is satisfied that the entity has breached this Act or the data sharing agreement, or is breaching or proposing to breach this Act or the data sharing agreement—an indication of any action the Commissioner has decided to take, or advise the Minister as accreditation authority to take, in relation to the entity's accreditation, or under Part 5.5 (regulatory powers and enforcement) of this Act or the Regulatory Powers Act as it applies in relation to this Act.

**Note:** The Commissioner must give the determination to the entity and may give it to the complainant (see subsection 103(3)).

- (2) The Commissioner may make the determination publicly available, in any manner, and for any period (including indefinitely), the Commissioner considers appropriate.

---

Section 103

---

- (2A) If the determination relates to an investigation under subsection 101(1A), the Commissioner must give the Minister a copy of the determination.
- (3) The Commissioner may, in writing, vary or revoke the determination.
- (4) A determination made under subsection (1) is not a legislative instrument.

### **103 Notices relating to investigation**

- (1) The Commissioner must give an entity written notice before starting an investigation of the operations of the entity.
- (2) The notice must specify the intended scope of the investigation.
- (3) On completion of the investigation, the Commissioner:
  - (a) must give the entity the determination made under section 102 in relation to the investigation together with, if the Commissioner decides to make the determination publicly available, notice of the entity's review rights under Part 6.2 in relation to that decision; and
  - (b) if the investigation relates to a complaint under section 88 or 94—may also give the complainant that determination.
- (3A) If the Commissioner ceases the investigation under subsection 101(4), the Commissioner must give the entity and any complainant written notice of the cessation.
- (4) If the Commissioner varies or revokes the determination, the Commissioner must give the variation or revocation to the entities that were given the determination under subsection (3).

### **103A Recommendations**

If the Commissioner completes an assessment or investigation, under this Part, of the operations of a data scheme entity, the Commissioner may give the entity written recommendations about any action the Commissioner considers the entity should take in relation to matters covered by the assessment or investigation.

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

### **104 Power to require information and documents**

- (1) If the Commissioner reasonably believes that a person has information or a document relevant to an investigation under section 101, or to any other of the Commissioner's regulatory functions set out in section 45, the Commissioner may, by written notice given to the person, require the person to give the information, or produce the document, to the Commissioner within the period specified in the notice.

Note: There are limits on the information and documents that may be required (see section 106).

- (2) If:
- (a) a person is given a notice under subsection (1); and
  - (b) the notice relates to an investigation under section 101;
- the person must comply with the notice.

Civil penalty: 30 penalty units.

- (3) A person commits an offence if:
- (a) the person is given a notice under subsection (1); and
  - (b) the notice relates to an investigation under section 101; and
  - (c) the person fails to comply with the notice.

Penalty: Imprisonment for 6 months.

- (4) If the person produces a document to the Commissioner in compliance with the notice, the Commissioner:
- (a) may take possession of, and may make copies of, or take extracts from, the document; and
  - (b) may retain possession of the document for any period necessary for the purposes of the investigation; and
  - (c) must, during that period, permit any person who would be entitled to inspect the document if it were not in the

Commissioner's possession to inspect the document at any reasonable time.

### **105 Legal professional privilege**

- (1) A person is not excused from complying with a notice under section 104 on the ground that giving the information or producing the document would disclose a communication protected against disclosure by legal professional privilege, if the communication is:
  - (a) legal advice given to a Minister or a Commonwealth body; or
  - (b) a communication between a designated individual for a Commonwealth body, if the communication is within the actual or apparent scope of the individual's designation, and another person or body.
- (2) However:
  - (a) the information given or document produced; and
  - (b) the giving of the information or production of the document;are not admissible in evidence against a person in any civil or criminal proceedings.
- (3) The fact that a person is not excused from complying with the notice on the ground mentioned in subsection (1) does not otherwise affect a claim of legal professional privilege that anyone may make in relation to that information or document.
- (4) If a person claims, by written notice given to the Commissioner, that, but for subsection (1), information or a document specified in a notice given to the person under section 104 would be protected against disclosure by legal professional privilege, the Commissioner:
  - (a) must withdraw the notice unless satisfied that it is reasonably necessary and proportionate to the investigation to require the person to give the information or produce the document; and
  - (b) must ensure that the information and documents are held securely and destroyed when the investigation ends; and
  - (c) may disclose the information or documents to a person if:
    - (i) the person is a member of the staff mentioned in section 47, or engaged as a contractor or consultant as

## Section 106

---

- mentioned in section 48 or 49, or otherwise providing services to the Commissioner; and
  - (ii) the Commissioner is satisfied that the disclosure is reasonably necessary for the purposes of the investigation; and
  - (d) must not disclose the information or documents except in accordance with paragraph (c).
- (5) Subsection (4) does not apply if there are no reasonable grounds for the person's claim.

### **106 Limits on power to require information and documents**

#### *Excluded entities*

- (1) A notice under subsection 104(1) must not require a person to give information or a document that is held by, or that originated with or was received from, an excluded entity.

#### *Public interest certificate*

- (2) A notice under subsection 104(1) must not require a person to give information relating to a matter, or to give a document, specified in a certificate given to the Commissioner under subsection (3) of this section.
- (3) The Attorney-General may give the Commissioner a certificate stating that, in the opinion of the Attorney-General, giving information in relation to a specified matter, or giving a specified document, would be contrary to the public interest because it would do any of the following:
- (a) prejudice the security, defence or international relations of Australia;
  - (b) involve the disclosure of communications between a Minister of the Commonwealth and a Minister of a State or Territory, being a disclosure that would prejudice relations between the Commonwealth government and the government of a State or Territory;
  - (c) involve the disclosure of deliberations or decisions of the Cabinet or of a Committee of the Cabinet;

- (d) involve the disclosure of deliberations or advice of the Executive Council;
- (e) prejudice the conduct of an investigation or inquiry into crime or criminal activity that is currently being pursued, or prejudice the fair trial of any person;
- (f) disclose, or enable a person to ascertain, the existence or identity of a confidential source of information in relation to the enforcement of the criminal law;
- (g) prejudice the effectiveness of the operational methods or investigative practices or techniques of agencies responsible for the enforcement of the criminal law;
- (h) endanger the life or physical safety of any person.

*Parliamentary privilege*

- (4) Nothing in section 104 affects the privileges and immunities of a House of the Parliament, a member of a House of the Parliament or a committee within the meaning of the *Parliamentary Privileges Act 1987*.

### **107 Transfer of matters to appropriate authority**

If, at any time while dealing with a matter under this Act (including a complaint under section 88 or 94), the Commissioner forms the opinion that the matter:

- (a) is capable of being dealt with by an agency or body to which the Commissioner is authorised to disclose information under section 108; and
- (b) could be more effectively or conveniently dealt with by that agency or body;

the Commissioner may cease to deal with the matter and request the other agency or body to deal with the matter instead.

Note: The Commissioner may give the agency or body any relevant information under section 108.

