Western Australia

Privacy and Responsible Information Sharing Act 2024

As at 01 Jul 2026 Official Version
[PCO 00-g0-03] Published on www.legislation.wa.gov.au

Western Australia

Privacy and Responsible Information Sharing Act 2024

Contents

Part 1 — Preliminary

1. Short title 2
2. Commencement 2
3. Objects 2
4. Terms used 3
5. References to information privacy principles 17
6. Public entities 17
7. Judicial bodies 19
8. State services contracts and contracted service providers 19
9. Principal officers 20
10. Disclosure by public entities and other IPP entities 21
11. De-identification and re-identification of information 21
12. Data sets, data analytics work, data linkage and data integration 22
13. Act binds Crown 22

Part 2 — Privacy

Division 1 — Key concepts and preliminary matters

14. IPP entities 23
15. Interferences with privacy 23
16. Automated decision-making processes and related concepts 24
17. Entities to which privacy obligations do not apply 25

18. Application of privacy obligations to judicial bodies 25

Division 2 — Information privacy principles

19. Information privacy principles 26
20. IPP entities must comply with information privacy principles 26
21. Exception: personal, family or household affairs 26
22. Exception: publicly available information 26
23. Exception: law enforcement functions 27
24. Exception: emergency response functions 27
25. Exception: child protection functions 28
26. Exception: family violence 28
27. Exception: IPP entities to which IPP 6 does not apply 28

Division 3 — Privacy codes of practice

28. Privacy code of practice 29
29. IPP entity may prepare and submit privacy code of practice or amendment 30
30. Commissioner may prepare privacy code of practice or amendment 30
31. Public consultation on privacy code of practice or amendment 31
32. Submission and approval of privacy code of practice or amendment 32
33. Effect of approved privacy code of practice 32
34. Revocation of approved privacy code of practice 34
35. Approved privacy code of practice or amendment is disallowable subsidiary legislation 35
36. Duration of approved privacy code of practice 36
37. Register of approved privacy codes of practice 36
38. Commissioner may review approved privacy code of practice 37

Division 4 — Requests for access to and correction of personal information

39. Purpose of Division 37
40. Request for access under IPP 6.1 or approved privacy code of practice 37
41. Request for correction under IPP 6.5 or approved privacy code of practice 38

42. IPP entity to provide assistance in making request 39
43. Protection from liability for providing access to information 39
44. Certain applications under *Freedom of Information Act 1992* taken to be requests under IPP 6 or approved privacy code of practice 40

Division 5 — Public interest determinations and temporary public interest determinations

Subdivision 1 — Public interest determinations

45. Public interest determination 41
46. Application for public interest determination 42
47. Procedure to be followed on application for public interest determination 42
48. Reporting on and review of determination 45

Subdivision 2 — Temporary public interest determinations

49. Temporary public interest determination 45
50. Application for temporary public interest determination 46
51. Procedure to be followed on application for temporary public interest determination 47
52. Extension of temporary public interest determination 48

Subdivision 3 — General provisions about public interest determinations and temporary public interest determinations

53. Effect of determination 48
54. Revocation of determination 49
55. Determination is disallowable subsidiary legislation and statement of reasons required 50
56. Duration of determination 51

Division 7 — Personal information in public registers

76. Disclosure of personal information in public registers 52
77. Removal of personal information affecting individual's safety or wellbeing 52
78. Interaction with written laws establishing public registers 53

Division 8 — Privacy impact assessments

79. Privacy impact assessment relating to high privacy impact function or activity 53
80. Commissioner may direct privacy impact assessment 54
81. Guidelines about significant impact on privacy 55

Division 9 — Privacy complaints

Subdivision 1 — Making a privacy complaint

82. Individual may complain about interference with privacy 55
83. Complaint on behalf of 2 or more individuals 56
84. Complaint by or on behalf of child 56
85. Complaint on behalf of individual with disability 57
86. Matter referred by Ombudsman may be treated as privacy complaint 57
87. Complaint referred by Health and Disability Complaints Office Director may be treated as privacy complaint 58

Subdivision 2 — Procedure after complaint is made

88. Notice of complaint 58
89. Withdrawal of complaint 58
90. Commissioner may decline to deal with complaint 58
91. Commissioner may decline to continue dealing with complaint 60
92. Commissioner may deal with complaint under *Freedom of Information Act 1992* 61
93. Commissioner may refer complaint to other authority 61

Subdivision 3 — Parties may resolve complaint

94. Parties may resolve complaint 63

Subdivision 4 — Conciliation of complaints

95. Commissioner must attempt to resolve complaint by conciliation 64
96. Procedure for conciliation 64
97. Representation in conciliation process 65
98. Conciliation agreement 65
99. Notice of complaint that cannot be resolved by conciliation 66
100. Statements made in conciliation protected 67

Subdivision 5 — Dealing with complaint not resolved by conciliation

101. Commissioner may deal with complaint not resolved by conciliation 67
102. General matters about dealing with complaints 67
103. Referral of question of law to Supreme Court 68
104. Determination of complaint 69
105. Review of determination 70

Division 10 — Investigations and enforcement

Subdivision 1 — Investigations of acts or practices that may be interferences with privacy

106. Commissioner may investigate act or practice that may be interference with privacy 71
107. Determination following investigation 71
108. Review of determination 72
109. Reports 73

Subdivision 2 — Monitoring and assessment of compliance

110. Commissioner may monitor or conduct assessment of compliance 73
111. Reports 74

Subdivision 3 — Notices to produce or attend

112. Purposes for exercise of powers 74
113. Notice to produce or attend 75
114. Contents of notice to produce or attend 76
115. Variation or withdrawal of notice to produce or attend 76
116. Powers of Commissioner in relation to persons attending and documents 76
117. Failure to comply with notice to produce or attend 77

Subdivision 5 — Compliance notices

122. Issue of compliance notice 78
123. IPP entity must comply with compliance notice 79
124. Review of decision to issue compliance notice 80

Subdivision 6 — Enforcement of orders made by Commissioner

125. Enforcement of orders requiring payment of compensation 80
126. Enforcement of other orders 80

127. Deferral of enforcement until review proceedings concluded 81

Division 11 — Contracted service providers

128. Purpose of Division 81
129. State services contract may provide for application of privacy obligations 81
130. Application of information privacy principles and approved privacy codes of practice to contracted service providers 82
131. Privacy codes of practice or amendments submitted by contracted service providers 82
132. Requests for access and correction made to contracted service providers 83
133. Public interest determinations and temporary public interest determinations applying to contracted service providers 83
137. Privacy impact assessments by contracted service providers 84
138. Directions about privacy impact assessments given to contracted service providers 85
139. Notices relating to privacy complaints or investigations about contracted service providers 85
140. Enforcement action may be taken against outsourcing entity in some circumstances 86

Division 12 — Administration

Subdivision 1 — Functions under this Act of Information Commissioner and Privacy Deputy Commissioner

141. Functions of Information Commissioner and Privacy Deputy Commissioner under this Act 88
142. Performance of privacy functions 89
143. Certain functions cannot be delegated 91
144. Information Commissioner and Privacy Deputy Commissioner must have regard to objects of Act in performing functions 92
145. Information Commissioner and Privacy Deputy Commissioner may request IPP entity to provide assistance 92

Subdivision 2 — Reporting
146. Matters to be included in annual report to Parliament 92
147. Special reports to Parliament 93
Subdivision 3 — Guidelines, documents and notices
148. Privacy guidelines 94
149. Making documents publicly available 94
150. Notices of decisions or determinations 95
Division 13 — General
151. Privacy officers of public entities 95
152. Nature of privacy rights created by this Act 96
153. Interaction with other laws 97
154. Exercise of powers relating to consent and access by authorised representative of individual 98
155. Review of privacy provisions of Act 100

Part 3 — Responsible information sharing

Division 1 — Key concepts and preliminary matters
156. Special information sharing entities and external entities 102
157. Government information 103
158. Exempt information 103
159. Permitted purposes for sharing of information 108
Division 2 — Information sharing requests
160. Information sharing request 109
161. Response to information sharing request 110
162. No obligation to disclose requested information 111
Division 3 — Information sharing directions
163. Responsible Minister for public entity may direct sharing of information 112
164. Notice of direction must be laid before Houses of Parliament 114
165. Revocation of direction 115
166. Requirement to comply with direction 115
167. Division has effect subject to laws restricting Ministerial direction 115

Division 4 — Information sharing agreements

Subdivision 1 — Entry into and contents of information sharing agreement

168. Information sharing agreement 116
169. Entering into information sharing agreement 117
170. Matters to be included in information sharing agreement 117
171. Other matters to be included in information sharing agreement 119
172. Information sharing agreement may provide for limited further disclosure 120
173. Other matters that may be dealt with in information sharing agreement 120
174. Activities under information sharing agreement may include data analytics work, data integration and data linkage 121

Subdivision 2 — Assessments to be conducted before entering into information sharing agreement

175. Assessment of responsible sharing principles 121
176. Privacy impact assessment 122
177. Aboriginal information assessment 123

Subdivision 3 — Other provisions about information sharing agreements

178. Duration of information sharing agreement 125
179. Variation of information sharing agreement 126
180. Withdrawal from and termination of information sharing agreement 127
181. Enforcement of information sharing agreement 127
182. Notification of Chief Data Officer 128
183. Register of information sharing agreements 128

Division 5 — Authorisations to share information and related matters

184. Authorisation to disclose information under information sharing agreement 129
185. Authorisation to collect, hold, manage and use information under information sharing agreement 130
186. Authorisation to further disclose information disclosed under information sharing agreement in certain circumstances 131

187. Authorisations override secrecy provisions 131
188. Protection from liability for authorised information sharing 132
189. Offences for unauthorised further disclosure or use of information 132
190. Regulations may prescribe safeguards 133

Division 7 — Information holdings requests

196. Information holdings request 134
197. Response to information holdings request 134

Division 8 — Administration

Subdivision 1 — Chief Data Officer

198. Chief Data Officer 136
199. Chief Data Officer is separate public entity for information sharing purposes 136
200. Functions of Chief Data Officer 136
201. Power to issue guidelines 138
202. Consultation on guidelines 139
203. Chief Data Officer must have regard to objects of Act 139

Subdivision 2 — Privacy and Responsible Information Sharing Advisory Committee

204. Privacy and Responsible Information Sharing Advisory Committee 139
205. Functions of Privacy and Responsible Information Sharing Advisory Committee 140
206. Regulations about Privacy and Responsible Information Sharing Advisory Committee 141

Subdivision 3 — Delegation and secrecy

207. Delegation by Chief Data Officer 141
208. Secrecy and authorised disclosure and use of information 142

Subdivision 4 — Making documents publicly available

209. Making documents publicly available 143

Division 9 — General

210. Information sharing officers of public entities 143
211. Matters to be included in annual report 144
212. Interaction with other laws 146

213. Application of *Freedom of Information Act 1992* to shared information 146
214. Review of information sharing provisions of Act 146

Part 4 — Miscellaneous

215. False or misleading information 148
216. Acts and practices of public entities and other IPP entities 148
217. States of mind of public entities and other IPP entities 149
218. Protection from personal liability 149
219. Giving documents 150
220. Laying documents before House of Parliament not sitting 150
221. General provisions about guidelines 151
222. Regulations 152

Part 5 — Transitional provisions

223. Application of information privacy principles 153
224. Application of approved privacy codes of practice 154
225. Notifiable information breach may involve personal information collected before commencement day 154
226. Public register obligations apply to personal information collected before commencement day 155
227. Privacy impact assessments not required for functions or activities performed before commencement day 155
228. State services contracts entered into before commencement day 156
229. Transitional regulations 156

Part 6 — Other Acts amended

Division 2 — *Freedom of Information Act 1992* amended

232. Act amended 158
233. Section 23 amended 158
234. Section 32 amended 158
235. Section 45 amended 159
236. Section 67A inserted 159

67A. Commissioner may deal with complaint under *Privacy and Responsible Information Sharing Act 2024* 159
237. Section 98 replaced 160
98. Application on behalf of child or person with disability 160
98A. Certain requests under *Privacy and Responsible Information Sharing Act 2024* taken to be applications for access or amendment 161
238. Glossary clause 1 amended 162
239. Various references to personal information "about" an individual amended 163
Division 3 — *Government Trading Enterprises Act 2023* amended
240. Act amended 164
241. Section 86 amended 164
Division 4 — *Health Practitioner Regulation National Law Application Act 2024* amended
242. Act amended 165
243. Section 22 amended 165
Division 5 — *National Health Funding Pool Act 2012* amended
244. Act amended 165
245. Section 25 amended 165
Part 7 — Amendment to this Act linked to commencement of *Criminal Law (Mental Impairment) Act 2023*
246. Act amended 167
247. Section 4 amended 167
Schedule 1 — Information privacy principles
1. Principle 1: Collection 168
2. Principle 2: Use and disclosure 171
3. Principle 3: Information quality 174
4. Principle 4: Information security 175

5. Principle 5: Openness and transparency 175
6. Principle 6: Access and correction 175
7. Principle 7: Unique identifiers 178
8. Principle 8: Anonymity 178
9. Principle 9: Disclosures outside Australia 179
10. Principle 10: Automated decision-making 180
11. Principle 11: De-identified information 181

Schedule 2 — Responsible sharing principles

1. Principle 1: Activities 183
2. Principle 2: Recipients 183
3. Principle 3: Information 184
4. Principle 4: Settings 185
5. Principle 5: Outputs 186

Notes

Compilation table 187
Uncommenced provisions table 188
Other notes 188

Defined terms

Western Australia

Privacy and Responsible Information Sharing Act 2024

An Act —

- **to provide a framework to protect the privacy of personal information handled by public entities, Ministers, Parliamentary Secretaries and contracted service providers to public entities; and**
- **to provide a framework to authorise the responsible sharing of information held by public entities; and**
- **to establish the office of Chief Data Officer; and**
- **to amend the *Freedom of Information Act 1992*; and**
- **to make consequential amendments to other Acts; and**
- **for related purposes.**

Part 1 — Preliminary

1. Short title

This is the *Privacy and Responsible Information Sharing Act 2024*.

2. Commencement

This Act comes into operation as follows —

(a) Part 1 — on the day on which this Act receives the Royal Assent;

(b) Part 7 —

(i) if the *Criminal Law (Mental Impairment) Act 2023* section 156 comes into operation on or before the day on which Part 1 of this Act comes into operation under paragraph (a) — immediately after Part 1 of this Act comes into operation; or

(ii) otherwise — on the day on which the *Criminal Law (Mental Impairment) Act 2023* section 156 comes into operation;

(c) the rest of the Act — on a day fixed by proclamation, and different days may be fixed for different provisions.

3. Objects

The objects of this Act are as follows —

(a) to promote responsible and transparent practices for handling personal information by IPP entities;

(b) to balance the public interest in protecting the privacy of personal information handled by IPP entities with the public interest in the free flow of information;

(c) to provide a means for individuals to complain about alleged interferences with their privacy;

(d) to promote responsible information security practices by IPP entities;

(e) to promote the responsible handling of information held by public entities as a public resource that supports government policy, programs and services;

(f) to facilitate the responsible collection, use and disclosure for permitted purposes of information held by public entities;

(g) to remove barriers that unnecessarily impede the responsible sharing of information held by public entities;

(h) to provide protections in connection with the sharing of information under this Act, including by —

(i) specifying the purposes for which, and the circumstances in which, information sharing is permitted or required; and

(ii) ensuring that information shared under this Act is protected from unauthorised use or disclosure.