Section 108

---

**108 Authorisation for Commissioner to disclose and receive information**

*Disclose*

- (1) The Commissioner may disclose, or authorise a member of the staff mentioned in section 47 to disclose, information or a document (including personal information) to an agency or body covered by subsection (2) if:
  - (a) the information or document was collected by the Commissioner or staff member in the course of performing functions under this Act; and
  - (b) the Commissioner is satisfied that the information or document will assist the agency or body to perform any of its functions or exercise any of its powers; and
  - (c) subsection 105(4) does not apply in relation to the information.
- (2) This subsection covers the following agencies and bodies:
  - (a) the Information Commissioner;
  - (b) a State body, or a Territory body, whose functions include functions that correspond to those of the Information Commissioner;
  - (c) the Commonwealth Ombudsman;
  - (d) a State body, or a Territory body, whose functions include functions that correspond to those of the Commonwealth Ombudsman;
  - (e) the Australian Securities and Investments Commission;
  - (f) the Australian Competition and Consumer Commission;
  - (g) a regulatory authority of a foreign country whose functions include functions that correspond to those of a person mentioned in paragraph (a), (c), (e) or (f);
  - (h) the Australian National Audit Office;
  - (i) the Australian Federal Police;
  - (j) the police force, or police service, of a State or Territory;
  - (k) the Australian Commission for Law Enforcement Integrity;
  - (l) AUSTRAC (within the meaning of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*);



- (m) the Australian Security Intelligence Organisation;
- (n) the Inspector-General of Intelligence and Security;
- (o) an agency or body prescribed by the rules for the purposes of this paragraph.

*Receive*

- (3) The Commissioner, or a member of the staff mentioned in section 47, is authorised to receive information or a document disclosed by an agency or body covered by subsection (2) for the purposes of assisting the Commissioner or staff member to perform any of their functions or exercise any of their powers.

## **109 Monitoring powers**

*Monitoring powers*

- (1) The following provisions of this Act are subject to monitoring under Part 2 of the Regulatory Powers Act:
  - (a) a civil penalty provision;
  - (b) an offence against section 14 or 14A (penalties for unauthorised sharing, collection and use) and subsection 104(3) (failure to comply with notice given under subsection 104(1));
  - (c) a provision of Chapter 3 (responsibilities of data scheme entities).

Note: Part 2 of the Regulatory Powers Act creates a framework for monitoring whether a provision is being complied with. It includes powers of entry and inspection.

*Information subject to monitoring*

- (2) Information given in compliance or purported compliance with a provision of this Act is subject to monitoring under Part 2 of the Regulatory Powers Act.

Note: Part 2 of the Regulatory Powers Act creates a framework for monitoring whether the information is correct. It includes powers of entry and inspection.

## Section 110

---

*Related provisions, authorised applicant, authorised person, issuing officer, relevant chief executive and relevant court*

- (3) For the purposes of Part 2 of the Regulatory Powers Act, as that Part applies in relation to the provisions mentioned in subsection (1) and the information mentioned in subsection (2):
- (a) there are no related provisions; and
  - (b) the Commissioner is an authorised applicant; and
  - (c) the Commissioner is an authorised person; and
  - (d) any judicial officer within the meaning of the Regulatory Powers Act is an issuing officer; and
  - (e) the Commissioner is the relevant chief executive; and
  - (f) each of the following is a relevant court:
    - (i) the Federal Court;
    - (ii) the Circuit Court;
    - (iii) a court of a State or Territory that has jurisdiction in relation to matters arising under this Act.

*Person assisting*

- (4) An authorised person may be assisted by other persons in exercising powers or performing functions or duties under Part 2 of the Regulatory Powers Act in relation to the provisions mentioned in subsection (1) and the information mentioned in subsection (2).

Note: The person assisting must have the necessary skills, qualifications or experience (see subsection 45(2)).

## 110 Investigation powers

*Provisions subject to investigation*

- (1) The following provisions of this Act are subject to investigation under Part 3 of the Regulatory Powers Act:
- (a) a civil penalty provision;
  - (b) an offence against this Act;
  - (c) a provision of Chapter 3 (responsibilities of data scheme entities).

Section 112

---

- Note 1: Part 3 of the Regulatory Powers Act creates a framework for investigating whether a provision has been contravened. It includes powers of entry, search and seizure.
- Note 2: The meaning of *offence against this Act* is extended by the definition in section 9.

*Related provisions, authorised applicant, authorised person, issuing officer, relevant chief executive and relevant court*

- (2) For the purposes of Part 3 of the Regulatory Powers Act, as that Part applies in relation to evidential material that relates to a provision mentioned in subsection (1):
- (a) there are no related provisions; and
  - (b) the Commissioner is an authorised applicant; and
  - (c) the Commissioner is an authorised person; and
  - (d) any judicial officer within the meaning of the Regulatory Powers Act is an issuing officer; and
  - (e) the Commissioner is the relevant chief executive; and
  - (f) each of the following is a relevant court:
    - (i) the Federal Court;
    - (ii) the Circuit Court;
    - (iii) a court of a State or Territory that has jurisdiction in relation to matters arising under this Act.

*Person assisting*

- (3) An authorised person may be assisted by other persons in exercising powers or performing functions or duties under Part 3 of the Regulatory Powers Act in relation to evidential material that relates to a provision mentioned in subsection (1).

Note: The person assisting must have the necessary skills, qualifications or experience (see subsection 45(2)).

## Section 112

---

### **112 Directions**

#### *Directions in situations of urgency*

- (1) The Commissioner may give a data scheme entity a written direction requiring the entity to take, or not to take, specified actions if the Commissioner is satisfied that:
  - (a) either of the following situations exists:
    - (i) the entity, or another entity, has acted or is likely to act in a way that is inconsistent with this Act or a data sharing agreement;
    - (ii) an emergency or high risk situation has arisen or is likely to arise; and
  - (b) for a requirement to take specified actions—it is necessary, to address the situation or prevent it arising again, for the entity to take the actions immediately or as soon as practicable; and
  - (c) for a requirement not to take specified actions—the entity is taking the actions or may take them imminently and it is necessary, to address the situation or prevent it arising again, for the entity not to take the actions.

#### *Directions in other situations*

- (2) The Commissioner may give a data scheme entity a written direction requiring the entity to take, or not to take, specified actions if the Commissioner is satisfied that:
  - (a) the entity, or another entity, has acted or is likely to act in a way that is inconsistent with this Act or a data sharing agreement; and
  - (b) for a requirement to take specified actions—it is necessary, to address the situation mentioned in paragraph (a) or prevent it arising again, for the entity to take the actions; and
  - (c) for a requirement not to take specified actions—the entity is taking the actions or may take them and it is necessary, to address the situation mentioned in paragraph (a) or prevent it arising again, for the entity not to take the actions.

---

Section 113

---

- (3) The Commissioner may give an accredited entity a written direction requiring the entity to take, or not to take, specified actions if the Commissioner is satisfied that:
- (a) the accreditation authority for the entity intends to cancel the entity's accreditation (whether at the entity's request or otherwise); and
  - (b) for a requirement to take specified actions—it is necessary, to ensure that the entity does not hold scheme data after the cancellation, for the entity to take the actions; and
  - (c) for a requirement not to take specified actions—it is necessary, to ensure that the entity does not hold scheme data after the cancellation, for the entity not to take the actions.

*Specified actions*

- (4) The specified actions may include providing another entity with access to scheme data.

*Compliance with directions*

- (5) An entity must comply with a direction given to the entity.

Civil penalty:           300 penalty units.

- (6) A direction made under subsection (1), (2) or (3) is not a legislative instrument.

## **113 Civil penalty provisions**

*Enforceable civil penalty provisions*

- (1) Each civil penalty provision of this Act is enforceable under Part 4 of the Regulatory Powers Act.

Note:           Part 4 of the Regulatory Powers Act allows a civil penalty provision to be enforced by obtaining an order for a person to pay a pecuniary penalty for the contravention of the provision.

- (2) However, an authorised applicant may not apply under section 82 of the Regulatory Powers Act for an order that a person pay a pecuniary penalty in relation to a contravention of a civil penalty provision of this Act unless the Commissioner has made a

## Section 114

---

determination under section 102 of this Act setting out the Commissioner's opinion that the person has contravened the provision.

### *Authorised applicant and relevant court*

- (3) For the purposes of Part 4 of the Regulatory Powers Act:
- (a) the Commissioner is an authorised applicant in relation to the civil penalty provisions in this Act; and
  - (b) each of the following is a relevant court in relation to the civil penalty provisions of this Act:
    - (i) the Federal Court;
    - (ii) the Circuit Court;
    - (iii) a court of a State or Territory that has jurisdiction in relation to the matter.

## **114 Infringement notices**

### *Provisions subject to an infringement notice*

- (1) A civil penalty provision of this Act is subject to an infringement notice under Part 5 of the Regulatory Powers Act.

Note: Part 5 of the Regulatory Powers Act creates a framework for using infringement notices in relation to provisions.

- (2) However, an infringement officer may not give a person an infringement notice under section 103 of the Regulatory Powers Act in relation to a contravention of a civil penalty provision of this Act unless the Commissioner has made a determination under section 102 of this Act setting out the Commissioner's opinion that the person has contravened the provision.

### *Infringement officer and relevant chief executive*

- (3) For the purposes of Part 5 of the Regulatory Powers Act:
- (a) the Commissioner is an infringement officer in relation to the provisions mentioned in subsection (1); and
  - (b) the Commissioner is the relevant chief executive in relation to the provisions mentioned in subsection (1).

*Single infringement notice may deal with more than one contravention*

- (4) Despite subsection 103(3) of the Regulatory Powers Act, a single infringement notice may be given to a person in respect of:
- (a) 2 or more alleged contraventions of a provision mentioned in subsection (1); or
  - (b) alleged contraventions of 2 or more provisions mentioned in subsection (1).

However, the notice must not require the person to pay more than one amount in respect of the same conduct.

## **115 Enforceable undertakings**

*Enforceable provisions*

- (1) The provisions of this Act are enforceable under Part 6 of the Regulatory Powers Act.

Note: Part 6 of the Regulatory Powers Act creates a framework for accepting and enforcing undertakings relating to compliance with provisions.

*Authorised person and relevant court*

- (2) For the purposes of Part 6 of the Regulatory Powers Act:
- (a) the Commissioner is an authorised person in relation to the provisions of this Act; and
  - (b) each of the following is a relevant court in relation to the provisions of this Act:
    - (i) the Federal Court;
    - (ii) the Circuit Court;
    - (iii) a court of a State or Territory that has jurisdiction in relation to the matter.

## Section 116

---

*Enforceable undertaking may be published on the Commissioner's website*

- (3) An authorised person in relation to a provision mentioned in subsection (1) may make an undertaking given in relation to the provision publicly available.

### 116 Injunctions

*Enforceable provisions*

- (1) The following provisions of this Act are enforceable under Part 7 of the Regulatory Powers Act:
- (a) a civil penalty provision;
  - (b) a provision of Chapter 3 (responsibilities of data scheme entities).

Note: Part 7 of the Regulatory Powers Act creates a framework for using injunctions to enforce provisions.

- (2) However, an authorised person may not apply under section 121 of the Regulatory Powers Act for an injunction in relation to conduct in contravention of a civil penalty provision of this Act unless the Commissioner has made a determination under section 102 of this Act setting out the Commissioner's opinion that the person has contravened, is contravening or is proposing to contravene the provision.

*Authorised person and relevant court*

- (3) For the purposes of Part 7 of the Regulatory Powers Act:
- (a) the Commissioner is an authorised person in relation to the provisions mentioned in subsection (1); and
  - (b) each of the following is a relevant court in relation to the provisions mentioned in subsection (1):
    - (i) the Federal Court;
    - (ii) the Circuit Court;
    - (iii) a court of a State or Territory that has jurisdiction in relation to matters arising under this Act.



## **Chapter 6—Other matters**

### **Part 6.1—Introduction**

#### **117 Simplified outline of this Chapter**

Some of the administrative aspects of the data sharing scheme are set out in this Chapter.

Certain administrative decisions made by the Minister or Commissioner are reviewable by the Administrative Appeals Tribunal.

The following kinds of legislative instruments may be made for the purposes of the data sharing scheme:

- (a) data codes and guidelines (made by the Commissioner);
- (b) rules (made by the Minister);
- (c) regulations (made by the Governor-General).

The Commissioner may also make the following non-legislative instruments:

- (b) registers making certain information about accredited entities and data sharing agreements publicly available;
- (c) instruments recognising external dispute resolution providers and approving forms.

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

Some other matters of detail are also set out in this Chapter.

## Part 6.2—Review of decisions

### 118 Reviewable decisions

- (1) Each of the following decisions made by the Commissioner is a ***reviewable decision***:
- (a) a decision under section 74 to accredit an entity with conditions of accreditation imposed by the Commissioner, or to refuse to accredit the entity;
  - (b) a decision under section 78 to impose conditions of accreditation on an accredited entity, or vary them;
  - (c) a decision under subsection 81(1), (2), (3) or (4) to suspend or cancel an entity's accreditation;
  - (d) a decision under section 84 to renew an entity's accreditation with conditions of accreditation imposed by the Commissioner, or to refuse to renew an entity's accreditation;
  - (e) a decision under subsection 91(2), or paragraph 101(4)(a), not to deal with a complaint;
  - (f) a decision under subsection 102(2) to make a determination publicly available;
  - (g) a decision under subsection 112(2) or (3) to give an entity a written direction.

The Commissioner is the ***reviewer*** for the decision.

Note: Decisions made personally by the Commissioner are reviewable by the AAT (see section 122). The Commissioner is the reviewer only for decisions made by delegates of the Commissioner.