4. Terms used

In this Act —

Aboriginal community controlled organisation means an organisation described in clause 44 of the "National Agreement on Closing the Gap" between the Coalition of Aboriginal and Torres Strait Islander Peak Organisations, the Commonwealth, the States, the Australian Capital Territory, the Northern Territory and the Australian Local Government Association dated July 2020;

Aboriginal information assessment has the meaning given in section 177(1);

Aboriginal information use plan has the meaning given in section 177(4);

act includes an omission;

affected individual —

(a) in relation to a notifiable information breach, has the meaning given in section 58; or

(b) in relation to a determination by the Information Commissioner under section 107, has the meaning given in section 107(1);

approved form means a form approved by the person to whom the form is permitted or required to be given under this Act;

approved privacy code of practice means a privacy code of practice approved by the Governor under section 32(3);

assessed notifiable information breach, in relation to an IPP entity, has the meaning given in section 61(3);

assessed shared information breach, in relation to a recipient under an information sharing agreement, has the meaning given in section 192(4);

Australian Information Commissioner means the person appointed as Australian Information Commissioner under the *Australian Information Commissioner Act 2010* (Commonwealth) section 14(1);

authorised officer means a person designated as an authorised officer under section 120(1);

automated decision-making process has the meaning given in section 16(2);

automated system has the meaning given in section 16(1);

care leaver means a person who —

(a) has reached 18 years of age; and

(b) qualifies for assistance under the *Children and Community Services Act 2004* section 96 for the purposes of Part 4 Division 6 of that Act;

Chief Data Officer means the Chief Data Officer appointed in accordance with section 198;

Chief Data Officer guidelines means guidelines issued under section 201, as in effect from time to time;

child means a person who is under 18 years of age;

child protection functions means functions that relate to —

(a) the protection and care of children, unborn children and care leavers; or

(b) promoting the wellbeing of children, unborn children and care leavers, including their —

(i) care; and

(ii) physical, emotional, psychological and educational development; and

(iii) physical, emotional and psychological health; and

(iv) safety;

collect, in relation to information —

(a) means to obtain the information from any source or by any means; and

(b) includes to infer the information from, or generate the information by the use or interpretation of, other information;

community policing functions, of the Police Force of Western Australia, includes the following —

(a) undertaking missing persons investigations;

(b) transferring individuals into the care or custody of another entity;

(c) supporting victims of crime;

(d) locating next of kin;

(e) employing diversionary strategies;

(f) coordinating operational response and dispatch;

(g) other functions prescribed by the regulations;

compliance notice has the meaning given in section 122(1);

conciliator means a person nominated as a conciliator under section 96(1);

confidential or commercially sensitive information means —

(a) information that is required to be kept confidential because of a contractual or equitable obligation; or

(b) any other information the disclosure of which would prejudice any person's legitimate business, professional, commercial or financial interests;

consent means express consent or implied consent;

contracted service provider has the meaning given in section 8(2);

data analytics work has the meaning given in section 12(2);

data integration has the meaning given in section 12(4);

data linkage has the meaning given in section 12(3);

data set has the meaning given in section 12(1);

de-identified information has the meaning given in section 11(2);

de-identify, in relation to personal information, has the meaning given in section 11(1);

derived information has the meaning given in section 170(d)(iv);

disability has the meaning given in the *Disability Services Act 1993* section 3;

disclose has a meaning affected by section 10;

electronic means includes —

(a) an electronic database or document system; and

(b) any other means by which a document can be given or accessed electronically;

emergency response functions means functions that relate to responding to an emergency, including by combating its effects,

providing emergency assistance to persons affected and reducing resulting damage;

exempt information has the meaning given in section 158;

external entity has the meaning given in section 156(2);

family violence has the meaning given in the *Restraining Orders Act 1997* section 5A(1);

government information, in relation to a public entity, has the meaning given in section 157;

handle, in relation to information, means to collect, hold, manage, use or disclose the information;

Health and Disability Services Complaints Office Director means the Director as defined in the *Health and Disability Services (Complaints) Act 1995* section 3(1);

health information means —

(a) personal information that relates to —

(i) the health (at any time) of an individual; or

(ii) the disability (at any time) of an individual; or

(iii) an individual's expressed wishes about the future provision of health services to the individual; or

(iv) a health service provided, or to be provided, to an individual;

or

(b) other personal information collected to provide, or in providing, a health service;

health service means any of the following —

(a) a health service as defined in the *Health Services Act 2016* section 7;

(b) the supply or prescription of a medicine by a person registered under the *Health Practitioner Regulation National Law (Western Australia)*;

(c) the prescription, supply or administration of a voluntary assisted dying substance under the *Voluntary Assisted Dying Act 2019*;

(d) a service or activity, provided in conjunction with a service or activity referred to in paragraph (a), (b) or (c), of a class prescribed by the regulations;

high privacy impact function or activity has the meaning given in section 79(1);

hold, in relation to information, means to have possession or control of the information, whether alone or jointly with others;

holding entity, in relation to an information sharing request, has the meaning given in section 160(3)(b);

information breach means —

(a) unauthorised access to, or unauthorised disclosure of, information; or

(b) loss of information;

Information Commissioner means the person appointed as Information Commissioner under the *Information Commissioner Act 2024* section 5(2);

information holdings request has the meaning given in section 196(2);

information privacy principle (***IPP***) means an information privacy principle set out in Schedule 1;

information sharing agreement has the meaning given in section 168(1);

information sharing CEO means the chief executive officer of the information sharing Department;

information sharing Department means the department of the Public Service principally assisting in the administration of Part 3;

information sharing direction has the meaning given in section 163(1);

Information Sharing Minister means the Minister to whom the administration of Part 3 is from time to time committed by the Governor;

information sharing request has the meaning given in section 160(3)(a);

interference with the privacy, of an individual, has the meaning given in section 15;

IPP entity has the meaning given in section 14;

judicial body has the meaning given in section 7;

law enforcement agency means any of the following bodies or persons, including staff under the control of the body or person —

(a) the Police Force of Western Australia; or

(b) the Corruption and Crime Commission established under the *Corruption, Crime and Misconduct Act 2003* section 8; or

(c) the Parliamentary Inspector of the Corruption and Crime Commission appointed under the *Corruption, Crime and Misconduct Act 2003* section 189; or

(d) a commission established under a written law or a law of the Commonwealth, another State or a Territory that has the function of investigating criminal activity or a class of criminal activity; or

(e) the Mental Impairment Review Tribunal established under the *Criminal Law (Mental Impairment) Act 2023* section 156; or

(f) the Prisoners Review Board established under the *Sentence Administration Act 2003* section 102; or

(g) the Supervised Release Review Board established under the *Young Offenders Act 1994* section 151; or

(h) the department of the Public Service principally assisting in the administration of the *Sentence Administration Act 2003* Part 8; or

(i) the department of the Public Service principally assisting in the administration of the *Police Act 1892*; or

(j) the Director of Public Prosecutions appointed under the *Director of Public Prosecutions Act 1991* section 5; or

(k) the Commissioner of State Revenue appointed in accordance with the *Taxation Administration Act 2003* section 6; or

(l) the sheriff referred to in the *Supreme Court Act 1935* section 156; or

(m) the Australian Crime Commission established by the *Australian Crime Commission Act 2002* (Commonwealth) section 7; or

(n) the Australian Federal Police; or

(o) the police force of another State or a Territory; or

(p) a public entity not covered by another paragraph of this definition that is responsible for the performance of functions related to —

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences or contraventions of a law that are subject to a penalty or sanction; or

(ii) the management of property seized or restrained under a law relating to the confiscation of proceeds of crime; or

(iii) the enforcement of a law, or of an order made under a law, relating to the confiscation of proceeds of crime; or

(iv) the execution or implementation of orders made by a court or tribunal; or

(v) the protection of public revenue;

or

(q) a body, or the holder of an office, prescribed by the regulations;

law enforcement functions, of a law enforcement agency —

(a) means functions of the law enforcement agency that relate to —

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences or contraventions of a law that are subject to a penalty or sanction; or

(ii) the management of property seized or restrained under a law relating to the confiscation of proceeds of crime; or

(iii) the enforcement of a law, or of an order made under a law, relating to the confiscation of proceeds of crime; or

(iv) the preparation for or conduct of proceedings in a court or tribunal; or

(v) the execution or implementation of orders made by a court or tribunal; or

(vi) the protection of public revenue;

and

(b) includes, in the case of the Police Force of Western Australia, community policing functions;

materially assisted, in relation to the making of a decision and an automated system, has the meaning given in section 16(3);

member of Commissioner staff means a member of staff as defined in the *Information Commissioner Act 2024* section 3;

notice to produce or attend has the meaning given in section 113(1);

notifiable information breach has the meaning given in section 57;

officer, of a public entity or other IPP entity, includes —

(a) the principal officer of the entity; and

(b) a person employed in, by, or for the purposes of, the entity; and

(c) if the entity is a body (whether incorporated or not) constituted by 2 or more persons — any of those persons;

outsourcing entity has the meaning given in section 8(1);

Parliamentary Commissioner for Administrative Investigations means the Commissioner as defined in the *Parliamentary Commissioner Act 1971* section 4;

Parliamentary Secretary means —

(a) a Parliamentary Secretary appointed under the *Constitution Acts Amendment Act 1899* section 44A(1); or

(b) the Parliamentary Secretary of the Cabinet;

permitted purpose has the meaning given in section 159(1);

personal information —

(a) means information or an opinion, whether true or not, and whether recorded in a material form or not, that relates to an individual, whether living or dead, whose identity is apparent or can reasonably be ascertained from the information or opinion; and

(b) includes information of the following kinds to which paragraph (a) applies —

(i) a name, date of birth or address;

(ii) a unique identifier, online identifier or pseudonym;

(iii) contact information;

(iv) information that relates to an individual's location;

(v) technical or behavioural information in relation to an individual's activities, preferences or identity;

(vi) inferred information that relates to an individual, including predictions in relation to an individual's behaviour or preferences and profiles generated from aggregated information;

(vii) information that relates to 1 or more features specific to the physical, physiological, genetic, mental, behavioural, economic, cultural or social identity of an individual;

Police Force of Western Australia means the Police Force of Western Australia provided for by the *Police Act 1892*;

principal officer, in relation to a public entity or other IPP entity, has the meaning given in section 9;

privacy code of practice has the meaning given in section 28(1);

privacy complaint means a complaint under section 82(1);

Privacy Deputy Commissioner means the person appointed as Privacy Deputy Commissioner under the *Information Commissioner Act 2024* section 13(2);

privacy functions has the meaning given in section 142(1);

privacy guidelines means guidelines issued under section 148, as in effect from time to time;

privacy impact assessment means —

(a) an assessment of a function or activity of an IPP entity conducted under section 79 or in compliance with a direction under section 80; or

(b) an assessment of a relevant activity to be carried out under a proposed information sharing agreement conducted under section 176;

Privacy Minister means the Minister to whom the administration of Part 2 is from time to time committed by the Governor;

proposed provider, in relation to a proposed information sharing agreement, means a public entity that would be a provider under the agreement;

proposed recipient, in relation to a proposed information sharing agreement, means a public entity or external entity that would be a recipient under the agreement;

provider, in relation to an information sharing agreement, has the meaning given in section 168(2);

public entity has the meaning given in section 6;

public interest determination has the meaning given in section 45(1);

public register means a register or other document that —

(a) is held by a public entity; and

(b) contains information that a person was required or permitted to give to that public entity under a written law; and

(c) is published, or available for inspection by members of the public (whether for a fee or charge or not), under a written law (other than as a result of a request for access under this Act or an application for access under the *Freedom of Information Act 1992* Part 2);

recipient, in relation to an information sharing agreement, has the meaning given in section 168(3);

re-identify, in relation to de-identified information, has the meaning given in section 11(3);

relevant activity, in relation to an information sharing agreement, has the meaning given in section 168(1)(c);

requesting entity, in relation to an information sharing request, has the meaning given in section 160(3)(c);

respondent, in relation to a privacy complaint, has the meaning given in section 82(2)(b);

responsible Minister means —

(a) in relation to a public entity that is a department as defined in the *Public Sector Management Act 1994* section 3(1) — the Minister responsible for the administration of the department; or

(b) in relation to a public entity to which paragraph (a) does not apply —

(i) for a public entity established or appointed under an enactment — the Minister to whom the administration of the enactment is from time to time committed by the Governor; or

(ii) for a public entity that is not established or appointed under an enactment — the Minister to whom the administration of the public entity is from time to time committed by the Governor;

or

(c) in relation to a secrecy provision — the Minister to whom the administration of the secrecy provision is from time to time committed by the Governor;

responsible sharing principle means a responsible sharing principle set out in Schedule 2;

secrecy provision means a provision of a written law that prohibits or regulates the handling of information;

senior executive officer has the meaning given in the *Public Sector Management Act 1994* section 3(1);

senior officer, of a public entity or other IPP entity —

(a) means an officer of the entity who has managerial responsibility; and

(b) includes the principal officer of the entity;

sensitive Aboriginal family history information means information, including family history information, that —

(a) relates to Aboriginal people and their ancestors; and

(b) was collected in the period from 1898 until 1972 for the purposes of implementing laws, and government policies and practices, applying specifically to Aboriginal people;

sensitive Aboriginal traditional information means information that, according to Aboriginal tradition, should not be disclosed to individuals who are not the knowledge holders of that information;

sensitive personal information means personal information —

(a) that relates to an individual's —

(i) racial or ethnic origin; or

(ii) gender identity, in a case where the individual's gender identity does not correspond with their designated sex at birth; or

(iii) sexual orientation or practices; or

(iv) political opinions; or

(v) membership of a political association; or

(vi) religious beliefs or affiliations; or

(vii) philosophical beliefs; or

(viii) membership of a professional or trade association; or

(ix) membership of a trade union; or

(x) criminal record;

or

(b) that is health information; or

(c) that is genetic or genomic information (other than health information); or

(d) that is biometric information; or

(e) from which information of a kind referred to in any of paragraphs (a) to (d) can reasonably be inferred;

shared information, in relation to a shared information breach, has the meaning given in section 191(a);

shared information breach has the meaning given in section 191;

significant decision has the meaning given in section 16(4);

special information sharing entity has the meaning given in section 156(1);

State services contract has the meaning given in section 8(1);

temporary public interest determination has the meaning given in section 49(1);

unique identifier —

(a) means a number or other identifier assigned by an entity to an individual to uniquely identify that individual for the purposes of the operations of the entity; but

(b) does not include an identifier that consists only of the individual's name;

variation agreement has the meaning given in section 179(1).

[Section 4 amended: No. 51 of 2024 s. 247.]

5. References to information privacy principles

A reference in this Act to an IPP followed by a designation is a reference to the provision with that designation in Schedule 1.

6. Public entities

(1) A ***public entity*** is —

(a) a department of the Public Service; or

(b) an entity specified in the *Public Sector Management Act 1994* Schedule 2 column 2; or

(c) the Police Force of Western Australia; or

(d) a local government, regional local government or regional subsidiary; or

(e) a body, or the holder of an office, that is established for a public purpose under a written law; or

(f) a body, or the holder of an office, that is established by the Governor or a Minister; or

(g) a judicial body; or

(h) any other body, or the holder of any other office, that is prescribed by the regulations to be a public entity, being —

(i) a body or office that is established under a written law; or

(ii) a corporation or association over which control can be exercised by the State, a Minister, a body referred to in paragraph (a), (b), (e) or (f) or subparagraph (i), or the holder of an office referred to in paragraph (f) or subparagraph (i).

(2) Despite subsection (1), each of the following is not a ***public entity*** —

(a) the Governor or the Governor's establishment;

(b) the Legislative Council or a member or committee of the Legislative Council;

(c) the Legislative Assembly or a member or committee of the Legislative Assembly;

(d) a joint committee or standing committee of the Legislative Council and the Legislative Assembly;

(e) a Royal Commission or member of a Royal Commission;

(f) a department of the staff of Parliament referred to in the *Parliamentary and Electorate Staff (Employment) Act 1992*;

(g) a person holding an office established under a written law for the purposes of a body referred to in any of paragraphs (a) to (f).

(3) Except to the extent provided by section 199 and regulations made under subsection (4), a person is not a separate public entity for the purposes of this Act by reason of —

(a) holding office as a member or other officer of a public entity; or

(b) holding an office established for the purposes of a public entity.

(4) The regulations may provide that, for the purposes of this Act or specified provisions of this Act —

(a) a specified body, or the holder of a specified office, is not a separate public entity but is part of a specified public entity; or

(b) a specified body, or the holder of a specified office, is a separate public entity and is not part of another public entity.

7. Judicial bodies

(1) A ***judicial body*** is a court or tribunal established under a written law.

(2) A registry or other office of a judicial body, and the staff of such a registry or other office, are part of the judicial body.

(3) A person holding judicial or quasi-judicial office is not themselves, and is not part of, a judicial body or other public entity.

8. State services contracts and contracted service providers

(1) A ***State services contract*** is a contract between a public entity (the ***outsourcing entity***) and another person (other than a public entity) under which services are provided to the outsourcing entity or to other persons on behalf of the outsourcing entity.

(2) A ***contracted service provider*** is —

(a) a party to a State services contract who provides services to or on behalf of an outsourcing entity under the contract; or

(b) a person who is a subcontractor (whether direct or indirect) of a person referred to in paragraph (a) for the purposes of the State services contract.

Note for this subsection:

Part 2 Division 11 provides for how Part 2 and the information privacy principles apply in relation to contracted service providers.

9. Principal officers

(1) The ***principal officer*** of a Minister or Parliamentary Secretary is the Minister or Parliamentary Secretary.

(2) The ***principal officer*** of a public entity is —

(a) in relation to a department of the Public Service or an entity specified in the *Public Sector Management Act 1994* Schedule 2 column 2 — the chief executive officer or chief employee of the department or entity; or

(b) in relation to the Police Force of Western Australia — the Commissioner of Police; or

(c) in relation to a local government — the chief executive officer of the local government; or

(d) in relation to a regional local government — the chief executive officer of the regional local government; or

(e) in relation to a regional subsidiary — the person who manages the affairs of the regional subsidiary; or

(f) in relation to any other public entity —

(i) if the regulations prescribe a person to be the principal officer of the public entity — that person; or

(ii) otherwise — the person determined under subsection (4).

(3) The ***principal officer*** of a contracted service provider is —

(a) if the relevant State services contract designates a person with managerial responsibility in relation to the contracted service provider as the principal officer of the contracted service provider for the purposes of this Act — that person; or

(b) otherwise — the person determined under subsection (4).

(4) For the purposes of subsection (2)(f)(ii) or (3)(b), the person is —

(a) if the public entity or contracted service provider consists of 1 person (other than a body corporate) — that person; or

(b) if the public entity or contracted service provider is a body (whether incorporated or not) constituted by 2 or more persons — the person entitled to preside at any meeting of the body at which the person is present; or

(c) otherwise — the person responsible for managing the affairs of the public entity or contracted service provider.

10. Disclosure by public entities and other IPP entities

A reference in this Act to a public entity or other IPP entity ***disclosing*** information —

(a) includes a reference to the entity making the information publicly available; and

(b) does not include a reference to the entity disclosing the information to the entity itself or to an officer of the entity.

11. De-identification and re-identification of information

(1) To ***de-identify*** personal information means to modify, or apply a process to, the information, with the result that the identity of an individual is not apparent, and cannot reasonably be ascertained, from the information.

(2) Information is ***de-identified information*** at a particular time if, at that time —

(a) the information has been de-identified; and

(b) the identity of an individual is not apparent, and cannot reasonably be ascertained, from the information.

(3) To ***re-identify*** de-identified information means to modify, or apply a process to, the information, with the result that the information again becomes personal information.

12. Data sets, data analytics work, data linkage and data integration

(1) A ***data set*** is an organised collection of information in a form that is capable of being analysed or processed (whether by an individual or an automated system).

(2) ***Data analytics work*** —

(a) is the examination and analysis of information for the purpose of drawing conclusions as a result of that examination and analysis; but

(b) does not include data linkage or data integration.

(3) ***Data linkage*** is a process for —

(a) detecting instances where separate records (whether within a single data set or different data sets) appear to relate to the same individual, family, place, event or matter; and

(b) assigning an identifier (a ***data linkage key***) to enable related records to be linked.

(4) ***Data integration*** is the combination or collation of information in 2 or more data sets, whether using data linkage keys or by another process.

13. Act binds Crown

This Act binds the Crown in right of Western Australia and, so far as the legislative power of the Parliament permits, the Crown in all its other capacities.