- (2) Each of the following decisions made by the Minister is also a ***reviewable decision***:
- (a) a decision to accredit an entity with conditions of accreditation imposed by the Minister, or to refuse to accredit the entity;
  - (b) a decision under section 78 to impose conditions of accreditation on an accredited entity, or vary them;

---

Section 119

---

- (c) a decision under subsection 81(1), (2), (3) or (4) to suspend or cancel an entity's accreditation.

The Minister is the **reviewer** for the decision.

Note: Decisions made personally by the Minister are reviewable by the AAT (see section 122). The Minister is the reviewer only for decisions made by the Commissioner as the Minister's delegate.

### **119 Applications for reconsideration of decisions made by delegates of the reviewer**

- (1) If a person is affected by a reviewable decision made by a delegate of the reviewer for the decision, the person may apply to the reviewer for reconsideration of the decision.
- (2) The application must:
  - (a) be in an approved form (if any); and
  - (b) set out the reasons for the application.
- (3) If the rules prescribe a fee for making an application under this section, the application is taken not to have been made unless the fee is paid.

### **120 Reconsideration by reviewer**

- (1) If a person applies under subsection 119(1) to the reviewer for a reviewable decision for reconsideration of the decision, the reviewer must reconsider the decision and do any of the following:
  - (a) affirm the decision;
  - (b) vary the decision;
  - (c) revoke the decision and substitute a new decision.
- (2) The reviewer's decision on reconsideration of a decision has effect as if it had been made under the provision under which the original decision was made.
- (3) The reviewer must give the applicant a written notice stating the reviewer's decision on the reconsideration.

## Section 121

---

- (4) Within 28 days after making the decision on the reconsideration, the reviewer must give the applicant a written statement of the reviewer's reasons for the decision.
- (5) If the reviewer's functions under this section are performed by a delegate of the reviewer, the delegate who reconsiders the reviewable decision:
  - (a) must not have been involved in making the reviewable decision; and
  - (b) must hold a position, or perform duties, of at least the same level as the delegate who made the reviewable decision.

Note: The Commissioner may delegate functions and powers to members of staff (see section 50). The Minister may delegate functions and powers to the Commissioner (see section 137A).

### **121 Deadline for reconsideration**

- (1) The reviewer must make a decision on reconsideration of a decision within 90 days after receiving an application for reconsideration.
- (2) The reviewer is taken, for the purposes of this Part, to have made a decision affirming the original decision if the reviewer has not informed the applicant of the reviewer's decision on the reconsideration before the end of the period of 90 days.

### **122 Review by the Administrative Appeals Tribunal**

Applications may be made to the Administrative Appeals Tribunal to review a reviewable decision if any of the following apply:

- (a) the decision was made personally by the Commissioner (other than a decision made by the Commissioner in the Commissioner's capacity as a delegate of the Minister);
- (aa) the decision was made personally by the Minister;
- (b) the decision has been affirmed or varied under paragraph 120(1)(b).

## Part 6.3—Extension of authorisations and attribution of conduct

### 123 Designated individuals and designation

- (1) For the purposes of this Act, the following table specifies individuals who are *designated individuals* for entities, and each such individual's *designation*.

Designated individuals and designation		
Item	Designated individuals	Designation
1	an authorised officer of the entity or an individual authorised under subsection 137(3) or (4)	section 137 and, if applicable, the authorisation of the individual under subsection 137(3) or (4)
2	a statutory officeholder of the entity	the individual's capacity as a statutory officeholder
3	an APS employee in the entity not covered by item 2	the individual's duties as an APS employee
4	an employee, officer or member of the entity not covered by item 2 or 3	the individual's employment or authority
5	an individual who is party to an approved contract with the entity, or an employee, officer or member of a body corporate that is party to an approved contract with the entity	the individual or body corporate's contract with the entity
6	an individual who is an agent appointed by the entity, or an employee, officer or member of a person that is an agent appointed by the entity	the individual or person's authority as an agent

- (2) If, for an individual to whom item 1 of the table in subsection (1) applies, any of items 2, 3 or 4 of the table also apply, the individual has the designation specified for each applicable item.

## Section 124

---

- (3) An individual or body corporate's contract with an entity is an **approved contract** if:
- (a) the entity is an accredited entity and party to a data sharing agreement; and
  - (b) the contract is authorised by, or approved under, the data sharing agreement in accordance with any requirements in a data code.

### 124 Extension of authorisations to share, collect or use data

#### *Designated individuals*

- (1) An authorisation in Chapter 2 for an entity to share, collect or use data also authorises a designated individual for the entity to engage in conduct that is, or is part of, the sharing, collection or use, if the conduct is within the actual scope of the individual's designation.
- (2) Subsection (1) does not apply to conduct of an individual if either of the following has the effect that the individual may not engage in such conduct:
  - (a) conditions of accreditation imposed on or applicable to the entity;
  - (b) the data sharing agreement that covers the sharing, collection or use.

#### *Bodies corporate*

- (3) An authorisation in Chapter 2 for an accredited entity to collect or use data also authorises a body corporate that is party to an approved contract with the accredited entity to engage in conduct that is, or is part of, the collection or use, if the conduct is within the actual scope of the approved contract.
- (4) Subsection (3) does not apply to conduct of a body corporate if either of the following has the effect that the body corporate may not engage in such conduct:
  - (a) conditions of accreditation imposed on or applicable to the entity;
  - (b) the approved contract;

- (c) the data sharing agreement for the project to which the collection or use relates.

*Access to data by designated individuals and certain bodies corporate*

- (5) If a designated individual for an entity, or a body corporate that is party to an approved contract with an entity, is given access to data by the entity, and the access is within the actual scope of the individual's designation or the body corporate's approved contract, giving the access is taken, for the purposes of the data sharing scheme, to be a use of the data, but not a provision of access to it.

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

- (1) If an entity may or must do something under the data sharing scheme, the thing may be done, for the entity, by any designated individual for the entity, if doing the thing is within the actual or apparent scope of the individual's designation.
- (2) Subsection (1) does not apply in relation to the authorisations in Chapter 2 to which section 124 applies, or in relation to things that may or must be done by an authorised officer or an officer authorised under subsection 137(3) or (4).

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

*Conduct attributed to entity*

- (1) In determining whether an entity has contravened a civil penalty provision of this Act, or otherwise breached this Act:
  - (a) the entity is taken to have engaged in any conduct engaged in:
    - (i) by a designated individual for the entity, if the conduct is within the actual or apparent scope of the individual's designation; or

## Section 125A

---

- (ii) by a body corporate that is party to an approved contract with the entity, if the conduct is within the actual or apparent scope of the approved contract; and
  - (b) if it is necessary to establish the entity's state of mind, it is sufficient to establish the state of mind of an individual who has engaged in conduct as mentioned in subparagraph (a)(i).
- (2) Despite subsection (1), a government entity does not contravene a civil penalty provision of this Act because of conduct that is attributed to the entity under subsection (1), if the entity took reasonable precautions and exercised due diligence to avoid the conduct.

Note: The government entity bears an evidential burden in relation to the matter in subsection (2) (see section 96 of the Regulatory Powers Act).
- (3) An individual whose conduct is attributed to a government entity under subsection (1) is not personally liable for a contravention of a civil penalty provision (including an ancillary contravention) in relation to the conduct.
- (4) Any of the following is a **government entity**:
  - (a) a Commonwealth body;
  - (b) a State body, or a Territory body, that is not a body corporate;
  - (c) the Commonwealth, a State or a Territory.

### *Interaction with Regulatory Powers Act*

- (5) Section 97 of the Regulatory Powers Act does not apply in relation to a body corporate that is a Commonwealth body (subsection (1) of this section applies instead).
- (6) Subsection (1) does not apply in relation to determining whether a body corporate that is not a Commonwealth body has contravened a civil penalty provision (section 97 of the Regulatory Powers Act applies instead).



Section 125B

---

**125B Offences by entities against this Act**

In determining whether an entity has committed an offence against this Act:

- (a) the entity is taken to have engaged in any conduct engaged in:
  - (i) by a designated individual for the entity, if the conduct is within the actual or apparent scope of the individual's designation; or
  - (ii) by a body corporate that is party to an approved contract with the entity, if the conduct is within the actual or apparent scope of the approved contract; and
- (b) if it is necessary to establish the entity's state of mind, it is sufficient to establish the state of mind of an individual who has engaged in conduct as mentioned in subparagraph (a)(i).

Note 1: Part 2.5 of the *Criminal Code* deals with criminal responsibility of bodies corporate.

Note 2: The Crown is not liable to be prosecuted for an offence.

## Part 6.4—Data sharing scheme instruments

### 126 Data codes

- (1) The Commissioner may, by legislative instrument, make codes of practice about the data sharing scheme (*data codes*).
- (2) Without limiting what a data code may do, it may do any of the following:
  - (a) set out how the definitions in sections 9, 10, 11 and 11A, and provisions of Chapters 2 and 3, are to be applied or complied with;
  - (b) impose additional requirements to those imposed by Chapters 2 and 3, so long as the additional requirements are not contrary to, or inconsistent with, those Chapters;
  - (c) deal with the internal handling of complaints;
  - (d) deal with the management of complaints under Part 5.3 and impose additional requirements to those set out in that Part, so long as the additional requirements are not contrary to, or inconsistent with, that Part;
  - (e) deal with any other matters the Commissioner considers necessary or convenient to deal with for carrying out or giving effect to the data sharing scheme.
- (2A) The Commissioner must make one or more data codes about:
  - (a) the data sharing principles in section 16; and
  - (b) the general privacy protections in section 16A; and
  - (c) the purpose-specific privacy protections in section 16B.
- (2B) A data code about the general privacy protections in section 16A must deal with consent by individuals to the sharing of their personal information.
- (2C) A data code about the purpose-specific privacy protections in section 16B must deal with the following:

---

Section 127

---

- (a) consent by individuals to the sharing and use of their personal information and circumstances in which it is unreasonable or impracticable to seek individuals' consent;
  - (b) principles to be applied by data custodians when determining:
    - (i) whether it is necessary to share personal information to properly deliver a government service; or
    - (ii) the circumstances, or categories of circumstances, where the public interest to be served by a project justifies the sharing of personal information without consent.
- (3) A data code that is inconsistent with the regulations or rules has no effect to the extent of the inconsistency, but a data code is taken to be consistent with the regulations and rules to the extent that the data code is capable of operating concurrently with them.

### 127 Guidelines

- (1) The Commissioner may, by legislative instrument, make written guidelines in relation to matters for which the Commissioner has functions under this Act.
- Note: Data scheme entities must have regard to the guidelines when engaging in conduct for the purposes of this Act (see section 27).
- (2) The guidelines may include principles and processes relating to:
- (a) any aspect of the data sharing scheme; and
  - (b) any matters incidental to the data sharing scheme, including:
    - (i) data release; and
    - (ii) data management and curation; and
    - (iii) technical matters and standards; and
    - (iv) emerging technologies.
- (3) Guidelines that are inconsistent with the regulations, rules or data codes have no effect to the extent of the inconsistency, but guidelines are taken to be consistent with those instruments to the extent that the guidelines are capable of operating concurrently with them.

Section 128

---

**128 Register of ADSPs**

- (1) The Commissioner must maintain a register of ADSPs. The register must include a publicly accessible part and may include a part that is not publicly accessible.
- (2) Subject to subsection (4), the Commissioner must include in the part of the register that is publicly accessible the following details for each ADSP:
  - (a) the name of the ADSP;
  - (b) contact details for the ADSP;
  - (c) conditions of the ADSP's accreditation;
  - (d) at any time while the ADSP's accreditation is suspended—the duration of the suspension (which may be indefinite);
  - (e) any other details prescribed by the rules to be included in the publicly accessible part of the register.
- (3) The rules may prescribe circumstances in which details mentioned in paragraph (2)(a), (b) or (c) must not be included in the publicly accessible part of the register.
- (4) The Commissioner must include in the part of the register that is not publicly accessible any details:
  - (a) prescribed for the purposes of subsection (3); or
  - (b) prescribed by the rules to be included in the part of the register that is not publicly accessible.
- (5) The register may be maintained in any form the Commissioner considers appropriate.
- (6) The register is not a legislative instrument.

**129 Register of accredited users**

- (1) The Commissioner must maintain a register of accredited users. The register must include a publicly accessible part and may include a part that is not publicly accessible.

- (2) Subject to subsection (4), the Commissioner must include in the part of the register that is publicly accessible the following details for each accredited user:
  - (a) the name of the accredited user;
  - (b) contact details for the accredited user;
  - (c) conditions of the accredited user's accreditation;
  - (d) at any time while the accredited user's accreditation is suspended—the duration of the suspension (which may be indefinite);
  - (e) any other details prescribed by the rules to be included in the publicly accessible part of the register.
- (3) The rules may prescribe circumstances in which details mentioned in paragraph (2)(a), (b) or (c) must not be included in the publicly accessible part of the register.
- (4) The Commissioner must include in the part of the register that is not publicly accessible any details:
  - (a) prescribed for the purposes of subsection (3); or
  - (b) prescribed by the rules to be included in the part of the register that is not publicly accessible.
- (5) The register may be maintained in any form the Commissioner considers appropriate.
- (6) The register is not a legislative instrument.