Part 2 — Privacy

Division 1 — Key concepts and preliminary matters

14. IPP entities

(1) An ***IPP entity*** is —

(a) a Minister; or

(b) a Parliamentary Secretary; or

(c) a public entity; or

(d) a contracted service provider.

(2) Subsection (1)(a) or (b) applies to a Minister or Parliamentary Secretary only in their capacity as a member of the Executive Government of the State in relation to a matter that is within their responsibilities as a Minister or Parliamentary Secretary and does not apply to that person in their capacity as a member of the Legislative Council or Legislative Assembly.

15. Interferences with privacy

Each of the following is an ***interference with the privacy*** of an individual —

(a) an act done, or practice engaged in, by an IPP entity in contravention of section 20(1) or 33(1)(a) in relation to personal information or de-identified information that relates to the individual;

(b) a failure by an IPP entity to comply with section 61 in relation to a suspected notifiable information breach involving personal information that relates to the individual;

(c) a failure by an IPP entity to comply with section 62 or 63 in relation to an assessed notifiable information breach involving personal information that relates to the individual;

(d) a failure by an IPP entity to comply with section 72(1) in relation to a direction given in relation to a suspected notifiable information breach involving personal information that relates to the individual;

(e) a failure by a public entity to comply with section 76 or 77(3) in relation to personal information that relates to the individual;

(f) a failure by an IPP entity to comply with section 79 or 80(4) in relation to a function or activity involving the handling of personal information that relates to the individual.

16. Automated decision-making processes and related concepts

(1) An ***automated system*** is an automated electronic system, including a computer information-processing system or artificial intelligence system.

(2) An ***automated decision-making process*** is a process under which —

(a) a decision is made by an automated system without the involvement of any individual; or

(b) the making of a decision is materially assisted by an automated system.

(3) The making of a decision is ***materially assisted*** by an automated system if —

(a) the decision is made by a person in reliance on a preliminary decision-making step (including a recommendation, assessment, conclusion or inference) made by an automated system; and

(b) that preliminary decision-making step has a material bearing on the decision that is made.

(4) A ***significant decision*** is a decision that —

(a) affects an individual's rights, entitlements, interests or liabilities; or

(b) otherwise has a significant effect on an individual's life circumstances, opportunities, behaviour or wellbeing.

(5) Privacy guidelines may set out matters to be taken into account in determining whether —

(a) the making of a decision is materially assisted by an automated system; or

(b) a decision is a significant decision.

(6) An IPP entity must have regard to guidelines referred to in subsection (5) in determining whether IPP 10 applies in relation to a decision-making process of the IPP entity.

17. Entities to which privacy obligations do not apply

The obligations imposed by this Part and the information privacy principles do not apply to —

(a) the Corruption and Crime Commission established under the *Corruption, Crime and Misconduct Act 2003* section 8; or

(b) the Parliamentary Inspector of the Corruption and Crime Commission appointed under the *Corruption, Crime and Misconduct Act 2003* section 189; or

(c) the Information Commissioner.

18. Application of privacy obligations to judicial bodies

The obligations imposed by this Part and the information privacy principles apply to an IPP entity that is a judicial body only in relation to the handling of information, or information that is held, in relation to matters of an administrative nature.

Division 2 — Information privacy principles

19. Information privacy principles

The information privacy principles are set out in Schedule 1.

20. IPP entities must comply with information privacy principles

(1) An IPP entity must not do an act, or engage in a practice, that is contrary to, or inconsistent with, an information privacy principle.

(2) Subsection (1) applies subject to —

(a) sections 21 to 27; and

(b) if an approved privacy code of practice is in force in relation to the IPP entity — section 33(1)(b); and

(c) if a public interest determination or temporary public interest determination is in force in relation to the IPP entity — section 53; and

(d) if the IPP entity is a contracted service provider — section 130.

21. Exception: personal, family or household affairs

The information privacy principles do not apply in relation to the handling of information by an individual, or to information held by an individual, only for the purposes of, or in connection with, the individual's personal, family or household affairs.

22. Exception: publicly available information

(1) The information privacy principles do not apply to the handling of information contained in a document that is —

(a) generally available to members of the public (whether for a fee or charge or not); or

(b) published or available for inspection by members of the public (whether for a fee or charge or not) under a written law, other than as a result of a request for access under this Act or an application for access under the *Freedom of Information Act 1992* Part 2; or

(c) a State archive to which a person has a right to be given access under the *State Records Act 2000* Part 6; or

(d) publicly available library material held by an IPP entity for reference purposes; or

(e) made or acquired by an art gallery, museum or library and preserved for public reference or exhibition purposes.

(2) The exception in subsection (1) does not apply in relation to the following information privacy principles —

(a) IPP 6.5 and IPP 6.6;

(b) IPP 6.7 and IPP 6.8, to the extent that those principles relate to correction of personal information.

23. Exception: law enforcement functions

An IPP entity that is a law enforcement agency is not required to comply with IPP 1.2, IPP 1.4, IPP 1.7, IPP 1.8, IPP 1.9, IPP 1.10, IPP 2, IPP 7, IPP 9 or IPP 11.2 if it believes on reasonable grounds that non-compliance is necessary for the purposes of its, or any other law enforcement agency's, law enforcement functions.

24. Exception: emergency response functions

An IPP entity is not required to comply with IPP 1.2, IPP 1.4, IPP 1.7, IPP 1.8, IPP 1.9, IPP 1.10, IPP 2, IPP 7, IPP 9 or IPP 11.2 if it believes on reasonable grounds that non-compliance is necessary for the purposes of its, or any other entity's, emergency response functions.

25. Exception: child protection functions

An IPP entity is not required to comply with IPP 1.2, IPP 1.8 or IPP 1.10 if it believes on reasonable grounds that non-compliance is necessary for the purposes of its, or any other entity's, child protection functions.

26. Exception: family violence

An IPP entity is not required to comply with IPP 1.2, IPP 1.8 or IPP 1.10 in relation to the collection of personal information if —

(a) the information relates to family violence or alleged family violence; and

(b) the individual to whom the collected information relates is the perpetrator, or alleged perpetrator, of the family violence.

27. Exception: IPP entities to which IPP 6 does not apply

IPP 6 does not apply to —

(a) an IPP entity that is an agency as defined in the *Freedom of Information Act 1992* Glossary clause 1 (whether or not the IPP entity is an exempt agency as defined in that clause); or

(b) a Parliamentary Secretary.

Notes for this section:

1. The *Freedom of Information Act 1992* provides for —
   (a) access to personal information contained in documents of an agency as defined in clause 1 of the Glossary of that Act (other than an exempt agency as defined in that clause); and
   (b) amendment of personal information contained in documents of an agency as defined in that clause.
2. Certain contractors and subcontractors in relation to contracts for security, custodial and prison services are agencies as defined in the *Freedom of Information Act 1992* Glossary clause 1.

Division 3 — Privacy codes of practice

28. Privacy code of practice

(1) A ***privacy code of practice*** is a code of practice that does either or both of the following —

(a) provides for modifications to the application of 1 or more of the information privacy principles by prescribing standards, whether or not in substitution for any information privacy principle, that are at least as stringent as the standards prescribed by the information privacy principles;

(b) provides for how 1 or more of the information privacy principles are to be applied or complied with.

(2) A privacy code of practice may also provide for any of the following —

(a) the imposition of requirements relating to the handling of personal information or de-identified information that are in addition to the information privacy principles, so long as those requirements are not inconsistent with the information privacy principles;

(b) without limiting paragraph (a), the imposition of requirements in relation to the use of personal information for data analytics work, data integration or data linkage;

(c) procedures to be followed by an IPP entity in dealing with complaints to the IPP entity alleging contraventions of the code;

(d) the review of the code at specified times;

(e) the expiry of the code at the end of a specified period.

(3) A privacy code of practice must specify —

(a) the IPP entities, or classes of IPP entity, to which it applies; or

(b) a means for determining the IPP entities, or classes of IPP entity, to which it applies.

(4) A privacy code of practice may apply in relation to either or both of the following —

(a) any specified information or class of information;

(b) any specified activity or class of activity.

29. IPP entity may prepare and submit privacy code of practice or amendment

(1) An IPP entity may, on its own initiative or on request by the Information Commissioner, prepare and submit to the Commissioner —

(a) a privacy code of practice; or

(b) an amendment to an approved privacy code of practice.

(2) In preparing the privacy code of practice or amendment, the IPP entity may undertake any consultation that the IPP entity considers appropriate.

30. Commissioner may prepare privacy code of practice or amendment

(1) If satisfied that it is in the public interest to do so, the Information Commissioner may, on the Commissioner's own initiative, prepare —

(a) a privacy code of practice; or

(b) an amendment to an approved privacy code of practice.

(2) In preparing the privacy code of practice or amendment, the Information Commissioner may undertake any consultation that the Commissioner considers appropriate.

31. Public consultation on privacy code of practice or amendment

(1) Before submitting a privacy code of practice or amendment submitted under section 29(1) or prepared under section 30(1) to the Governor under section 32(1), the Information Commissioner must —

(a) make publicly available for a period of at least 28 days —

(i) the privacy code of practice or amendment; and

(ii) a written notice inviting submissions on the privacy code of practice or amendment;

and

(b) have regard to any submissions made in relation to the privacy code of practice or amendment in accordance with the notice; and

(c) make the modifications, if any, the Commissioner considers appropriate to the privacy code of practice or amendment.

(2) The notice referred to in subsection (1)(a)(ii) must —

(a) invite persons whose interests may be affected by the privacy code of practice or amendment to make submissions; and

(b) specify the manner in which those submissions must be made; and

(c) specify the period within which those submissions must be made, which must be a period of at least 28 days beginning on the day on which the documents referred to in subsection (1)(a) are first made publicly available.

32. Submission and approval of privacy code of practice or amendment

(1) After complying with the requirements of section 31 in relation to a privacy code of practice or amendment, the Information Commissioner may submit to the Governor —

(a) the privacy code of practice or amendment; and

(b) a recommendation that the Governor approve the privacy code of practice or amendment.

(2) The Information Commissioner must not submit a privacy code of practice or amendment under subsection (1) unless the Commissioner is satisfied of the following in relation to the privacy code of practice or the approved privacy code of practice as it will be amended by the amendment (as the case requires) —

(a) that it is consistent with the objects of this Act set out in section 3(a) to (d);

(b) if it prescribes standards as referred to in section 28(1)(a) — that those standards are at least as stringent as the standards prescribed by the information privacy principles.

(3) The Governor may approve a privacy code of practice, or an amendment to an approved privacy code of practice, submitted and recommended under subsection (1).

33. Effect of approved privacy code of practice

(1) If an approved privacy code of practice is in force that applies to an IPP entity —

(a) the IPP entity must not do an act, or engage in a practice, that is contrary to or inconsistent with the approved privacy code of practice; and

(b) any act done or practice engaged in by the IPP entity in compliance with the approved privacy code of practice is taken to be done or engaged in in compliance with the information privacy principles.

(2) Subsection (1)(a) applies subject to —

(a) subsections (3) to (6); and

(b) if a public interest determination or temporary public interest determination is in force in relation to the IPP entity — section 53; and

(c) if the IPP entity is a contracted service provider — section 130.

(3) An approved privacy code of practice does not apply in relation to any handling of information to which the information privacy principles do not apply under sections 21 and 22.

(4) An IPP entity is not required to comply with an approved privacy code of practice to the extent that —

(a) the code provides for —

(i) modifications to the application of IPP 1.2, IPP 1.4, IPP 1.7, IPP 1.8, IPP 1.9, IPP 1.10, IPP 2, IPP 7, IPP 9 or IPP 11.2; or

(ii) how IPP 1.2, IPP 1.4, IPP 1.7, IPP 1.8, IPP 1.9, IPP 1.10, IPP 2, IPP 7, IPP 9 or IPP 11.2 is to be applied or complied with;

and

(b) either —

(i) the IPP entity is a law enforcement agency and believes on reasonable grounds that non-compliance is necessary for the purposes of its, or any other law enforcement agency's, law enforcement functions; or

(ii) the IPP entity believes on reasonable grounds that non-compliance is necessary for the purposes of its, or any other entity's, emergency response functions.

(5) An IPP entity is not required to comply with an approved privacy code of practice to the extent that —

(a) the code provides for —

(i) modifications to the application of IPP 1.2, IPP 1.8 or IPP 1.10; or

(ii) how IPP 1.2, IPP 1.8 or IPP 1.10 is to be applied or complied with;

and

(b) either —

(i) the IPP entity believes on reasonable grounds that non-compliance is necessary for the purposes of its, or any other entity's, child protection functions; or

(ii) the non-compliance relates to the collection of personal information that relates to family violence or alleged family violence and the individual to whom the collected information relates is the perpetrator, or alleged perpetrator, of the family violence.

(6) An IPP entity to which IPP 6 does not apply because of section 27 is not required to comply with an approved privacy code of practice to the extent that it provides for modifications to IPP 6 or for how IPP 6 is to be applied or complied with.

34. Revocation of approved privacy code of practice

(1) The Governor may, on the recommendation of the Information Commissioner, revoke an approved privacy code of practice by written instrument.

(2) Before making a recommendation to the Governor to revoke an approved privacy code of practice, the Information Commissioner must —

(a) make a written notice inviting submissions on the proposed revocation publicly available for a period of at least 28 days; and

(b) have regard to any submissions made in accordance with the notice.

(3) The notice referred to in subsection (2)(a) must —

(a) invite persons whose interests may be affected by the revocation of the approved privacy code of practice to make submissions; and

(b) specify the manner in which those submissions must be made; and

(c) specify the period within which those submissions must be made, which must be a period of at least 28 days beginning on the day on which the notice is first made publicly available.

35. Approved privacy code of practice or amendment is disallowable subsidiary legislation

(1) An approved privacy code of practice, or an approved amendment to an approved privacy code of practice, is subsidiary legislation for the purposes of the *Interpretation Act 1984*.

(2) The *Interpretation Act 1984* section 42 applies to an approved privacy code of practice, or an approved amendment to an approved privacy code of practice, as if it were regulations.

(3) An instrument revoking an approved privacy code of practice is subsidiary legislation for the purposes of the *Interpretation Act 1984*, but subsection (2) does not apply to the instrument.

36. Duration of approved privacy code of practice

(1) An approved privacy code of practice comes into operation in accordance with the *Interpretation Act 1984* section 41(1)(b).

(2) Subject to the *Interpretation Act 1984* section 42, an approved privacy code of practice remains in force until either of the following occurs —

(a) the period (if any) specified in the approved privacy code of practice under section 28(2)(e) ends;

(b) the approved privacy code of practice is revoked under section 34(1).

37. Register of approved privacy codes of practice

(1) The Information Commissioner must establish and maintain a register of approved privacy codes of practice.

(2) The register must include —

(a) a copy of each approved privacy code of practice that is in force; and

(b) the following information in relation to each approved privacy code of practice that is in force —

(i) the IPP entities, or classes of IPP entity, to which the code applies;

(ii) the day on which the code came into force;

(iii) if applicable — the day on which the code will expire;

(iv) any other information the Information Commissioner considers appropriate.

(3) The Information Commissioner must make the register publicly available.

(4) Without limiting subsection (3), the Information Commissioner must make the register available for public inspection during business hours.

38. Commissioner may review approved privacy code of practice

The Information Commissioner may review an approved privacy code of practice at any time.

Division 4 — Requests for access to and correction of personal information

39. Purpose of Division

This Division makes provision in relation to requests for access to, and correction of, personal information held by IPP entities to which IPP 6 applies.

Notes for this section:

1. Under section 27, IPP 6 does not apply to an IPP entity that is an agency as defined in the *Freedom of Information Act 1992* Glossary clause 1 or a Parliamentary Secretary.
2. The *Freedom of Information Act 1992* provides for —
   (a) access to personal information contained in documents of an agency as defined in clause 1 of the Glossary of that Act (other than an exempt agency as defined in that clause); and
   (b) amendment of personal information contained in documents of an agency as defined in that clause.

40. Request for access under IPP 6.1 or approved privacy code of practice

(1) An individual who wishes to access personal information that relates to the individual held by an IPP entity to which IPP 6 applies may request access to the information under IPP 6.1 or an applicable approved privacy code of practice.

(2) A request for access to personal information under IPP 6.1 or an applicable approved privacy code of practice must —
   (a) be given to the IPP entity in writing; and
   (b) give enough information to enable the personal information to which access is requested to be ascertained; and

(c) give an address in Australia to which notices under this Act can be sent; and

(d) give any other information or details prescribed by the regulations; and

(e) be accompanied by any fee for making the request prescribed by the regulations.

41. Request for correction under IPP 6.5 or approved privacy code of practice

(1) If an individual believes that personal information that relates to the individual held by an IPP entity to which IPP 6 applies is not accurate, complete and up-to-date, the individual may request the correction of the information under IPP 6.5 or an applicable approved privacy code of practice.

(2) A request for correction under IPP 6.5 or an applicable approved privacy code of practice must —

(a) be given to the IPP entity in writing; and

(b) give enough information to enable the personal information the subject of the request to be ascertained; and

(c) give details of the matters in relation to which the individual believes that the personal information is not accurate, complete and up-to-date; and

(d) give the individual's reasons for holding that belief; and

(e) give details of the correction that the individual wishes to have made; and

(f) give an address in Australia to which notices under this Act can be sent; and

(g) give any other information or details prescribed by the regulations.

(3) For the purposes of subsection (2)(e), the request must state whether the individual wishes the correction to be made —

(a) by altering information; or

(b) by striking out or deleting information; or

(c) by inserting information; or

(d) by inserting a note in relation to information; or

(e) in 2 or more of those ways.

42. IPP entity to provide assistance in making request

(1) If the circumstances of an individual require it, an IPP entity must take reasonable steps to help the individual to make to the appropriate IPP entity in accordance with this Act —

(a) a request for access under IPP 6.1 or an applicable approved privacy code of practice; or

(b) a request for correction under IPP 6.5 or an applicable approved privacy code of practice.

(2) In particular, if a request for access does not comply with the requirements of section 40(2), or a request for correction does not comply with the requirements of section 41(2), the IPP entity must take reasonable steps to help the individual to change the request so that it complies with those requirements.