### **130 Register of data sharing agreements**

- (1) The Commissioner must maintain a register of data sharing agreements. The register must include a publicly accessible part and a part that is not publicly accessible.
- (2) Subject to subsection (4), the Commissioner must include in the part of the register that is publicly accessible the following details in relation to each registered data sharing agreement:
  - (a) the entities that are parties and the capacity in which each entity is a party;
  - (b) the date the parties entered into the agreement;

Section 130

---

- (c) the date the Commissioner registered the agreement;
  - (d) a description of the project the agreement covers;
  - (e) the data sharing purpose of the project;
  - (f) a description of the data to be shared;
  - (g) whether personal information is to be shared;
  - (h) if personal information is to be shared—a statement in the approved form (if any) relating to the privacy obligations applicable to the accredited user in relation to its use of output of the project and the person or body to whom individuals may complain about use inconsistent with those obligations;
  - (i) if subsection 16B(7) applies in relation to the agreement—a copy of the statement and explanation required by that subsection;
  - (j) if subsection 16B(8) applies in relation to the agreement—a copy of the statement required by that subsection;
  - (k) if, but for section 23, sharing, collecting or using data under the agreement would contravene another law—the title of the other law;
  - (l) a statement of how the project will serve the public interest;
  - (m) a description of the final output of the project;
  - (n) if output of the project may exit the data sharing scheme under section 20E—the circumstances in which the exit may occur;
  - (o) if the agreement has an expiry date—the expiry date;
  - (p) whether the agreement is in effect or has expired or been terminated;
  - (q) if any details are affected by a variation of the agreement—the details as varied and the date the variation was registered;
  - (r) any other details prescribed by the rules to be included in the publicly accessible part of the register.
- (3) The rules may prescribe circumstances in which details mentioned in subsection (2) must not be included in the publicly accessible part of the register.
- (4) The Commissioner must include in the part of the register that is not publicly accessible:
-

---

Section 131

---

- (a) copies of data sharing agreements and variations given to the Commissioner under section 33; and
  - (b) any details prescribed for the purposes of subsection (3); and
  - (c) any details prescribed by the rules to be included in the part of the register that is not publicly accessible.
- (5) The register may be maintained in any form the Commissioner considers appropriate.
- (6) The register is not a legislative instrument.

### **131 Recognition of external dispute resolution schemes**

- (1) The Commissioner may, by written notice, recognise an external dispute resolution scheme for:
  - (a) a data scheme entity or a class of data scheme entities; or
  - (b) a specified purpose.
- (2) In considering whether to recognise an external dispute resolution scheme, the Commissioner:
  - (a) must take the following aspects of the scheme into account:
    - (i) accessibility;
    - (ii) independence;
    - (iii) fairness;
    - (iv) accountability;
    - (v) efficiency;
    - (vi) effectiveness; and
  - (b) may take into account any other matter the Commissioner considers relevant.
- (3) The Commissioner may:
  - (a) specify a period for which the recognition of an external dispute resolution scheme is in force; and
  - (b) make the recognition of an external dispute resolution scheme subject to specified conditions, including conditions relating to the conduct of an independent review of the operation of the scheme; and
  - (c) vary or revoke:

## Section 132

---

- (i) the recognition of an external dispute resolution scheme; or
  - (ii) the period for which the recognition is in force; or
  - (iii) a condition to which the recognition is subject.
- (4) A notice under subsection (1) is not a legislative instrument.

### **132 Approved forms**

The Commissioner may, by writing, approve a form for the purposes of a provision of the data sharing scheme.

### **133 Rules**

- (1) The Minister may, by legislative instrument, make rules prescribing matters:
  - (a) required or permitted by this Act to be prescribed by the rules; or
  - (b) necessary or convenient to be prescribed for carrying out or giving effect to this Act.
- (2) To avoid doubt, the rules may not do the following:
  - (a) create an offence or civil penalty;
  - (b) provide powers of:
    - (i) arrest or detention; or
    - (ii) entry, search or seizure;
  - (c) impose a tax;
  - (d) set an amount to be appropriated from the Consolidated Revenue Fund under an appropriation in this Act;
  - (e) directly amend the text of this Act.
- (3) Rules that are inconsistent with the regulations have no effect to the extent of the inconsistency, but rules are taken to be consistent with the regulations to the extent that the rules are capable of operating concurrently with the regulations.

### **134 Regulations**

The Governor-General may make regulations prescribing matters:

---



Section 134

---

- (a) required or permitted by this Act to be prescribed by the regulations; or
- (b) necessary or convenient to be prescribed for carrying out or giving effect to this Act.

## Part 6.5—Other matters

### 135 Disclosure of scheme data in relation to information-gathering powers

A data scheme entity is authorised to disclose scheme data held by the entity:

- (a) to the Auditor-General, if the disclosure is required under the *Auditor-General Act 1997*; or
- (b) to the Commonwealth Ombudsman, if the disclosure is requested or required under the *Ombudsman Act 1976*; or
- (c) to the Information Commissioner, if the disclosure is required under the *Freedom of Information Act 1982* or the *Privacy Act 1988*; or
- (d) to a court or tribunal of the Commonwealth or a State or Territory, or a Royal Commission (within the meaning of the *Royal Commissions Act 1902*), that orders or directs the disclosure.

Note 1: Except as authorised by this section, data scheme entities must not provide access to scheme data unless authorised to do so by Chapter 2 or by a direction under section 112.

Note 2: Section 23 (authorisations override other laws) applies only in relation to provision of access to data authorised by Chapter 2.

### 135A Data held by National Archives of Australia

*Before the open access period*

- (1) Where public sector data is transferred by its data custodian to the National Archives of Australia before the start of the open access period (within the meaning of the *Archives Act 1983*) in relation to the data, then, for the purposes of this Act and until the start of the open access period in relation to the data:
  - (a) the data custodian continues to be the data custodian of the data; and

---

Section 136

- (b) the National Archives of Australia is not a data custodian of the data.
- (2) Subsection (1) has effect despite anything in the definition of ***data custodian*** in subsection 11(2).

*Records in the open access period*

- (3) An authorisation in Chapter 2 does not apply in relation to sharing, collecting or using a record in the open access period, unless the sharing, collection or use is part of a project covered by a data sharing agreement registered before the start of the open access period.

Note: Records that are in the open access period may be accessed under the *Archives Act 1983*.

### **136 Geographical jurisdiction of civil penalty provisions and offences**

*Geographical jurisdiction of offences and civil penalty provisions*

- (1) A person does not contravene a civil penalty provision of this Act, or commit an offence against this Act, unless at least one of the following paragraphs applies in relation to the conduct constituting the alleged contravention or offence:
  - (a) the conduct, or a result of the conduct, occurs wholly or partly in Australia, or on board an Australian aircraft or Australian ship;
  - (b) for conduct alleged to constitute an ancillary contravention—the conduct, or a result of the conduct, that would constitute the primary contravention to which the ancillary contravention relates would have occurred wholly or partly in a place covered by paragraph (a);
  - (c) for conduct alleged to constitute an ancillary offence—the conduct, or a result of the conduct, that would constitute the primary offence to which the ancillary offence relates was intended by the person to occur wholly or partly in a place covered by paragraph (a);

Section 136

---

- (d) the conduct occurs wholly outside Australia and the person engaging in the conduct is an Australian entity, an Australian citizen or a permanent resident of Australia.

*Defence for primary contravention or primary offence*

- (2) Despite subsection (1), a person does not contravene a civil penalty provision of this Act, or commit an offence against this Act, if:
  - (a) the alleged contravention or offence is a primary contravention or primary offence; and
  - (b) the conduct constituting the alleged contravention or offence occurs wholly in a foreign country, but not on board an Australian aircraft or Australian ship; and
  - (c) the person is not an Australian entity, an Australian citizen or a permanent resident of Australia; and
  - (d) there is not in force, in the foreign country or the part of the foreign country where the conduct constituting the alleged contravention or offence occurred, a law creating a pecuniary or criminal penalty for conduct corresponding to the conduct constituting the alleged contravention or offence.

*Defence for ancillary contravention or ancillary offence*

- (3) Despite subsection (1), a person does not contravene a civil penalty provision of this Act, or commit an offence against this Act, if:
  - (a) the alleged contravention or offence is an ancillary contravention or ancillary offence; and
  - (b) for conduct constituting an alleged contravention—the conduct constituting the primary contravention to which the alleged contravention relates, or a result of that conduct, occurs, or would have occurred, wholly in a foreign country, but not on board an Australian aircraft or Australian ship; and
  - (c) for conduct constituting an alleged offence—the conduct constituting the primary offence to which the alleged offence relates, or a result of that conduct, occurs, or was intended by the person to occur, wholly in a foreign country, but not on board an Australian aircraft or Australian ship; and
  - (d) the person is not an Australian entity, an Australian citizen or a permanent resident of Australia; and

Section 136

---

- (e) there is not in force, in the foreign country or the part of the foreign country where the conduct constituting the alleged contravention or offence occurred, a law creating a pecuniary or criminal penalty for conduct corresponding to the conduct constituting the primary contravention or primary offence to which the alleged contravention or offence relates.
- (4) A person who is alleged to have contravened a civil penalty provision of this Act and who wishes to rely on subsection (2) or (3) bears an evidential burden (within the meaning of the *Criminal Code*) in relation to the matters set out in the subsection.
- (5) For the purposes of the application of subsection 13.3(3) of the *Criminal Code* to an offence against this Act, subsections (2) and (3) of this section are taken to be exceptions provided by the law creating the offence.

Note: This means that a defendant bears an evidential burden in relation to the matters in subsections (2) and (3).

*Other matters*

- (6) Division 14 of the *Criminal Code* (standard geographical jurisdiction) does not apply in relation to an offence against this Act (this section applies instead).
- (7) A reference in this section to a result of conduct is a reference to a result that is an element of the civil penalty provision or offence.
- (8) For the purposes of this section and without limitation, if a person sends, or causes to be sent, an electronic communication or other thing:
  - (a) from a point outside Australia to a point in Australia; or
  - (b) from a point in Australia to a point outside Australia;that conduct is taken to have occurred partly in Australia.
- (9) A **point** includes a mobile or potentially mobile point, whether on land, underground, in the atmosphere, underwater, at sea or anywhere else.

Section 137

**137 Authorised officers and individuals authorised to do particular things**

- (1) An individual is an **authorised officer** of an entity if the individual is specified in paragraph (a) of the column headed “Individuals” in an item in the following table, or authorised under subsection (2), in relation to the entity.

Note: An individual may also be authorised under subsection (3) or (4) to do particular things. These individuals are authorised to do those things but are not **authorised officers**.

Authorised officers and individuals authorised to do particular things		
Item	Kind of entity	Individuals
1	Any of the following: (a) a Department; (b) an Executive Agency within the meaning of the <i>Public Service Act 1999</i> ; (c) a Statutory Agency within the meaning of the <i>Public Service Act 1999</i>	The following: (a) the Agency Head within the meaning of the <i>Public Service Act 1999</i> ; (b) an SES employee, or an acting SES employee, in the entity authorised by the Agency Head under subsection (2), (3) or (4); (c) an SES employee, or an acting SES employee, in another Department, Executive Agency or Statutory Agency authorised by the Agency Head under subsection (4)
2	Any of the following: (a) a corporate Commonwealth entity within the meaning of the <i>Public Governance, Performance and Accountability Act 2013</i> ; (b) a Commonwealth company within the meaning of the <i>Public Governance, Performance and Accountability Act 2013</i>	The following: (a) the chief executive officer (however described) of the entity; (b) an individual authorised by the chief executive officer under subsection (2) or (3)
3	A person who is a prescribed authority within the meaning of	The following: (a) the person;

Section 137

<b>Authorised officers and individuals authorised to do particular things</b>		
<b>Item</b>	<b>Kind of entity</b>	<b>Individuals</b>
	paragraph (c) or (d) of the definition of <i>prescribed authority</i> in subsection 4(1) of the <i>Freedom of Information Act 1982</i> and not covered by item 1 or 2	(b) a person authorised by that person under subsection (2) or (3)
4	A State body or a Territory body that is the holder of a statutory office	The following: (a) the holder of the statutory office; (b) a person authorised by the holder of the statutory office under subsection (2) or (3)
5	A State body or a Territory body other than the holder of a statutory office	The following: (a) the chief executive officer (however described) of the body; (b) a person authorised by the chief executive officer under subsection (2) or (3)
6	A body corporate not covered by any other item	The following: (a) the chief executive officer (however described) of the entity and any director of the entity; (b) an employee of the entity authorised by the chief executive officer under subsection (2) or (3)
7	A body politic not covered by any other item	The following: (a) the chief Minister (however described); (b) a person authorised by the chief Minister under subsection (2) or (3)

Note: The expressions **SES employee** and **acting SES employee** are defined in the *Acts Interpretation Act 1901*.

(2) If an item of the table in subsection (1) refers to an individual (the **authoriser**) authorising another individual under this subsection,

## Section 137A

---

the authoriser may, by written instrument, authorise the other individual to be an authorised officer for the purposes of the data sharing scheme.

Note: An individual authorised under this subsection is an **authorised officer** (see subsection (1)).

- (3) If an item of the table in subsection (1) refers to an individual (the **authoriser**) authorising another individual under this subsection, the authoriser may, by written instrument, authorise the other individual to enter into variations to data sharing agreements for the entity.
- (4) If an item of the table in subsection (1) refers to an individual (the **authoriser**) authorising another individual under this subsection, the authoriser may, by written instrument, authorise the other individual to do all of the following for the entity:
  - (a) enter into data sharing agreements;
  - (b) enter into variations to data sharing agreements;
  - (c) make decisions that subsection 16D(4) applies to a proposed integration of data and make the required records under subsection 16D(6).

### 137A Delegation by Minister

- (1) The Minister may, in writing, delegate any or all of the Minister's powers under Part 5.2 to the Commissioner.

Note: Sections 34AA to 34A of the *Acts Interpretation Act 1901* contain provisions relating to delegations.

- (2) In exercising a delegated power, the Commissioner must comply with any written directions of the Minister.

### 138 Annual report

- (1) After the end of each financial year, the Commissioner must prepare and give a report to the Minister, for presentation to the Parliament, on the Commissioner's activities during the financial year.