43. Protection from liability for providing access to information

If an IPP entity provides an individual with access to information on request by the individual believing in good faith that the provision of access to the information is in compliance with IPP 6 or an applicable approved privacy code of practice —

(a) no civil or criminal liability is incurred in respect of the provision of access to the information; and

(b) the provision of access to the information is not to be regarded as a breach of any duty of confidentiality or secrecy imposed by law; and

(c) the provision of access to the information is not to be regarded as a breach of professional ethics or standards or as unprofessional conduct.

44. Certain applications under *Freedom of Information Act 1992* taken to be requests under IPP 6 or approved privacy code of practice

(1) If an application made by an individual to an IPP entity to which IPP 6 applies purports to be an application under the *Freedom of Information Act 1992* for access to a document containing personal information that relates to the individual, and the application meets the requirements of section 12 of that Act —

(a) the application is taken to be a request for access to personal information that relates to the individual under IPP 6.1 or an applicable approved privacy code of practice (as the case requires) that meets the requirements of section 40; and

(b) the IPP entity must deal with the application accordingly under this Act.

(2) If an application made by an individual to an IPP entity to which IPP 6 applies purports to be an application under the *Freedom of Information Act 1992* for amendment of personal information that relates to the individual contained in a document, and the application meets the requirements of section 46 of that Act —

(a) the application is taken to be a request for correction of personal information that relates to the individual under IPP 6.5 or an applicable approved privacy code of practice (as the case requires) that meets the requirements of section 41; and

(b) the IPP entity must deal with the application accordingly under this Act.

(3) If an application made by an individual to an IPP entity to which IPP 6 applies purports to be an application under the *Freedom of Information Act 1992* of a kind referred to in subsection (1) or (2), but does not meet the requirements of section 12 or 46 of that Act (as the case requires), the IPP entity must comply with its obligations under section 42 to help the individual to make a request for access or correction under IPP 6.1 or IPP 6.5 or an applicable approved privacy code of practice.

Division 5 — Public interest determinations and temporary public interest determinations

Subdivision 1 — Public interest determinations

45. Public interest determination

(1) The Information Commissioner may, on application by an IPP entity under section 46 and in accordance with the procedure set out in section 47, make a determination (a ***public interest determination***) that the Commissioner is satisfied —

(a) that a specified act or practice that an IPP entity proposes to do or engage in is inconsistent with either or both of the following —

(i) a specified information privacy principle;

(ii) a specified approved privacy code of practice in force in relation to the IPP entity;

but

(b) that —

(i) the public interest in the IPP entity doing the act or engaging in the practice substantially outweighs the public interest in the IPP entity complying with the information privacy principle, or approved privacy code of practice, or both; and

(ii) the IPP entity should therefore not be required to comply with the information privacy principle, or approved privacy code of practice, or both, either wholly or to the extent specified in the determination.

(2) A public interest determination cannot be made in relation to —

(a) IPP 4 or IPP 6; or

(b) an approved privacy code of practice, to the extent that it provides for modifications to IPP 4 or IPP 6 or for how IPP 4 or IPP 6 is to be applied or complied with.

(3) A public interest determination may, but is not required to, provide for the determination to expire at the end of a specified period.

46. Application for public interest determination

(1) An IPP entity may apply to the Information Commissioner for a public interest determination to be made in relation to an act or practice that the IPP entity proposes to do or engage in.

(2) The application must be in the approved form and must specify —

(a) the act or practice to which the determination would apply; and

(b) the information privacy principle, or approved privacy code of practice, or both, to which the determination would apply; and

(c) the reasons for seeking the determination.

47. Procedure to be followed on application for public interest determination

(1) If an IPP entity makes an application for a public interest determination under section 46, the Information Commissioner must —

(a) make publicly available for a period of at least 28 days a written notice that —

(i) states that the application has been received; and

(ii) specifies the IPP entity, the act or practice, and the information privacy principle or approved privacy code of practice, or both, to which the application relates; and

(iii) invites persons whose interests may be affected by the public interest determination to make submissions in relation to the application; and

(iv) specifies the manner in which those submissions must be made; and

(v) specifies the period within which those submissions must be made, which must be a period of at least 28 days beginning on the day on which the notice is first made publicly available;

and

(b) have regard to any submissions made in relation to the application in accordance with the notice.

(2) After complying with subsection (1), the Information Commissioner must prepare 1 of the following (the ***draft determination***) —

(a) a draft of the public interest determination the Commissioner proposes to make on the application;

(b) a draft determination dismissing the application.

(3) In preparing the draft determination, the Information Commissioner may undertake any consultation that the Commissioner considers appropriate.

(4) The Information Commissioner must —

(a) give a copy of the draft determination to the IPP entity and each person who made a submission referred to in subsection (1)(b); and

(b) give the IPP entity and each other person given a copy of the draft determination an opportunity to make submissions in relation to the draft determination, either —

(i) by attending a conference about the draft determination at a time, and at a place or by a means of audiovisual communication, specified by the Commissioner; or

(ii) by making written submissions in the manner, and within the period, specified by the Commissioner;

and

(c) have regard to any submissions made in relation to the draft determination as referred to in paragraph (b).

(5) After complying with subsection (4), the Information Commissioner may —

(a) under section 45 make a public interest determination that the Commissioner considers is appropriate in response to the application; or

(b) make a determination dismissing the application.

(6) If the Information Commissioner makes a public interest determination, or a determination dismissing an application for a public interest determination, the Commissioner —

(a) must give notice of the determination to the IPP entity; and

(b) may give notice of the determination to persons who made submissions referred to in subsection (1)(b).

48. Reporting on and review of determination

(1) If a public interest determination does not provide for the determination to expire within 12 months after the day on which it comes into force, the IPP entity must give the Information Commissioner a report on the public interest determination —

(a) as soon as practicable after the end of each of the following periods —

(i) the period of 12 months beginning on the day on which the determination comes into force;

(ii) each subsequent period of 12 months for which the determination is in force;

and

(b) at any other time requested by the Commissioner.

(2) A report under subsection (1) must include the information required by the Information Commissioner.

(3) Within 60 days after the day on which a report under subsection (1) is given to the Information Commissioner, the Commissioner must review the public interest determination and consider whether it should be revoked under section 54(2).

Subdivision 2 — Temporary public interest determinations

49. Temporary public interest determination

(1) The Information Commissioner may, on application by an IPP entity under section 50 and in accordance with the procedure set out in section 51, make a determination (a ***temporary public interest determination***) that the Commissioner is satisfied —

(a) that a specified act or practice that an IPP entity proposes to do or engage in is inconsistent with either or both of the following —

(i) a specified information privacy principle;

(ii) a specified approved privacy code of practice in force in relation to the IPP entity;

but

(b) that —

(i) the public interest in the IPP entity doing the act or engaging in the practice substantially outweighs the public interest in the IPP entity complying with the information privacy principle, or approved privacy code of practice, or both; and

(ii) the IPP entity should therefore not be required to comply with the information privacy principle, or approved privacy code of practice, or both, either wholly or to the extent specified in the determination.

(2) A temporary public interest determination cannot be made in relation to —

(a) IPP 4 or IPP 6; or

(b) an approved privacy code of practice, to the extent that it provides for modifications to IPP 4 or IPP 6 or for how IPP 4 or IPP 6 is to be applied or complied with.

(3) The Information Commissioner must not make a temporary public interest determination in relation to an act or practice of an IPP entity unless the Commissioner is satisfied that the application for the determination raises issues that require an urgent decision.

(4) A temporary public interest determination must provide for the determination to expire at the end of a specified period of no more than 6 months.

50. Application for temporary public interest determination

(1) An IPP entity may apply to the Information Commissioner for a temporary public interest determination to be made urgently in

relation to an act or practice that the IPP entity proposes to do or engage in.

(2) The application must be in the approved form and must specify —

(a) the act or practice to which the determination would apply; and

(b) the information privacy principle, or approved privacy code of practice, or both, to which the determination would apply; and

(c) the reasons for seeking the determination; and

(d) the reasons for the urgency.

51. Procedure to be followed on application for temporary public interest determination

(1) If an IPP entity makes an application for a temporary public interest determination under section 50, the Information Commissioner must make publicly available a written notice that —

(a) states that the application has been received; and

(b) specifies the IPP entity, the act or practice, and the information privacy principle or approved privacy code of practice, or both, to which the application relates.

(2) After complying with subsection (1), the Information Commissioner may —

(a) under section 49 make a temporary public interest determination that the Commissioner considers is appropriate in response to the application; or

(b) make a determination dismissing the application.

(3) If the Information Commissioner makes a temporary public interest determination, or a determination dismissing an application for a temporary public interest determination, the

Commissioner must give notice of the determination to the IPP entity.

52. Extension of temporary public interest determination

(1) An IPP entity in relation to which a temporary public interest determination is in force may apply to the Information Commissioner in the approved form for an extension of the temporary public interest determination.

(2) If an IPP entity makes an application under subsection (1), the Information Commissioner must make publicly available a written notice that states that an application for an extension of the temporary public interest determination has been received.

(3) After complying with subsection (2), the Information Commissioner may, by written instrument, extend the temporary public interest determination by no more than 6 months.

(4) No more than 1 extension can be granted in relation to a temporary public interest determination under subsection (3).

(5) The Information Commissioner must give written notice of a decision to extend, or refuse to extend, a temporary public interest determination to the IPP entity.

Subdivision 3 — General provisions about public interest determinations and temporary public interest determinations

53. Effect of determination

(1) This section applies if a public interest determination or temporary public interest determination is in force in relation to an act or practice of an IPP entity and an information privacy principle or approved privacy code of practice.

(2) In doing the act or engaging in the practice, the IPP entity is not required to comply with the information privacy principle or

approved privacy code of practice to the extent specified in the determination.

54. Revocation of determination

(1) The Information Commissioner may, by written instrument, revoke a public interest determination or temporary public interest determination on application by the IPP entity to which the determination applies.

(2) The Information Commissioner must, by written instrument, revoke a public interest determination or temporary public interest determination made in relation to an IPP entity if the Commissioner is satisfied that —

(a) the public interest in the IPP entity doing the act or engaging in the practice no longer substantially outweighs the public interest in the IPP entity complying with the relevant information privacy principle, or approved privacy code of practice, or both; or

(b) the IPP entity's reasons for seeking the determination set out in the application for the determination under section 46 or 50 are no longer applicable.

(3) Before revoking a public interest determination or temporary public interest determination under subsection (2), the Information Commissioner must —

(a) give the IPP entity a written notice that —

(i) states that the Commissioner intends to revoke the determination; and

(ii) states the reasons for the proposed revocation; and

(iii) invites the IPP entity to make submissions in relation to the proposed revocation; and

(iv) specifies the manner in which those submissions must be made; and

(v) specifies the period within which those submissions must be made;

and

(b) have regard to any submissions made by the IPP entity in accordance with the notice.

55. Determination is disallowable subsidiary legislation and statement of reasons required

(1) The following are subsidiary legislation for the purposes of the *Interpretation Act 1984* —

(a) a public interest determination;

(b) a temporary public interest determination;

(c) an instrument (an ***instrument of extension***) extending a temporary public interest determination under section 52(3);

(d) an instrument revoking a public interest determination or temporary public interest determination under section 54(1) or (2).

(2) When a public interest determination, temporary public interest determination or instrument of extension is published in accordance with the *Interpretation Act 1984* section 41(1)(a), a statement of reasons for making the determination or instrument must also be published in accordance with that section.

(3) The *Interpretation Act 1984* section 42 applies to a public interest determination as if the determination were regulations.

(4) The *Interpretation Act 1984* section 42 applies to a temporary public interest determination or instrument of extension as if —

(a) the determination or instrument were regulations; and

(b) the reference in subsection (2) of that section to 14 sitting days were a reference to 7 sitting days; and

(c) the reference in subsection (3) of that section to 14 days were a reference to 7 days.

(5) When a public interest determination, temporary public interest determination or instrument of extension is laid before a House of Parliament under the *Interpretation Act 1984* section 42(1), a statement of reasons for making the determination or instrument must also be laid before the House.

(6) Subsections (2) to (5) do not apply to an instrument revoking a public interest determination or temporary public interest determination under section 54(1) or (2).

56. Duration of determination

(1) A public interest determination or temporary public interest determination comes into force in accordance with the *Interpretation Act 1984* section 41(1)(b).

(2) Subject to the *Interpretation Act 1984* section 42, a public interest determination remains in force until either of the following occurs —

(a) the period (if any) specified in the determination under section 45(3) ends;

(b) the determination is revoked under section 54(1) or (2).

(3) Subject to the *Interpretation Act 1984* section 42, a temporary public interest determination remains in force until any of the following occurs —

(a) the period specified in the determination under section 49(4) or, if the determination has been extended under section 52(3), the period of the extension, ends;

(b) the determination is revoked under section 54(1) or (2);

(c) a public interest determination in substantially the same terms as the temporary public interest determination —

(i) comes into force; or

(ii) ceases to have effect under the *Interpretation Act 1984* section 42(2).

[Division 6 (s. 57-75) has not come into operation.]

Division 7 — Personal information in public registers

76. Disclosure of personal information in public registers

A public entity responsible for administering a public register must not disclose any personal information contained in the register unless the public entity is satisfied that it is to be used for a purpose related to the purpose of the register or the written law under which the register is maintained.

Note for this section:

Information contained in a public register is publicly available information to which the information privacy principles do not apply (see section 22).

77. Removal of personal information affecting individual's safety or wellbeing

(1) If personal information that relates to an individual is contained, or proposed to be contained, in a public register, the individual may request the public entity responsible for the administration of the public register to remove the information from, or not to include the information in, the public register.

(2) A request under subsection (1) must be made on the grounds that any individual's safety or wellbeing is or would be substantially affected by the information being made publicly available.

(3) If the public entity is satisfied that the grounds referred to in subsection (2) exist, the public entity must comply with the request unless the public entity is satisfied that the public interest in maintaining public access to the information outweighs any individual interest in the information not being made publicly available.

(4) This section does not prevent personal information removed from, or not included in, a public register under this section from being included in a version of the register that is not made publicly available.

78. Interaction with written laws establishing public registers

If there is a conflict or inconsistency between a provision of this Division and a provision of the written law under which a public register is established or maintained, the provision of this Division prevails.

Division 8 — Privacy impact assessments

79. Privacy impact assessment relating to high privacy impact function or activity

(1) A function or activity of an IPP entity is a ***high privacy impact function or activity*** if the performance of the function or activity —

(a) involves the handling of personal information; and

(b) is likely to have a significant impact on the privacy of individuals.

(2) Before an IPP entity first performs a high privacy impact function or activity, or makes a significant change to the way in which personal information is handled as part of a high privacy impact function or activity, the IPP entity must —

(a) conduct an assessment (a ***privacy impact assessment***) of the function or activity; and

(b) prepare a written report on the assessment in accordance with subsection (3).

(3) The report on the privacy impact assessment must —

(a) set out an assessment of the likelihood that the performance of the function or activity will result in an interference with the privacy of any individual; and

(b) identify the impact that the performance of the function or activity might have on the privacy of individuals; and

(c) set out recommendations for managing, minimising or eliminating that impact; and

(d) include any other information the IPP entity considers is relevant.

(4) In complying with the requirements of this section, the IPP entity must have regard to —

(a) any privacy guidelines referred to in section 81; and

(b) any other privacy guidelines relating to privacy impact assessments.

(5) On request by the Information Commissioner, the IPP entity must give the Commissioner a copy of the report on the privacy impact assessment.

(6) If the IPP entity is a contracted service provider, this section has effect subject to section 137.

80. Commissioner may direct privacy impact assessment

(1) The Information Commissioner may give an IPP entity a written direction in accordance with subsection (2) if —

(a) the IPP entity performs, or proposes to perform, a function or activity; and

(b) the Commissioner considers that the function or activity is a high privacy impact function or activity.

(2) The direction must —

(a) identify the function or activity to which it relates; and

(b) require the IPP entity to —

(i) conduct, and prepare a report on, an assessment (a ***privacy impact assessment***) of the function or activity in accordance with section 79(3) and (4); and

(ii) give the report to the Information Commissioner within a specified period.

(3) The direction may require specified information (in addition to the information referred to in section 79(3)) to be included in the report on the privacy impact assessment.

(4) An IPP entity must comply with a direction given to the IPP entity under this section.

(5) If the IPP entity is a contracted service provider, this section has effect subject to section 137.

81. Guidelines about significant impact on privacy

Privacy guidelines may set out matters to be taken into account in determining for the purposes of sections 79(1)(b) and 176(1)(a)(i) whether the performance of a function or activity, or a relevant activity under an information sharing agreement, is likely to have a significant impact on the privacy of individuals.

Division 9 — Privacy complaints

Subdivision 1 — Making a privacy complaint

82. Individual may complain about interference with privacy

(1) An individual may complain to the Information Commissioner about an act or practice of an IPP entity that may be an interference with the privacy of the individual.

(2) A privacy complaint must —

(a) be given to the Information Commissioner in writing; and

(b) state the IPP entity (the ***respondent***) to which the complaint relates; and

(c) give details of —

(i) the act or practice to which the complaint relates; and

(ii) any prior complaint made to the respondent about the act or practice and any response by the respondent to that complaint;

and

(d) give an address in Australia to which notices under this Part can be sent; and

(e) give any other information prescribed by the regulations.

(3) It is the duty of the Information Commissioner and members of Commissioner staff to assist an individual who wishes to make a privacy complaint and requires assistance to formulate the complaint.

83. Complaint on behalf of 2 or more individuals

A privacy complaint about an act or practice that may be an interference with the privacy of 2 or more individuals may be made by any of those individuals on behalf of all of them.

84. Complaint by or on behalf of child

A privacy complaint about an act or practice that may constitute an interference with the privacy of a child may be made —

(a) by the child; or

(b) on behalf of the child by —

(i) a parent or guardian of the child; or

(ii) another individual chosen by the child, or chosen by a parent or guardian of the child, to make the complaint on the child's behalf; or

(iii) another individual who, in the opinion of the Information Commissioner, has a sufficient interest in the subject matter of the complaint.