- (2) The report must include the following in relation to the financial year:
- (a) information about legislative instruments and guidelines made by the Commissioner under this Act;
  - (b) information about activities undertaken for the purposes of the regulatory functions set out in section 45;
  - (c) a description of any efforts made by the Commissioner to assist data scheme entities to comply with the requirements of the data sharing scheme;
  - (d) a statement of the following:
    - (i) the number of requests received by data custodians of public sector data from accredited users for sharing of data under this Act and information about the reasons for requests being agreed to or refused;
    - (ia) the number of such requests refused by data custodians where reasons for the refusal were not given within the time required by subsection 25(3);
    - (ii) the number of data sharing agreements made;
    - (iii) the number of entities accredited;
    - (iv) the number of accredited entities as at the end of the financial year;
    - (v) the number of complaints received by the Commissioner under Division 1 of Part 5.3 (scheme complaints);
    - (vi) the number of complaints received by the Commissioner under Division 2 of Part 5.3 (general complaints);
    - (vii) the number of complaints received by data custodians relating to the data sharing scheme or a data custodian's conduct in relation to the data sharing scheme;
  - (e) information about the activities of the National Data Advisory Council;
  - (f) information about the number of APS employees made available to the Commissioner as mentioned in section 47;
  - (g) a report on financial matters, including a discussion and analysis of the financial resources available to the Commissioner in the financial year and how they were used.

## Section 139

---

Note: The Commissioner may require data scheme entities to give information and assistance for the purposes of preparing the report (see section 34).

- (3) The report may include any other information relating to the operation of the data sharing scheme that the Commissioner considers appropriate.
- (4) The report must be given to the Minister by the 15th day of the fourth month after the end of the financial year, or by the end of any further period granted under subsection 34C(5) of the *Acts Interpretation Act 1901*.

### **139 Charging of fees by Commissioner**

- (1) The rules may prescribe fees to be charged by the Commissioner for services provided by or on behalf of the Commissioner, or for or on behalf of the Minister in the Minister's capacity as an accreditation authority for an entity, in performing or exercising functions or powers under this Act, the rules or the data codes.
- (2) Without limiting subsection (1), the rules may provide for the amount of a fee to be the cost incurred by the Commonwealth in arranging and paying for another person to perform functions or exercise powers.
- (3) A fee prescribed by the rules is payable to the Commonwealth.
- (4) The rules may make provision for:
  - (a) when and how fees are payable;
  - (b) any other matters in relation to fees including exemptions, refunds and remissions.
- (5) If a fee is payable for a service, the service need not be provided while the fee remains unpaid. The rules may provide for the extension of any times for providing services accordingly.

### **140 Charging of fees by data scheme entities**

- (1) A data custodian of public sector data may charge fees to an accredited entity for services performed by or on behalf of the data

## Section 141

---

custodian in dealing with a request by the accredited entity for data to be shared under this Act.

- (2) A data custodian that charges fees must do so in a way that is not inconsistent with the policies of the Australian Government.
- (3) Nothing in this section has the effect of preventing an accredited entity (including a Commonwealth body) from charging fees in relation to services it performs in relation to the data sharing scheme.

### 141 Commonwealth not liable to pay a fee

- (1) The Commonwealth is not liable to pay a fee that is payable under this Act. However, it is the Parliament's intention that the Commonwealth should be notionally liable to pay such a fee.
- (2) The Finance Minister may give such written directions as are necessary or convenient for carrying out or giving effect to subsection (1) and, in particular, may give directions in relation to the transfer of money within an account, or between accounts, operated by the Commonwealth.
- (3) Directions under subsection (2) have effect, and must be complied with, despite any other Commonwealth law.
- (4) In subsections (1) and (2), **Commonwealth** includes a Commonwealth entity (within the meaning of the *Public Governance, Performance and Accountability Act 2013*) that cannot be made liable to taxation by a Commonwealth law.

### 142 Periodic reviews of operation of Act

- (1) The Minister must cause periodic reviews of the operation of this Act to be undertaken.
- (2) A review must start by, and be completed within 12 months (or a longer period agreed by the Minister) of:
  - (a) the third anniversary of the commencement of this section; and

## Section 143

---

- (b) the day that is 3 months after the commencement of any amendments of the *Privacy Act 1988* that:
    - (i) are made in response to the review of that Act announced by the Attorney-General on 12 December 2019; and
    - (ii) in the Minister's opinion, are likely to have a material impact on the data sharing scheme.
- (3) If subsection (2) would have the effect that a review must start before another review is completed:
  - (a) the reviews may be combined; and
  - (b) the combined review must be completed within 12 months (or a longer period agreed by the Minister) of the day the latest of the reviews was required to start.
- (4) The Minister must cause a written report about each review to be prepared. A review is taken to be completed when the Minister is given the report about the review.
- (5) The Minister must cause a copy of the report about each review to be laid before each House of the Parliament within 15 sitting days of that House after the Minister receives the report.

### 143 Sunset of the data sharing scheme

- (1) Subject to this section, this Act ceases to have effect at the end of the day (the ***sunset day***) that is the fifth anniversary of the commencement of this section.

Note: Section 7 of the *Acts Interpretation Act 1901* (effect of repeal or amendment of Act) applies in relation to this section.
- (2) Despite subsection (1), regulations may be made under section 134 for the purposes of subsection (3) of this section at any time during the period starting 12 months before the sunset day and ending immediately before the first anniversary of the sunset day.
- (3) The regulations may, for the purposes of ensuring that scheme data is appropriately dealt with, prescribe matters of a transitional nature relating to this Act ceasing to have effect under subsection (1), including:

Section 143

---

- (a) prescribing any saving or application provisions; and
  - (b) the matters set out in subsections (4) to (7).
- (4) The regulations may provide that certain provisions of this Act continue to apply, or to apply in a modified way, after the sunset day, for the purposes set out in the regulations. Those provisions continue to apply, or continue to apply in the modified way, as set out in the regulations.

Note: For example, the regulations may continue in existence the Commissioner and the Council.
- (5) The regulations may empower the Commissioner to give a data scheme entity, or an entity that was a data scheme entity before the sunset day, a written direction requiring the entity to take, or not to take, specified actions in order to ensure that scheme data is appropriately dealt with in connection with this Act ceasing to have effect.
- (6) The regulations may create offences or civil penalties for failure to comply with a direction mentioned in subsection (5).
- (7) The regulations may prescribe:
  - (a) penalties, not exceeding 50 penalty units for individuals and entities other than bodies corporate or 250 penalty units for bodies corporate, for offences against the regulations; and
  - (b) civil penalties, not exceeding 300 penalty units for individuals and entities other than bodies corporate or 1,500 penalty units for bodies corporate, for contraventions of the regulations.
- (8) Regulations made for the purposes of subsection (3) of this section must not have the effect of allowing data to be shared under section 13 (authorisation for data custodian to share public sector data) after the sunset day.
- (9) All legislative instruments made under this Act (including regulations made for the purposes of subsection (3) of this section) are repealed on the first anniversary of the sunset day.

---

*[Minister's second reading speech made in—  
House of Representatives on 9 December 2020  
Senate on 30 March 2022]*

(174/20)