85. Complaint on behalf of individual with disability

If an adult is incapable of making a privacy complaint because of disability, a complaint may be made on behalf of the individual by —

(a) another individual chosen by the individual to make the complaint on their behalf; or

(b) if the individual is incapable of choosing another individual to make the complaint on their behalf —

(i) a guardian (as defined in the *Guardianship and Administration Act 1990* section 3(1)) of the individual; or

(ii) another individual who is related to the individual by blood or marriage or is a de facto partner of the individual; or

(iii) another individual who, in the opinion of the Information Commissioner, has a sufficient interest in the subject matter of the complaint.

86. Matter referred by Ombudsman may be treated as privacy complaint

(1) This section applies if, under the *Parliamentary Commissioner Act 1971* section 25(2), the Parliamentary Commissioner for Administrative Investigations reports to the Information Commissioner that a matter connected with a possible interference with the privacy of 1 or more individuals should be referred to the Information Commissioner for further consideration.

(2) The matter may be dealt with under this Division as if a privacy complaint had been made in relation to the matter.

(3) The privacy complaint may be treated as having been made by the individual or, if there are 2 or more individuals concerned, by each of them or any of them on behalf of all of them, as the Information Commissioner considers appropriate.

87. Complaint referred by Health and Disability Complaints Office Director may be treated as privacy complaint

(1) This section applies if the Health and Disability Services Complaints Office Director refers a complaint to the Information Commissioner under —

(a) the *Health and Disability Services (Complaints) Act 1995* section 28 or 32; or

(b) the *Disability Services Act 1993* section 38(4); or

(c) the *Mental Health Act 2014* section 323(2) or 329(4).

(2) The referred complaint is taken to be a privacy complaint made under section 82.

Subdivision 2 — Procedure after complaint is made

88. Notice of complaint

As soon as practicable after a privacy complaint is made, the Information Commissioner must give written notice of the complaint to the respondent.

89. Withdrawal of complaint

(1) A complainant may withdraw a privacy complaint at any time by written notice given to the Information Commissioner.

(2) If a privacy complaint is withdrawn, the Information Commissioner must give the respondent written notice of the withdrawal.

90. Commissioner may decline to deal with complaint

(1) The Information Commissioner may decline to deal with a privacy complaint if —

(a) before making the privacy complaint, the complainant did not first complain to the respondent in accordance with the complaints management system of the respondent (unless the Commissioner considers that it

was reasonable in the circumstances not to complain to the respondent); or

(b) the complainant has complained to the respondent and the Commissioner considers —

(i) that the respondent has not had sufficient time to deal with the complaint; or

(ii) that the respondent is dealing adequately with the complaint;

or

(c) the Commissioner considers that the act or practice (the ***relevant act or practice***) about which the complaint is made is not an interference with the privacy of an individual; or

(d) the Commissioner considers that the privacy complaint was made more than 12 months after the day on which the complainant became aware of the relevant act or practice; or

(e) the relevant act or practice has been the subject of a previous privacy complaint by the complainant that was withdrawn; or

(f) the Commissioner considers that the complaint is frivolous, vexatious, misconceived or lacking in substance; or

(g) the relevant act or practice is the subject of an application or complaint under another written law; or

(h) the Commissioner considers that the relevant act or practice has been adequately dealt with under another written law.

(2) The Information Commissioner may conduct a preliminary assessment of a privacy complaint for the purpose of deciding whether to deal with the complaint.

(3) For the purpose of a preliminary assessment the Information Commissioner may, by written notice, request any person to —

(a) attend before the Commissioner for the purpose of discussing the subject matter of the privacy complaint; or

(b) give the Commissioner any information or document specified in the notice.

(4) The Information Commissioner must give written notice of a decision to decline to deal with a privacy complaint under subsection (1) to the complainant and the respondent within 90 days after the day on which the complaint is made.

(5) A complainant given a notice under subsection (4) may apply to the State Administrative Tribunal for a review of the decision to decline to deal with the privacy complaint.

91. Commissioner may decline to continue dealing with complaint

(1) The Information Commissioner may decline to continue dealing with a privacy complaint if —

(a) the complainant does not comply with a reasonable request made by the Commissioner or a conciliator in dealing with the complaint; or

(b) the Commissioner is satisfied that the complainant, without reasonable excuse, has failed to cooperate with the Commissioner or a conciliator in dealing with the complaint.

(2) The Information Commissioner must give written notice of a decision to decline to continue dealing with a privacy complaint under subsection (1) to the complainant and the respondent.

(3) A complainant given a notice under subsection (2) may apply to the State Administrative Tribunal for a review of the decision to decline to continue dealing with the privacy complaint.

92. Commissioner may deal with complaint under *Freedom of Information Act 1992*

(1) If the Information Commissioner considers that the act or practice about which a privacy complaint is made could be the subject of a complaint under the *Freedom of Information Act 1992* Part 4 Division 3 —

(a) the Commissioner may decide that the complaint should be dealt with under that Act; and

(b) if the Commissioner so decides, the complaint is taken to be a complaint made under section 65 of that Act.

(2) If the Information Commissioner makes a decision that a complaint should be dealt with under the *Freedom of Information Act 1992*, the Commissioner must give written notice of the decision to the complainant and the respondent.

93. Commissioner may refer complaint to other authority

(1) If the Information Commissioner considers that the act or practice about which a privacy complaint is made could be the subject of a complaint under the *Privacy Act 1988* (Commonwealth) Part V, the Commissioner may refer the complaint to the Australian Information Commissioner.

(2) If the Information Commissioner considers that the act or practice about which a privacy complaint is made could be the subject of a complaint under the *Parliamentary Commissioner Act 1971* —

(a) the Information Commissioner may refer the complaint to the Parliamentary Commissioner for Administrative Investigations; and

(b) the referred complaint is taken to be a complaint made to the Parliamentary Commissioner for Administrative Investigations under the *Parliamentary Commissioner Act 1971* section 17.

(3) If the Information Commissioner considers that the act or practice about which a privacy complaint is made could be the subject of a complaint under the *Health and Disability Services (Complaints) Act 1995* Part 3 —

(a) the Commissioner may refer the complaint to the Health and Disability Services Complaints Office Director; and

(b) the referred complaint is taken to be a complaint made to that Director under the *Health and Disability Services (Complaints) Act 1995* section 19.

(4) If the Information Commissioner considers that the act or practice about which a privacy complaint is made could be the subject of a complaint under the *Disability Services Act 1993* Part 6 —

(a) the Commissioner may refer the complaint to the Health and Disability Services Complaints Office Director; and

(b) the referred complaint is taken to be a complaint made to that Director under the *Disability Services Act 1993* section 32.

(5) If the Information Commissioner considers that the act or practice about which a privacy complaint is made could be the subject of a complaint under the *Mental Health Act 2014* Part 19 —

(a) the Commissioner may refer the complaint to the Health and Disability Services Complaints Office Director; and

(b) the referred complaint is taken to be a complaint made to that Director under the *Mental Health Act 2014* Part 19 Division 3 Subdivision 3.

(6) If the Information Commissioner considers that the act or practice about which a privacy complaint is made could be the subject of a complaint under a scheme approved under the *Electricity Industry Act 2004* section 92, the *Energy*

Coordination Act 1994 section 11ZPZ or the *Water Services Act 2012* section 65 —

(a) the Commissioner may refer the complaint to the person (the ***scheme ombudsman***) who investigates and deals with complaints under the scheme; and

(b) the referred complaint is taken to be a complaint made to the scheme ombudsman in accordance with the scheme.

(7) The Information Commissioner cannot refer a privacy complaint to another authority under this section unless the Commissioner has undertaken appropriate consultation with, and had regard to any views expressed by, the other authority.

(8) If the Information Commissioner refers a privacy complaint under this section, the Commissioner must give written notice of the referral to the complainant and the respondent.

Subdivision 3 — Parties may resolve complaint

94. Parties may resolve complaint

(1) A complainant and respondent may resolve a privacy complaint by agreement at any time, whether or not with the assistance of the Information Commissioner and whether or not a conciliation process has begun under Subdivision 4.

(2) If a resolution of that kind occurs, the complainant must as soon as practicable give notice of the resolution to the Information Commissioner.

(3) If the Information Commissioner becomes aware that a privacy complaint has been resolved, the Commissioner must stop dealing with the complaint under this Division.

Subdivision 4 — Conciliation of complaints

95. Commissioner must attempt to resolve complaint by conciliation

(1) If the Information Commissioner considers that there is a reasonable likelihood that a privacy complaint can be resolved by conciliation, the Commissioner must —

(a) nominate a person to act as a conciliator in relation to the complaint under section 96(1); and

(b) otherwise take all reasonable steps to facilitate the resolution of the complaint by conciliation.

(2) Subsection (1) does not apply if the Information Commissioner has —

(a) declined under section 90(1) to deal with the complaint; or

(b) declined under section 91(1) to continue dealing with the complaint; or

(c) made a decision under section 92(1) that the complaint should be dealt with under the *Freedom of Information Act 1992*; or

(d) referred the complaint under section 93.

96. Procedure for conciliation

(1) The Information Commissioner may nominate a person to act as a conciliator in relation to a privacy complaint.

(2) A conciliator's function is to encourage the resolution of the complaint by —

(a) arranging for the complainant and the respondent to hold informal discussions about the complaint; and

(b) assisting in the conduct of those discussions; and

(c) if possible, assisting the complainant and respondent to reach agreement.

(3) A conciliator —

(a) may require the complainant and respondent to attend conciliation conferences (either in person or by a means of audiovisual communication); but

(b) does not have the power to require the production of documents or provision of information.

(4) The Information Commissioner may give any direction, or do any other thing, that the Commissioner considers appropriate to facilitate the resolution of a privacy complaint by conciliation.

(5) Without limiting subsection (4), the Information Commissioner may determine the procedure to be followed in a conciliation.

97. Representation in conciliation process

(1) Neither a complainant nor a respondent may be represented by another person during a conciliation process unless the Information Commissioner or a conciliator determines otherwise on the ground that the process will not work effectively without that representation.

(2) Subsection (1) does not prevent the personal attendance of any other person who may, in the opinion of the conciliator, assist in the conciliation.

98. Conciliation agreement

(1) If a privacy complaint is resolved by conciliation, the conciliator must prepare a document (the ***conciliation agreement***) that sets out the terms on which the complaint is agreed to be resolved.

(2) The conciliator must give a copy of the conciliation agreement to the complainant, the respondent and the Information Commissioner.

(3) The Information Commissioner may, with the written consent of the complainant and respondent, make 1 or more of the

following orders for the purpose of giving effect to the conciliation agreement or any part of the conciliation agreement —

(a) an order that the respondent must take specified action within a specified period to ensure that the respondent does not repeat or continue the act or practice (the ***relevant act or practice***) about which the complaint was made;

(b) an order that the respondent must perform any reasonable act, or carry out any reasonable course of conduct, to redress any loss or damage suffered by the complainant by reason of the relevant act or practice;

(c) an order that the respondent must pay the complainant a specified amount of compensation, not exceeding $75 000, for loss or damage suffered by the complainant by reason of the relevant act or practice.

Note for this subsection:

Division 10 Subdivision 6 provides for the enforcement of orders made under this subsection.

(4) Loss or damage referred to in subsection (3)(b) and (c) may include —

(a) an injury to the feelings of the complainant; and

(b) humiliation suffered by the complainant.

99. Notice of complaint that cannot be resolved by conciliation

(1) The Information Commissioner may decide that a privacy complaint cannot be resolved by conciliation if the Commissioner considers that —

(a) there is no reasonable likelihood that the complaint can be resolved by conciliation; or

(b) efforts to deal with the complaint by conciliation have not been successful.

(2) The Information Commissioner must give written notice of a decision under subsection (1) to the complainant and respondent.

(3) The notice must state that, as a result of the decision, the Information Commissioner may exercise powers under Subdivision 5 in relation to the privacy complaint.

100. Statements made in conciliation protected

Unless the complainant and respondent otherwise agree, evidence of anything said or admitted during the conciliation process for a privacy complaint —

(a) is not admissible in proceedings before a court or tribunal; and

(b) cannot be used by the Information Commissioner for the purposes of exercising a power under Subdivision 5 or Division 10.

Subdivision 5 — Dealing with complaint not resolved by conciliation

101. Commissioner may deal with complaint not resolved by conciliation

The powers under this Subdivision may be exercised in relation to a privacy complaint if the Information Commissioner has given notice under section 99(2) in relation to the complaint.

102. General matters about dealing with complaints

(1) In order to deal with a privacy complaint under this Subdivision, the Information Commissioner may obtain information from any persons and sources, and make any investigations and inquiries, that the Commissioner considers appropriate.

(2) Without limiting subsection (1), the Information Commissioner may, for the purposes of dealing with a privacy complaint —

(a) issue a notice to produce or attend and exercise related powers under Division 10 Subdivision 3; and

(b) if applicable, exercise powers under section 119.

(3) Subject to this Act, the Information Commissioner may determine the procedure for investigating and dealing with complaints and may give any necessary directions as to the conduct of the proceedings.

(4) The Information Commissioner must ensure that the complainant and respondent are given a reasonable opportunity to make submissions to the Commissioner.

(5) Proceedings for dealing with a privacy complaint must be conducted with as little formality and technicality, and with as much expedition, as the requirements of this Act and a proper consideration of the matters before the Information Commissioner permit, and the Commissioner is not bound by rules of evidence.

103. Referral of question of law to Supreme Court

(1) The Information Commissioner may refer to the Supreme Court any question of law that arises in the course of dealing with a privacy complaint.

(2) A question may be referred under this section on the Information Commissioner's own initiative or at the request of the complainant or respondent.

(3) The Supreme Court has jurisdiction to hear and determine a question of law referred to it under this section and, in exercising that jurisdiction, may —

(a) as well as determining that question, determine any related or incidental question of law that it considers to be raised; or

(b) instead of determining that question, determine any other question of law that it considers to be more pertinent.

(4) If a question of law in relation to a privacy complaint is referred to the Supreme Court under this section, the Information Commissioner must not —

(a) make a determination in relation to the complaint under section 104 before the Supreme Court makes a decision on the question; or

(b) proceed in a manner, or make a decision, that is inconsistent with the decision of the Supreme Court on the question.

(5) A complainant or respondent who did not request the referral of a question of law to the Supreme Court —

(a) is not required to appear, be represented or make submissions at, or otherwise participate in, the hearing of the referral; and

(b) is not liable for any costs in relation to the referral.

104. Determination of complaint

(1) The Information Commissioner may determine a privacy complaint —

(a) if the Commissioner is satisfied that the act or practice to which the complaint relates is an interference with the privacy of an individual — by making a determination to that effect; or

(b) otherwise — by making a determination dismissing the complaint.

(2) A determination under subsection (1)(a) may include 1 or more of the following orders —

(a) an order that the respondent must take specified action within a specified period to ensure that the respondent does not repeat or continue the interference with privacy;

(b) an order that the respondent must perform any reasonable act, or carry out any reasonable course of

conduct, to redress any loss or damage suffered by the complainant by reason of the interference with privacy;

(c) an order that the respondent must pay the complainant a specified amount of compensation, not exceeding $75 000, for loss or damage suffered by the complainant by reason of the interference with privacy;

(d) an order that it would be inappropriate for further action to be taken in relation to the interference with privacy.

Note for this subsection:

Division 10 Subdivision 6 provides for the enforcement of orders made under this subsection.

(3) Loss or damage referred to in subsection (2)(b) and (c) may include —

(a) an injury to the feelings of the complainant; and

(b) humiliation suffered by the complainant.

(4) The Information Commissioner must give the complainant and respondent written notice of a determination under subsection (1).

(5) The Information Commissioner may make a determination under subsection (1) publicly available.

105. Review of determination

The complainant or respondent in relation to a privacy complaint determined by the Information Commissioner under section 104 may apply to the State Administrative Tribunal for a review of the determination.

Division 10 — Investigations and enforcement

Subdivision 1 — Investigations of acts or practices that may be interferences with privacy

106. Commissioner may investigate act or practice that may be interference with privacy

(1) The Information Commissioner may investigate an act or practice of an IPP entity that may be an interference with the privacy of an individual.

(2) An investigation under this section may be conducted on the Information Commissioner's own initiative.

(3) In conducting the investigation the Information Commissioner may obtain information from any persons and sources, and make any investigations and inquiries, that the Commissioner considers appropriate.

(4) Without limiting subsection (3), the Information Commissioner may, for the purposes of conducting the investigation —

(a) issue a notice to produce or attend and exercise related powers under Subdivision 3; and

(b) if applicable, exercise powers under section 119.

(5) The Information Commissioner must ensure that the IPP entity the subject of the investigation is given a reasonable opportunity to make submissions to the Commissioner.

107. Determination following investigation

(1) If, after conducting an investigation under section 106, the Information Commissioner is satisfied that an act or practice of an IPP entity is an interference with the privacy of 1 or more individuals (the ***affected individuals***), the Commissioner may make a determination to that effect.

(2) A determination under subsection (1) may include 1 or more of the following orders —

(a) an order that the IPP entity must take specified action within a specified period to ensure that the IPP entity does not repeat or continue the interference with privacy;

(b) an order that the IPP entity must perform any reasonable act, or carry out any reasonable course of conduct, to redress any loss or damage suffered by any affected individual by reason of the interference with privacy;

(c) an order that it would be inappropriate for further action to be taken in relation to the interference with privacy.

Note for this subsection:

Subdivision 6 provides for the enforcement of orders under this subsection.

(3) Loss or damage referred to in subsection (2)(b) may include —

(a) an injury to the feelings of the individual; and

(b) humiliation suffered by the individual.

(4) The Information Commissioner must give the IPP entity written notice of a determination under subsection (1).

(5) The Information Commissioner may give an affected individual whose identity is known written notice of a determination under subsection (1).

(6) The Information Commissioner may make a determination under subsection (1) publicly available.

108. Review of determination

The IPP entity in relation to a which a determination is made by the Information Commissioner under section 107 may apply to the State Administrative Tribunal for a review of the determination.

109. Reports

(1) The Information Commissioner may prepare a report in relation to an investigation conducted under section 106.

(2) A report may be prepared whether or not the Information Commissioner has made a determination under section 107 following the investigation.

(3) Before including in a report any matters adverse to an IPP entity or an individual, the Information Commissioner must give a reasonable opportunity to make submissions to the Commissioner concerning those matters to —

(a) if the comment relates to an IPP entity — the principal officer of the IPP entity; or

(b) if the comment relates to an individual — the individual and any IPP entity of which the individual is an officer.

(4) If the Information Commissioner prepares a report under subsection (1), the Commissioner may do any of the following —

(a) give the report to the principal officer of the IPP entity to which it relates;

(b) give the report to the Privacy Minister;

(c) give the report to the responsible Minister for any public entity to which the report relates;

(d) make the report publicly available.

Subdivision 2 — Monitoring and assessment of compliance

110. Commissioner may monitor or conduct assessment of compliance

(1) The Information Commissioner may monitor, or conduct an assessment of, an IPP entity's compliance with any or all of its obligations under this Part and the information privacy principles.

(2) Without limiting subsection (1), the Information Commissioner may, for the purposes of monitoring or conducting an assessment under that subsection —

(a) issue a notice to produce or attend and exercise related powers under Subdivision 3; and

(b) if applicable, exercise powers under section 119.

111. Reports

(1) The Information Commissioner may prepare a report in relation to any monitoring or assessment conducted under section 110.

(2) Before including in a report any matters adverse to an IPP entity or an individual, the Information Commissioner must give a reasonable opportunity to make submissions to the Commissioner concerning those matters to —

(a) if the comment relates to an IPP entity — the principal officer of the IPP entity; or

(b) if the comment relates to an individual — the individual and any IPP entity of which the individual is an officer.

(3) If the Information Commissioner prepares a report under subsection (1), the Commissioner may do any of the following —

(a) give the report to the principal officer of the IPP entity to which it relates;

(b) give the report to the Privacy Minister;

(c) give the report to the responsible Minister for any public entity to which the report relates;

(d) make the report publicly available.

Subdivision 3 — Notices to produce or attend

112. Purposes for exercise of powers

The powers in this Subdivision may be exercised for the purpose of —

(a) under Division 9 Subdivision 5 investigating, and making a determination in relation to, a privacy complaint not resolved by conciliation; or

(b) under Subdivision 1 investigating, and making a determination in relation to, an act or practice of an IPP entity; or

(c) under Subdivision 2 monitoring, or conducting an assessment of, an IPP entity's compliance with any or all of its obligations under this Part.

113. Notice to produce or attend

(1) If the Information Commissioner has reason to believe that a person has information or a document that is relevant for a purpose referred to in section 112, the Commissioner may give the person a written notice (a ***notice to produce or attend***) requiring the person —

(a) to give to the Commissioner specified relevant information or documents; or

(b) to attend before the Commissioner to do either or both of the following —

(i) give to the Commissioner specified relevant documents;

(ii) answer relevant questions.

(2) The Information Commissioner must not give a notice to produce or attend for a purpose referred to in section 112(c) unless the Commissioner is satisfied that it is reasonable in the circumstances to do so, having regard to the following —

(a) the public interest;

(b) the impact on the person of complying with the notice;

(c) any other matters the Commissioner considers relevant.

114. Contents of notice to produce or attend

(1) A notice to produce or attend that includes a requirement to give information or documents under section 113(1)(a) must specify —

(a) the time by which, or period within which, the information or documents must be given; and

(b) the manner in which the documents must be given, which may be by electronic means.

(2) A notice to produce or attend that includes a requirement for a person to attend before the Information Commissioner under section 113(1)(b) must specify —

(a) the day and time when the person must attend; and

(b) the place at which, or means of audiovisual communication by which, the person must attend; and

(c) if documents are required to be given — the manner in which the documents must be given, which may be by electronic means.

(3) A notice to produce or attend must also include an explanation of the effect of section 117.

115. Variation or withdrawal of notice to produce or attend

The Information Commissioner may vary or withdraw a notice to produce or attend given to a person by further written notice given to the person.

116. Powers of Commissioner in relation to persons attending and documents

(1) The Information Commissioner may administer an oath or affirmation to a person attending before the Commissioner in accordance with a notice to produce or attend and may examine the person on oath or affirmation.

(2) The oath or affirmation to be taken or made by a person for the purposes of this section is an oath or affirmation that the answers the person will give will be true.

(3) The Information Commissioner may do any of the following in relation to a document given to the Commissioner in accordance with a notice to produce or attend —

(a) inspect the document;

(b) retain the document for a period the Commissioner considers reasonable;

(c) make copies of the document or any of its contents.

117. Failure to comply with notice to produce or attend

(1) A person given a notice to produce or attend must not, without reasonable excuse, refuse or fail to comply with a requirement under the notice.

Penalty for this subsection: a fine of $6 000.

(2) Without limiting what is a reasonable excuse for the purposes of subsection (1), it is a reasonable excuse to refuse or fail to comply with a requirement to give information or a document or answer questions if compliance with the requirement would require the person to give information or a document that is exempt matter for the purposes of the *Freedom of Information Act 1992* under Schedule 1 clause 1 of that Act.

(3) It is not a reasonable excuse to refuse or fail to comply with a requirement under a notice to produce or attend on the basis that compliance would be inconsistent with a secrecy provision or another duty of confidentiality or secrecy imposed by law.

(4) If a person gives information or documents, or answers questions, in good faith in compliance with a requirement under a notice to produce or attend —

(a) no civil or criminal liability is incurred in respect of the giving of the information or documents or answering of questions; and

(b) the giving of the information or documents or answering of questions is not to be regarded as a breach of any secrecy provision or other duty of confidentiality or secrecy imposed by law; and

(c) the giving of the information or documents or answering of questions is not to be regarded as a breach of professional ethics or standards or as unprofessional conduct.

[Subdivision 4 (s. 118-121) has not come into operation.]

Subdivision 5 — Compliance notices

122. Issue of compliance notice

(1) The Information Commissioner may issue a written notice (a ***compliance notice***) to an IPP entity if the Commissioner is satisfied that —

(a) an act or practice of the IPP entity constitutes an interference with the privacy of an individual; and

(b) the act or practice —

(i) has been done or engaged in repeatedly; or

(ii) constitutes a serious or flagrant interference with the privacy of an individual.

(2) A compliance notice may be issued on the Information Commissioner's own initiative, whether following a privacy complaint or an investigation under section 106 or otherwise.

(3) The compliance notice must be given to the principal officer of the IPP entity.

(4) The compliance notice must —

(a) specify the action that the IPP entity is required to take to ensure that the IPP entity does not repeat or continue the act or practice; and

(b) specify the period within which the action must be taken.

(5) The IPP entity may, before the end of the period specified in the compliance notice, apply to the Information Commissioner for an extension of the period within which the action specified in the notice must be taken.

(6) An application under subsection (5) must be in the approved form.

(7) The Information Commissioner may, on application under subsection (5), extend the period within which the action specified in the notice must be taken if —

(a) the Commissioner is satisfied that it is not reasonably practicable for the IPP entity to take the specified action within the period specified in the notice; and

(b) the IPP entity has given the Commissioner an undertaking to take the specified action within the extended period.

123. IPP entity must comply with compliance notice

The principal officer of an IPP entity to which a compliance notice is issued must take all reasonable steps to ensure that the IPP entity complies with the compliance notice.

Penalty: a fine of $60 000.

124. Review of decision to issue compliance notice

An IPP entity to which a compliance notice is issued may apply to the State Administrative Tribunal for a review of the decision to issue the compliance notice.

Subdivision 6 — Enforcement of orders made by Commissioner

125. Enforcement of orders requiring payment of compensation

(1) A person to whom a payment of an amount of compensation is to be made under an order under section 98(3)(c) or 104(2)(c) may enforce the order by filing in a court of competent jurisdiction —

(a) a copy of the order that the Information Commissioner has certified to be a true copy; and

(b) the person's affidavit as to —

(i) the amount not paid under the order; and

(ii) if the order is to take effect upon any default — the making of that default.

(2) No charge is to be made for filing a copy of an order or an affidavit under this section.

(3) On filing, the order is taken to be an order of the court and may be enforced accordingly.

126. Enforcement of other orders

(1) A person seeking to enforce an order under section 98(3)(a) or (b), 104(2)(a) or (b) or 107(2)(a) or (b) may file in the Supreme Court —

(a) a copy of the order that the Information Commissioner has certified to be a true copy; and

(b) the person's affidavit as to the non-compliance with the order; and

(c) a certificate from the Information Commissioner stating that the order is appropriate for filing in the Supreme Court.

(2) No charge is to be made for filing a copy of an order, affidavit or certificate under this section.

(3) On filing, the order is taken to be an order of the Supreme Court and may be enforced accordingly.

127. Deferral of enforcement until review proceedings concluded

An order made under section 104(2) or 107(2) cannot be filed under section 125 or 126 unless —

(a) the period within which an application may be made to the State Administrative Tribunal for a review of the determination that includes the order has passed; and

(b) if an application referred to in paragraph (a) has been made — review proceedings under the *State Administrative Tribunal Act 2004* in relation to the application have concluded.

Division 11 — Contracted service providers

128. Purpose of Division

This Division provides for how this Part and the information privacy principles apply in relation to IPP entities that are contracted service providers.

129. State services contract may provide for application of privacy obligations

A State services contract may include a provision to the effect that this Part, the information privacy principles and any applicable approved privacy code of practice apply in the manner provided for in this Division in relation to the handling of information by the contracted service provider for the purposes of the State services contract.

130. Application of information privacy principles and approved privacy codes of practice to contracted service providers

(1) If a State services contract in relation to a contracted service provider includes a provision of a kind referred to in section 129 —

(a) the information privacy principles, and any approved privacy code of practice that applies to the outsourcing entity (the ***relevant outsourcing entity***) that is a party to the contract, apply to an act done, or practice engaged in, by the contracted service provider for the purposes of the contract in the same way and to the same extent as they would apply if the act were done, or practice were engaged in, by the relevant outsourcing entity; and

(b) IPP 6, and any approved privacy code of practice that applies to the contracted service provider, apply to information held by the contracted service provider in connection with services provided under the contract.

(2) The information privacy principles, and any approved privacy code of practice, apply to a contracted service provider only to the extent provided for in subsection (1) and not otherwise.

131. Privacy codes of practice or amendments submitted by contracted service providers

(1) If a contracted service provider submits a privacy code of practice, or an amendment to an approved privacy code of practice, to the Information Commissioner under section 29(1), the Commissioner must give written notice of the submission to each relevant outsourcing entity.

(2) A ***relevant outsourcing entity*** for the purposes of subsection (1) is an outsourcing entity that is a party to a State services contract, if the privacy code of practice or the amended approved privacy code of practice (as the case requires) would apply in relation to the handling of information by the contracted service provider for the purposes of the contract.

132. Requests for access and correction made to contracted service providers

(1) A contracted service provider to which a request for access or correction under IPP 6 or an applicable approved privacy code of practice is made must —

(a) notify the relevant outsourcing entity of the request as soon as practicable; and

(b) consult with the relevant outsourcing entity in relation to dealing with the request.

(2) The ***relevant outsourcing entity*** for the purposes of subsection (1) is the outsourcing entity that is a party to the State services contract in connection with which the contracted service provider holds the information in relation to which the request is made.

(3) In dealing with a request for access or correction under IPP 6 or an applicable approved privacy code of practice, a contracted service provider must have regard to any privacy guidelines in relation to requests under IPP 6 made to contracted service providers.

133. Public interest determinations and temporary public interest determinations applying to contracted service providers

(1) If a contracted service provider makes an application under section 46 for a public interest determination, or an application under section 50 for a temporary public interest determination, the Information Commissioner must give each relevant outsourcing entity a written notice that —

(a) states that the application has been received from the contracted service provider; and

(b) specifies the act or practice, and the information privacy principle or approved privacy code of practice, or both, to which the application relates; and

(c) in the case of an application for a public interest determination —

(i) invites the relevant outsourcing entity to make submissions in relation to the application in accordance with the notice made publicly available in relation to the application under section 47(1)(a); and

(ii) specifies the manner in which, and period within which, those submissions must be made.

(2) If the Information Commissioner gives a notice under section 54(3)(a) in relation to the proposed revocation of a public interest determination or temporary public interest determination to an IPP entity that is a contracted service provider, the Commissioner must also give a copy of the notice to each relevant outsourcing entity.

(3) A ***relevant outsourcing entity*** for the purposes of subsection (1) or (2) is an outsourcing entity that is a party to a State services contract, if the public interest determination or temporary public interest determination (as the case requires) applies or would apply in relation to an act or practice done or engaged in by the contracted service provider for the purposes of the contract.

*[**134-136.** Have not come into operation.]*

137. Privacy impact assessments by contracted service providers

(1) If a State services contract in relation to a contracted service provider includes a provision of a kind referred to in section 129, sections 79 and 80 apply to a contracted service provider in relation to a function or activity carried out, or proposed to be carried out, for the purposes of the State services contract.

(2) Sections 79 and 80 apply to a contracted service provider only to the extent provided for in subsection (1) and not otherwise.

138. Directions about privacy impact assessments given to contracted service providers

(1) If the Information Commissioner gives a direction under section 80(1) to an IPP entity that is a contracted service provider, the Commissioner must also give a copy of the direction to the relevant outsourcing entity.

(2) The ***relevant outsourcing entity*** for the purposes of subsection (1) is the outsourcing entity that is a party to the State services contract for the purposes of which the contracted service provider carries out, or proposes to carry out, the function or activity to which the direction relates.

139. Notices relating to privacy complaints or investigations about contracted service providers

(1) If the Information Commissioner gives a notice in relation to a privacy complaint, or a determination of a privacy complaint, under Division 9 to a respondent that is a contracted service provider, the Commissioner must also give a copy of the notice to the relevant outsourcing entity.

(2) If the Information Commissioner gives a notice in relation to an investigation under section 106, or a determination under section 107, to an IPP entity that is a contracted service provider, the Commissioner must also give a copy of the notice to the relevant outsourcing entity.

(3) The ***relevant outsourcing entity*** for the purposes of subsection (1) or (2) is the outsourcing entity that is a party to the State services contract for the purposes of which the contracted service provider did the act, or engaged in the practice, to which the complaint, investigation or determination relates.

140. Enforcement action may be taken against outsourcing entity in some circumstances

(1) In this section —

enforcement action means —

(a) making, dealing with or determining a privacy complaint under Division 9; or

(b) investigating, or making a determination in relation to, an act or practice under Division 10 Subdivision 1; or

(c) exercising any power under Division 10 for the purpose of a matter referred to in paragraph (a) or (b);

insolvent —

(a) in relation to an individual — means that the individual is, according to the *Interpretation Act 1984* section 13D, a bankrupt or a person whose affairs are under insolvency laws; or

(b) in relation to a body corporate — means that —

(i) a liquidator, provisional liquidator or receiver has been appointed in relation to the body corporate; or

(ii) the body corporate is otherwise being wound up;

relevant act or practice means an act or practice of a contracted service provider that is done or engaged in for the purposes of a State services contract, or in relation to information held in connection with services provided under a State services contract;

relevant outsourcing entity, in relation to a relevant act or practice, means the outsourcing entity that is a party to the State services contract in connection with which the relevant act or practice is done or engaged in.

(2) If, at the time of a relevant act or practice of a contracted service provider, the State services contract does not include a provision of the kind referred to in section 129, then any enforcement

action in relation to the act or practice may be taken in relation to the relevant outsourcing entity as if the act or practice had been done or engaged in by the relevant outsourcing entity instead of the contracted service provider.

(3) If subsection (2) does not apply, but any enforcement action cannot be taken in relation to a relevant act or practice of a contracted service provider because at the time of the proposed enforcement action the contracted service provider has died, ceased to exist or become insolvent, the enforcement action may instead be taken in relation to the relevant outsourcing entity as if it were the contracted service provider and had done or engaged in the relevant act or practice.

(4) If a privacy complaint is made in relation to a relevant act or practice of a contracted service provider and the contracted service provider dies, ceases to exist or becomes insolvent before the Information Commissioner makes a determination under section 104 in relation to the complaint, the Commissioner may amend the complaint to substitute the relevant outsourcing entity as the respondent, instead of the contracted service provider.

(5) If the Information Commissioner makes an order under section 98(3)(c) or 104(2)(c) requiring the payment of compensation by a contracted service provider in relation to a relevant act or practice, and the contracted service provider dies, ceases to exist or becomes insolvent before the compensation is paid or recovered, the Commissioner may amend the order so that it applies to the relevant outsourcing entity instead of the contracted service provider.

(6) Before making an amendment under subsection (4) or (5), the Information Commissioner must give the relevant outsourcing entity written notice of, and a reasonable opportunity to make submissions on, the proposed amendment.

Division 12 — Administration

Subdivision 1 — Functions under this Act of Information Commissioner and Privacy Deputy Commissioner

141. Functions of Information Commissioner and Privacy Deputy Commissioner under this Act

(1) The Information Commissioner has the following functions under this Act —

(a) to promote the understanding of matters relating to the information privacy principles and this Part;

(b) to promote the objects of this Act set out in section 3(a) to (e);

(c) to promote compliance with the information privacy principles and this Part;

(d) to prepare and make available information and material in relation to protecting the privacy of personal information;

(e) to provide assistance to members of the public and IPP entities in relation to any matter relevant to the operation of this Part;

(f) to undertake reviews of any matter relating to the privacy of personal information, on request by the Privacy Minister or on the Commissioner's own initiative;

(g) to report and make recommendations on any matter relating to the privacy of personal information;

(h) to undertake, participate in or promote research in relation to any matter relating to the privacy of personal information;

(i) any other function given to the Information Commissioner under this Act.

(2) The Privacy Deputy Commissioner also has all the functions of the Information Commissioner under this Act, other than the following —

(a) giving approvals under section 142(3) and directions under section 142(4);

(b) any function in relation to a report under Subdivision 2;

(c) any function in relation to consultation under section 202(2) or serving as a member of the Privacy and Responsible Information Sharing Advisory Committee.

Note for this section:

The *Information Commissioner Act 2024* sections 25 and 27 provide for the functions of the Information Commissioner and Privacy Deputy Commissioner generally.

142. Performance of privacy functions

(1) The functions under this Act that are functions of both the Information Commissioner and the Privacy Deputy Commissioner are the ***privacy functions***.

(2) A privacy function may be performed —

(a) by the Information Commissioner; or

(b) by the Privacy Deputy Commissioner, subject to subsection (3) and any direction given under subsection (4).

(3) The Privacy Deputy Commissioner must obtain the approval of the Information Commissioner before performing any of the following privacy functions —

(a) making a public interest determination under section 45(1);

(b) making a temporary public interest determination under section 49(1);

(c) extending a temporary public interest determination under section 52(3);

(d) revoking a public interest determination or temporary public interest determination under section 54(1) or (2);

(e) making a notifiable information breach determination under section 60(1);

(f) amending or repealing a notifiable information breach determination;

(g) issuing privacy guidelines under section 148(1);

(h) amending or revoking privacy guidelines under section 148(2).

(4) The Information Commissioner may direct the Privacy Deputy Commissioner as to —

(a) which of the privacy functions the Privacy Deputy Commissioner is to perform; and

(b) the manner in which the Privacy Deputy Commissioner must perform any privacy function.

(5) If the Privacy Deputy Commissioner performs a privacy function —

(a) the Privacy Deputy Commissioner performs the function in the Privacy Deputy Commissioner's own right and not on behalf of the Information Commissioner; and

(b) the Privacy Deputy Commissioner may perform the function upon the Privacy Deputy Commissioner's own belief or state of mind (to the extent that the performance or exercise is dependent on the belief or state of mind of the Information Commissioner); and

(c) the performance of the function is as effectual for all purposes as if it were performed by the Information Commissioner; and

(d) a reference in this Act or another written law to anything done by, to, or in relation to, the Information Commissioner in connection with the function includes a reference to the thing as done by, to, or in relation to, the Privacy Deputy Commissioner; and

(e) the Information Commissioner is not prevented from performing the same function on another occasion (in relation to a different matter).

143. Certain functions cannot be delegated

The following privacy functions cannot be delegated by the Information Commissioner or the Privacy Deputy Commissioner under the *Information Commissioner Act 2024* section 28 —

(a) making a public interest determination under section 45(1);

(b) making a temporary public interest determination under section 49(1);

(c) extending a temporary public interest determination under section 52(3);

(d) revoking a public interest determination or temporary public interest determination under section 54(1) or (2);

(e) making a notifiable information breach determination under section 60(1);

(f) amending or repealing a notifiable information breach determination;

(g) making an order to give effect to a conciliation agreement under section 98(3);

(h) determining a privacy complaint under section 104(1);

(i) making a determination following an investigation under section 107(1);

(j) issuing a compliance notice under section 122(1);

(k) issuing privacy guidelines under section 148(1);

(l) amending or revoking privacy guidelines under section 148(2).

144. Information Commissioner and Privacy Deputy Commissioner must have regard to objects of Act in performing functions

In performing their functions under this Act, the Information Commissioner and Privacy Deputy Commissioner must have regard to the objects of this Act.

145. Information Commissioner and Privacy Deputy Commissioner may request IPP entity to provide assistance

The Information Commissioner or Privacy Deputy Commissioner may request an IPP entity to provide any assistance that that Commissioner reasonably considers appropriate to perform their functions under this Act.

Subdivision 2 — Reporting

146. Matters to be included in annual report to Parliament

(1) Without limiting the *Information Commissioner Act 2024* section 32, the Information Commissioner must include the following information in the annual report required under that section for a financial year —

(a) the number of applications for public interest determinations made under section 46 and the outcome of those applications;

(b) the number of applications for temporary public interest determinations made under section 50 and the outcome of those applications;

(c) the number of applications for extensions of temporary public interest determinations made under section 52(1) and the outcome of those applications;

(d) the number of privacy complaints made and the outcome of those complaints;

(e) the number of applications for review made to the State Administrative Tribunal under

sections 70(5), 90(5), 91(3), 105, 108 and 124 and the outcome of those applications;

(f) the number of appeals made to the Supreme Court under the *State Administrative Tribunal Act 2004* section 105 from decisions of the State Administrative Tribunal on applications referred to in paragraph (e) and the outcome of those appeals;

(g) the number of notifiable information breaches notified under section 62;

(h) the number, or an estimate of the number, of affected individuals in relation to notifiable information breaches notified under section 62;

(i) the number of compliance notices issued under section 122;

(j) any other information prescribed by the regulations.

(2) A public entity must provide the Information Commissioner with any information the Information Commissioner requires for the purposes of including the matters referred to in subsection (1) in the annual report.

147. Special reports to Parliament

(1) The Information Commissioner may, if the Information Commissioner considers it to be in the public interest to do so —

(a) prepare a report on —

(i) any matter arising in connection with the performance of the privacy functions; or

(ii) any act or practice of an IPP entity that the Information Commissioner considers to be an interference with the privacy of an individual;

and

(b) submit the report to the President of the Legislative Council and the Speaker of the Legislative Assembly.

(2) A report under subsection (1) may include recommendations.

(3) The President or Speaker must cause a copy of a report submitted to them under subsection (1) to be laid before the Legislative Council or Legislative Assembly, as the case requires, within 15 sitting days of that House after the report is submitted.

Subdivision 3 — Guidelines, documents and notices

148. Privacy guidelines

(1) The Information Commissioner may issue guidelines —

(a) in relation to any matter required or permitted by this Part or section 176 to be the subject of privacy guidelines; or

(b) to provide information and guidance in relation to the application and administration of the information privacy principles and this Part.

(2) The Information Commissioner may amend or revoke privacy guidelines.

(3) The Information Commissioner may consult with any person or body the Commissioner considers appropriate before issuing, amending or revoking any privacy guidelines.

(4) The Information Commissioner must ensure that privacy guidelines are made publicly available.

Note for this section:

Section 221 makes provision for the status and effect of privacy guidelines.

149. Making documents publicly available

(1) The regulations may make provision for how documents are to be made publicly available by the Information Commissioner or an entity for the purposes of any provision of this Part.

(2) If a provision of this Part requires or permits the Information Commissioner to make a document publicly available, the Commissioner must comply with that requirement or exercise that power —

(a) if regulations under subsection (1) apply — in accordance with those regulations; or

(b) otherwise — by making the document publicly available in the manner the Commissioner considers appropriate.

150. Notices of decisions or determinations

Without limiting any other provision of this Part, the Information Commissioner must include the following information in a notice of a decision or determination of the Commissioner given under this Part —

(a) the day on which the decision or determination was made;

(b) the name and designation of the person who made the decision or determination;

(c) the reasons for the decision or determination;

(d) any right under this Act to apply for a review of the decision or determination.

Division 13 — General

151. Privacy officers of public entities

(1) The principal officer of a public entity must ensure that the principal officer, or another senior officer, of the entity is designated as the privacy officer for the public entity.

(2) A privacy officer of a public entity is responsible for the following —

(a) promoting the public entity's compliance with the information privacy principles and this Part;

(b) assisting in the preparation of the public entity's information breach policy under section 73;

(c) assisting in the establishment and maintenance of the public entity's register of notifiable information breaches under section 74;

(d) assisting in the conduct of privacy impact assessments by the public entity under sections 79 and 80;

(e) coordinating the public entity's response to complaints made to the public entity in relation to acts or practices of the public entity that may constitute an interference with the privacy of an individual;

(f) coordinating the public entity's dealings with the Information Commissioner in relation to —

(i) privacy impact assessments conducted by the public entity under sections 79 and 80; and

(ii) privacy complaints in relation to the public entity; and

(iii) any investigation, monitoring or assessment conducted by the Commissioner under Division 10 in relation to the public entity.

(3) The principal officer of a public entity must ensure that the Information Commissioner is notified of —

(a) the name and contact details of the privacy officer; and

(b) any change to the individual designated as privacy officer or to the privacy officer's contact details.

152. Nature of privacy rights created by this Act

(1) Except in accordance with the procedures set out in this Act, nothing in Division 2, 3, 4, 6, 7, 8 or 11, an approved privacy code of practice or the information privacy principles —

(a) gives rise to a civil cause of action; or

(b) operates to create in any person a legal right enforceable in a court or tribunal.

(2) A contravention of Division 2, 3, 4, 6, 7, 8 or 11, an approved privacy code of practice or the information privacy principles does not give rise to an offence except to the extent expressly provided by this Part.

(3) A failure to comply with an information privacy principle or approved privacy code of practice does not invalidate any decision made, or thing done, by an IPP entity.

153. Interaction with other laws

(1) Nothing in this Part or the information privacy principles limits the operation of the *Freedom of Information Act 1992* or the *State Records Act 2000*.

(2) The information privacy principles and approved privacy codes of practice do not limit the operation of other secrecy provisions that apply to information.

(3) If an enactment is expressed to apply despite the *Freedom of Information Act 1992*, or to disapply or limit the application of the *Freedom of Information Act 1992* or Parts 2 and 4 of that Act in relation to any matter, then (as the case requires) the enactment also applies despite, or disapplies or so limits, any application in the circumstances of —

(a) IPP 6; or

(b) an approved privacy code of practice that provides for modifications to the application of IPP 6 or for how IPP 6 is to be applied or complied with.

154. Exercise of powers relating to consent and access by authorised representative of individual

(1) In this section —

authorised representative, in relation to an individual —

(a) means a person who is —

(i) a guardian or enduring guardian (as those terms are defined in the *Guardianship and Administration Act 1990* section 3(1)) of the individual; or

(ii) an attorney for the individual under an enduring power of attorney; or

(iii) an administrator (as defined in the *Guardianship and Administration Act 1990* section 3(1)) of the individual's estate; or

(iv) a person authorised to make treatment decisions for the individual under the *Guardianship and Administration Act 1990* Part 9C or 9D; or

(v) if the individual is a child — a parent or guardian of the child; or

(vi) otherwise empowered under law to perform any functions or duties, or exercise powers, as an agent or in the best interests of the individual;

but

(b) does not include a person acting as referred to in paragraph (a) in a manner that is inconsistent with an order made by a court or tribunal.

(2) If an information privacy principle or approved privacy code of practice requires the consent of an individual to the collection, holding, management, use or disclosure of personal information, an authorised representative of the individual may give consent if —

(a) the individual is incapable of giving consent; and

(b) the consent is reasonably necessary for the lawful performance of functions or duties or exercise of powers in relation to the individual by the authorised representative.

(3) If an information privacy principle or approved privacy code of practice permits an individual to request access to or correction of personal information, or confers on an individual a right of access to personal information, the power to make that request, or that right of access, may be exercised —

(a) by the individual personally, unless the individual is a child who is incapable of making the request; or

(b) by an authorised representative of the individual if —

(i) the individual is incapable of making the request or exercising the right of access; and

(ii) the personal information to be accessed, or the correction of the personal information, is reasonably necessary for the lawful performance of functions or duties or exercise of powers in relation to the individual by the authorised representative.

(4) For the purposes of this section and the information privacy principles, an individual is incapable of giving consent, making a request or exercising a right of access if the individual, by reason of age, injury, disease, senility, illness, disability, physical impairment or mental disorder, is incapable (despite the provision of reasonable assistance by another individual) of —

(a) understanding the general nature and effect of giving the consent, making the request or exercising the right of access (as the case requires); or

(b) communicating the consent or refusal of consent, making the request or personally exercising the right of access (as the case requires).

(5) An authorised representative of an individual must not give consent under subsection (2), or make a request under subsection (3), if the authorised representative knows or believes that the consent or request does not accord with wishes expressed, and not changed or withdrawn, by the individual before the individual became incapable of giving the consent or making the request.

(6) A consent given, or request made, in circumstances referred to in subsection (5) is of no effect.

(7) An IPP entity may refuse a request by an authorised representative of an individual for access to personal information that relates to the individual if the IPP entity believes on reasonable grounds that access by the authorised representative may endanger the individual or any other individual.

155. Review of privacy provisions of Act

(1) In this section —

privacy provisions means the following —

(a) this Part;

(b) Schedule 1;

(c) the provisions of Parts 1, 4 and 5, to the extent that those provisions relate to terms or matters relevant to this Part and Schedule 1;

(d) regulations made for the purposes of provisions referred to in paragraphs (a) to (c).

(2) The Privacy Minister must review the operation and effectiveness of the privacy provisions, and prepare a report based on the review —

(a) as soon as practicable after the 3rd anniversary of the day on which section 20 comes into operation; and

(b) after that, at intervals of not more than 5 years.

(3) The Privacy Minister must cause the report to be laid before each House of Parliament as soon as practicable after it is prepared, but not later than 12 months after the 3rd anniversary or the expiry of the period of 5 years, as the case may be.

Part 3 — Responsible information sharing

Division 1 — Key concepts and preliminary matters

156. Special information sharing entities and external entities

(1) A ***special information sharing entity*** is —

(a) a judicial body; or

(b) a public entity that is an exempt agency as defined in the *Freedom of Information Act 1992* Glossary clause 1; or

(c) another public entity prescribed by the regulations.

(2) An ***external entity*** —

(a) is any of the following —

(i) an agency or instrumentality of the Commonwealth, another State or a Territory;

(ii) a contracted service provider;

(iii) an Aboriginal community controlled organisation;

(iv) a person or body that provides or promotes social services as defined in the *Children and Community Services Act 2004* section 3;

(v) a higher education provider, as defined in the *Tertiary Education Quality and Standards Agency Act 2011* (Commonwealth) section 5, that is registered in the "Australian University" provider category under that Act;

(vi) a body that carries out health-related research;

(vii) any other body, or the holder of any other office, that is prescribed by the regulations;

but

(b) does not include a public entity.

157. Government information

The ***government information*** of a public entity —

(a) is the information (including personal information) held by the public entity; but

(b) does not include any exempt information held by the public entity.

158. Exempt information

(1) The following information is ***exempt information*** —

(a) information the disclosure of which would reasonably be expected to reveal, or enable to be ascertained, the identity of any person as —

(i) a confidential source of information in relation to the enforcement of a law; or

(ii) a person who is the subject of enforcement proceedings under a law; or

(iii) a person who has made an appropriate disclosure of public interest information under the *Public Interest Disclosure Act 2003*; or

(iv) a person in respect of whom a disclosure of public interest information has been made under the *Public Interest Disclosure Act 2003*; or

(v) a participant in a witness protection program; or

(vi) a person who has made, or a person who is mentioned in, a report under the *Children and Community Services Act 2004* section 124B(1); or

(vii) a person who is a notifier as defined in the *Children and Community Services Act 2004* section 240(1) or a person about whom the information mentioned in that definition is given; or

(viii) a person who has made, or a person who is mentioned in, a report under the *Parliamentary Commissioner Act 1971* section 19T; or

(ix) a person who has given, or a person who is mentioned in, a notification under the *Family Court Act 1997* section 160(2) or (3); or

(x) a person who has given, or a person who is mentioned in, a notification under the *Family Law Act 1975* (Commonwealth) section 67ZA(2) or (3); or

(xi) a person in relation to whom information is contained in the Community Protection Offender Register established under the *Community Protection (Offender Reporting) Act 2004* section 80; or

(xii) a person on whom an abortion has been performed or who has performed, or assisted in the performance of, an abortion (as defined in the *Public Health Act 2016* section 202MB); or

(xiii) a patient who has requested access to, or accessed, voluntary assisted dying under the *Voluntary Assisted Dying Act 2019* or a person who has acted as a coordinating practitioner, consulting practitioner or administering practitioner under that Act;

(b) information the disclosure of which could reasonably be expected to reveal, or enable to be ascertained —

(i) the identity of a person who is a complainant (as defined in the *Evidence Act 1906* section 36C(4)) in relation to a person accused of, or an accusation alleging, a sexual offence (as defined in section 36A(1) of that Act); or

(ii) the school that a complainant referred to in subparagraph (i) attends;

(c) information the disclosure of which could reasonably be expected to prejudice national security;

(d) information the disclosure of which could reasonably be expected to reveal, or enable to be ascertained, investigative measures or procedures of a law enforcement agency;

(e) information that is —

(i) restricted matter as defined in the *Corruption, Crime and Misconduct Act 2003* section 151(1); or

(ii) subject to a notation under section 99 of that Act;

(f) information of a kind referred to in, or contained in a document referred to in, the *Equal Opportunity Act 1984* section 167(1)(a) or (c) or (2)(a) or (b);

(g) information of a kind referred to in the *Inspector of Custodial Services Act 2003* section 47(1) or to which a direction under section 48 of that Act applies;

(h) information of a kind referred to in, or contained in a document referred to in, the *Legal Aid Commission Act 1976* section 64(2)(a) or (b) or (3) (other than administrative information as defined in section 64(2b) of that Act);

(i) information of a kind referred to in the *Parliamentary Commissioner Act 1971* section 23(1) or to which a direction under section 23(1a) of that Act applies;

(j) information the disclosure of which could reasonably be expected to reveal, or enable to be ascertained, information relating to —

(i) the adoption of a child or arrangements or negotiations for, towards, or with a view to, the adoption of a child; or

(ii) the participation of a person in an ART procedure (as defined in the *Assisted*

Reproductive Technology and Surrogacy Act 2025 section 8) or a person born as a result of an ART procedure;

(k) entry registration information as defined in the *Protection of Information (Entry Registration Information Relating to COVID-19 and Other Infectious Diseases) Act 2021* section 3;

(l) information obtained under a taxation Act as defined in the *Taxation Administration Act 2003* Glossary clause 1;

(m) confidential information as defined in the *First Home Owner Grant Act 2000* section 65(7);

(n) information given to the Treasurer under the *Bank of Western Australia Act 1995* section 22 or to the Minister responsible for the administration of that Act under section 42O of that Act;

(o) sensitive Aboriginal family history information, or sensitive Aboriginal traditional information, given in relation to an application or potential application under the *Native Title Act 1993* (Commonwealth) section 61 (whether given by or on behalf of the applicant or potential applicant or otherwise);

(p) a photograph or signature referred to in paragraph (a) or (b) of the definition of ***identifying information*** in the *Road Traffic (Authorisation to Drive) Act 2008* section 11B(1);

(q) a photograph or signature referred to in paragraph (a) or (b) of the definition of ***identifying information*** in the *Western Australian Photo Card Act 2014* section 12(1);

(r) information of a class prescribed by the regulations.

(2) Without limiting subsection (1) but subject to subsection (3), information is also ***exempt information*** if the information originated with or was obtained from any of the following special information sharing entities (including staff under the control of any of the following special information sharing entities) —

(a) the Auditor General appointed under the *Auditor General Act 2006* or the Office of the Auditor General;

(b) the Corruption and Crime Commission established under the *Corruption, Crime and Misconduct Act 2003* section 8;

(c) the Director of Public Prosecutions appointed under the *Director of Public Prosecutions Act 1991* section 5;

(d) the Information Commissioner;

(e) the Parliamentary Commissioner for Administrative Investigations;

(f) the Public Sector Commissioner, but only in relation to their functions under the *Corruption, Crime and Misconduct Act 2003*;

(g) a judicial body;

(h) a special information sharing entity prescribed by the regulations.

(3) Information (other than information to which subsection (1) applies) that originated with or was obtained from a special information sharing entity referred to in subsection (2) is not ***exempt information*** in relation to —

(a) an information sharing request made to the special information sharing entity; or

(b) an information sharing agreement or proposed information sharing agreement under which the special information sharing entity is a provider or proposed provider in relation to the information.

[Section 158 amended: No. 19 of 2025 s. 384.]

159. Permitted purposes for sharing of information

(1) A ***permitted purpose*** is a purpose for which, under subsections (2) and (3), information may be handled under an information sharing agreement.

(2) Information may be handled under an information sharing agreement for any of the following purposes —

(a) to inform or enable the making or implementation of government policy;

(b) to inform or enable the design, management, delivery or evaluation of government programs and services;

(c) to inform or enable research and development with clear and direct benefits to the public;

(d) to inform or enable emergency management (including prevention of, preparedness for, response to, and recovery from, emergencies);

(e) any other purpose prescribed by the regulations.

(3) Despite subsection (2), information cannot be handled under an information sharing agreement for —

(a) a purpose that relates to a law enforcement function of a law enforcement agency (other than a community policing function of the Police Force of Western Australia that is prescribed by the regulations for the purposes of this paragraph); or

(b) a purpose that relates to determining whether a person has complied with a law or monitoring compliance with a law; or

(c) a purpose that relates to national security; or

(d) a primary purpose of obtaining commercial gain.

(4) Subsection (3) applies even if the purpose referred to in subsection (3) is also of a kind referred to in subsection (2).

Division 2 — Information sharing requests

160. Information sharing request

(1) A public entity may, by written notice, request another public entity to disclose government information under this Part to the public entity making the request.

(2) An external entity may, by written notice, request a public entity to disclose government information under this Part to the external entity making the request.

(3) If an entity makes a request under subsection (1) or (2) —

(a) the request is an ***information sharing request***; and

(b) the public entity to which the request is made is the ***holding entity***; and

(c) the public entity or external entity that makes the request is the ***requesting entity***.

(4) An information sharing request must be given to the principal officer of the holding entity and must state —

(a) that the request is an information sharing request for the purposes of this Act; and

(b) the government information of the holding entity to which the request relates; and

(c) the permitted purpose for which the information would be handled; and

(d) the activity that would be carried out for that permitted purpose by the requesting entity using the information; and

(e) how the information would be used for the purposes of that activity; and

(f) how the requesting entity would otherwise handle the information.

(5) A requesting entity may withdraw an information sharing request.

161. Response to information sharing request

(1) If an information sharing request is made under section 160 and is not withdrawn, the holding entity must give the requesting entity a written notice responding to the request in accordance with subsection (2) within —

(a) 45 days after the day on which the request is made; or

(b) a longer period agreed with the requesting entity.

(2) A notice responding to an information sharing request must do 1 of the following —

(a) state that the holding entity —

(i) considers that the requested information may be disclosed to the requesting entity otherwise than under this Part; and

(ii) agrees to disclose the requested information to the requesting entity;

(b) state that the holding entity may be willing to disclose some or all of the requested information to the requesting entity under this Part, subject to conducting the required assessments under Division 4 Subdivision 2 and entering into an information sharing agreement providing for the disclosure;

(c) state that the holding entity refuses to disclose the requested information and the reasons for the refusal.

(3) Despite subsection (1), a holding entity is not required to respond to an information sharing request if —

(a) either or both of the following apply —

(i) the holding entity is a special information sharing entity;

(ii) the requesting entity is an external entity;

and

(b) the holding entity does not intend to share the requested information with the requesting entity.

(4) A holding entity is not bound by any response that the holding entity gives to an information sharing request.

(5) If the requesting entity is a public entity, a response to an information sharing request must be given to the principal officer of the entity.

162. No obligation to disclose requested information

(1) A holding entity to which an information sharing request is made may refuse to disclose information to which the request relates if, for any reason, the holding entity considers that the information should not be disclosed to the requesting entity.

(2) Without limiting subsection (1), the holding entity may refuse to disclose information because —

(a) the information would be privileged from production in legal proceedings on the ground of legal professional privilege; or

(b) the disclosure of the information would constitute a breach of any of the following —

(i) a contract;

(ii) an obligation of confidence for which a legal or equitable remedy could be obtained;

(iii) an order of a court or tribunal;

or

(c) the disclosure or proposed use of the information would contravene —

(i) a law of the State (whether or not that law could be overridden by section 187); or

(ii) a law of the Commonwealth, another State or a Territory;

or

(d) the disclosure or proposed use of the information would be likely to prejudice —

(i) an investigation of any contravention or possible contravention of a law of the State, the Commonwealth, another State or a Territory; or

(ii) the administration or enforcement of a law of the State, the Commonwealth, another State or a Territory; or

(iii) a proceeding before a court or tribunal; or

(iv) any disciplinary proceedings; or

(v) a coronial investigation or inquest;

or

(e) the disclosure or proposed use of any of the information could reasonably be expected to result in —

(i) a serious threat to the life, health, safety or welfare of any individual; or

(ii) a threat to the life, health, safety or welfare of any individual due to family violence.

Division 3 — Information sharing directions

163. Responsible Minister for public entity may direct sharing of information

(1) The responsible Minister for a public entity (other than a special information sharing entity) may give the public entity a written direction (an ***information sharing direction***) requiring the

public entity to enter into an information sharing agreement that provides for —

(a) the disclosure for a permitted purpose of government information by the public entity to —

(i) another public entity; or

(ii) an external entity;

and

(b) the collection, holding, management and use of that information by that other entity for a permitted purpose.

(2) If there is more than 1 responsible Minister for the public entity, an information sharing direction can be given to the public entity only by the Minister principally responsible for the functions or activities of the public entity for the purposes of which the relevant government information is held.

(3) An information sharing direction must be given to the principal officer of the public entity and must —

(a) identify the public entity to which it is given; and

(b) identify the public entity or external entity with which the information sharing agreement is required to be entered into; and

(c) describe the information sharing agreement that the public entity is required to enter into, including —

(i) the information that may be handled under the agreement; and

(ii) the permitted purpose for which the information may be handled; and

(iii) the activity to be carried out for that permitted purpose using the information.

(4) An information sharing direction cannot be given in relation to government information of a public entity unless —

(a) an information sharing request has previously been given to the public entity in relation to the information; and

(b) the public entity has —

(i) not responded to the request within 45 days after the day on which the request is made, or a longer period agreed with the requesting entity; or

(ii) responded to the request by refusing to disclose the information;

and

(c) the responsible Minister is satisfied that —

(i) the purpose referred to in subsection (3)(c)(ii) is a permitted purpose; and

(ii) the proposed handling of information contemplated by the direction will be consistent with the responsible sharing principles and appropriate in all the circumstances.

164. Notice of direction must be laid before Houses of Parliament

(1) A responsible Minister who gives an information sharing direction to a public entity must, within 14 days after the day on which the direction is given, cause notice of the direction to be —

(a) laid before each House of Parliament or dealt with under section 220; and

(b) given to the Chief Data Officer.

(2) A notice required under subsection (1) must state —

(a) the matters referred to in section 163(3); and

(b) the reasons why the responsible Minister is satisfied that the proposed handling of information contemplated by

the direction will be consistent with the responsible sharing principles and appropriate in all the circumstances.

165. Revocation of direction

(1) A responsible Minister who gives an information sharing direction to a public entity may revoke the direction by written notice given to the public entity.

(2) A responsible Minister who revokes an information sharing direction must cause notice of the revocation to be given to the Chief Data Officer.

166. Requirement to comply with direction

If an information sharing direction has been given and not revoked, the public entity given the direction must take all reasonable steps to —

(a) enter into an information sharing agreement in compliance with the direction; and

(b) disclose information in accordance with the agreement.

167. Division has effect subject to laws restricting Ministerial direction

(1) This section applies if there is a conflict or inconsistency between —

(a) this Division; and

(b) a provision of another written law that —

(i) provides that a public entity is not subject to direction by a Minister; or

(ii) restricts the extent to which a public entity is subject to direction by a Minister.

(2) The provision referred to in subsection (1)(b) prevails over this Division.

Division 4 — Information sharing agreements

Subdivision 1 — Entry into and contents of information sharing agreement

168. Information sharing agreement

(1) An ***information sharing agreement*** is a written agreement entered into in accordance with the requirements of this Division that provides for —

(a) the disclosure for a permitted purpose of government information by a public entity to —

(i) another public entity; or

(ii) an external entity;

and

(b) the collection, holding, management and use of that information by that other entity for a permitted purpose; and

(c) the activity (the ***relevant activity***) to be carried out for that permitted purpose using the information.

(2) A public entity that discloses information under an information sharing agreement (otherwise than as provided for under section 172) is a ***provider*** under the agreement.

(3) A public entity or external entity that collects, holds, manages and uses information disclosed to it under an information sharing agreement (otherwise than as provided for under section 172) is a ***recipient*** under the agreement.

(4) An information sharing agreement —

(a) may be a multilateral agreement involving 2 or more providers, or 2 or more recipients, or both; and

(b) may provide for a public entity to be both a provider and a recipient under the agreement in relation to different information.

(5) Each provider and each recipient under an information sharing agreement must be a party to the agreement.

169. Entering into information sharing agreement

(1) A public entity may enter into an information sharing agreement if —

(a) an associated information sharing request has been made under Division 2; or

(b) the agreement is entered into in compliance with an information sharing direction given under Division 3.

(2) An information sharing request is ***associated*** with an information sharing agreement for the purposes of subsection (1) if —

(a) the requesting entity in relation to the request is a recipient under the agreement (whether or not there are other recipients); and

(b) the holding entity in relation to the request is a provider under the agreement (whether or not there are other providers); and

(c) the information to which the request relates is or includes information to which the agreement relates (whether or not the agreement also relates to other information).

(3) Before entering into an information sharing agreement, each proposed provider and proposed recipient must comply with the applicable requirements of Subdivision 2.

170. Matters to be included in information sharing agreement

An information sharing agreement must —

(a) identify each party to the agreement and whether the party is —

(i) a provider; or

(ii) a recipient; or

(iii) both a provider and a recipient;

and

(b) state that the agreement is an information sharing agreement for the purposes of this Act; and

(c) provide for the term of the agreement, which must not be more than 5 years; and

(d) describe —

(i) the information that may be handled under the agreement; and

(ii) the permitted purpose for which the information may be handled; and

(iii) the relevant activity to be carried out using the information for that purpose; and

(iv) if the relevant activity is to involve the use or interpretation of the information to generate new information (***derived information***) — the derived information to be generated;

and

(e) require each recipient under the agreement to comply with sections 192, 193 and 194(4) in relation to a shared information breach or suspected shared information breach involving information disclosed under the agreement; and

(f) provide for the consequences of non-compliance with sections 192, 193 or 194(4) by a recipient; and

(g) provide for the consequences of a party withdrawing from the agreement; and

(h) include provisions about how the disclosed information will be treated —

(i) when the agreement ceases to be in force; or

(ii) if a party withdraws from the agreement;

and

(i) include any other matters the agreement is required to include under section 171 and Subdivision 2; and

(j) include any other matters prescribed by the regulations.

171. Other matters to be included in information sharing agreement

(1) If any secrecy provision would be contravened by the handling of information under an information sharing agreement but for the effect of section 187, the agreement must —

(a) identify the secrecy provision; and

(b) state whether the secrecy provision is an offence and, if so, the applicable penalty.

(2) If any information that may be disclosed by a provider under an information sharing agreement is confidential or commercially sensitive information, the agreement must —

(a) describe any contractual or equitable obligations of the provider in relation to how the information is dealt with; and

(b) require a recipient to which the information is disclosed to ensure that the information is dealt with in accordance with those obligations.

(3) If the relevant activity specified in an information sharing agreement involves the generation of derived information, the agreement must provide for —

(a) the ownership of any intellectual property in the derived information; and

(b) how the derived information is otherwise to be dealt with; and

(c) how the derived information will be treated —

(i) when the agreement ceases to be in force; or

(ii) if a party withdraws from the agreement.

172. Information sharing agreement may provide for limited further disclosure

An information sharing agreement —

(a) may provide for a recipient to be permitted to further disclose information it collects under the agreement to another person who is not a party to the agreement —

(i) in specified circumstances in connection with the relevant activity under the agreement; and

(ii) with the approval of the responsible Minister for any secrecy provision that would, but for section 187, be contravened by the further disclosure;

but

(b) must not otherwise permit the further disclosure of information disclosed under the agreement to persons who are not parties to the agreement.

173. Other matters that may be dealt with in information sharing agreement

An information sharing agreement may also provide for any of the following —

(a) the review of the agreement at intervals;

(b) how contraventions of the agreement must be dealt with;

(c) the termination of the agreement in specified circumstances (including, without limitation, if a party to the agreement commits an offence under section 189 or contravenes regulations made under section 190);

(d) subject to this Subdivision, any other matters the parties to the agreement consider it appropriate to deal with.

174. Activities under information sharing agreement may include data analytics work, data integration and data linkage

Without limiting section 168(1)(c), an information sharing agreement may provide for the use of information disclosed under the agreement for a relevant activity involving data analytics work, data integration or data linkage.

Subdivision 2 — Assessments to be conducted before entering into information sharing agreement

175. Assessment of responsible sharing principles

(1) The responsible sharing principles are set out in Schedule 2.

(2) Before entering into an information sharing agreement, each proposed provider must —

(a) conduct, and prepare a written report on, an assessment applying each of the responsible sharing principles to the proposed agreement; and

(b) be satisfied that the proposed handling of information in accordance with the agreement is consistent with the responsible sharing principles and appropriate in all the circumstances.

(3) The agreement must include provisions (***responsible sharing safeguards***) for the purposes of ensuring that the handling of information under the agreement is consistent with the responsible sharing principles.

(4) Without limiting subsection (3), responsible sharing safeguards may include provisions —

(a) regulating the manner in which the information may or must be handled; and

(b) setting out how identified risks will be managed; and

(c) setting out the action that must be taken if any of the responsible sharing safeguards is contravened.

(5) If there is more than 1 proposed recipient, an assessment conducted under subsection (2)(a) must apply the responsible sharing principles in relation to each proposed recipient.

(6) In conducting and preparing the report on the assessment, a proposed provider must have regard to any Chief Data Officer guidelines about assessments applying the responsible sharing principles.

176. Privacy impact assessment

(1) This section applies to a proposed information sharing agreement if —

(a) the relevant activity under the agreement —

(i) is likely to have a significant impact on the privacy of individuals; or

(ii) involves data integration or data linkage;

or

(b) any of the proposed recipients is an external entity.

(2) Before entering into the information sharing agreement, the proposed parties must —

(a) conduct an assessment (a ***privacy impact assessment***) of the proposed information sharing agreement; and

(b) prepare a written report on the assessment in accordance with subsection (3).

(3) The report on the privacy impact assessment must —

(a) set out an assessment of the likelihood that the relevant activity will result in an interference with the privacy of any individual; and

(b) identify the impact that the relevant activity might have on the privacy of individuals; and

(c) set out recommendations for managing, minimising or eliminating that impact; and

(d) include any other information the proposed parties consider is relevant.

(4) In complying with the requirements of this section, the proposed parties must have regard to —

(a) any privacy guidelines referred to in section 81; and

(b) any other privacy guidelines relating to privacy impact assessments.

(5) If an information sharing agreement is entered into, the parties to the agreement must ensure that a privacy impact assessment report prepared under this section in relation to the agreement is made publicly available.

(6) Despite subsection (5), a privacy impact assessment report is not required to be made publicly available —

(a) if the Chief Data Officer considers that making the report publicly available would be likely to prejudice any law enforcement function of a law enforcement agency; or

(b) in circumstances prescribed by the regulations.

177. Aboriginal information assessment

(1) Before entering into an information sharing agreement, the proposed parties must conduct, and prepare a written report on, an assessment (an ***Aboriginal information assessment***) in order to determine if either or both of the following apply —

(a) any of the information to be disclosed under the agreement is sensitive Aboriginal family history information or sensitive Aboriginal traditional information;

(b) the relevant activity under the agreement will primarily or especially affect Aboriginal people.

(2) If the assessment determines that any of the information to be disclosed under the agreement is sensitive Aboriginal family

history information or sensitive Aboriginal traditional information, the proposed provider that is to disclose the relevant information must —

(a) before entering into the information sharing agreement, take all reasonable steps to —

(i) identify and consult with relevant Aboriginal stakeholders in relation to that information; and

(ii) obtain consent from relevant Aboriginal stakeholders for the handling of that information under the agreement;

and

(b) take all reasonable steps to ensure that the agreement includes provisions (***sensitive Aboriginal information safeguards***), developed in consultation with relevant Aboriginal stakeholders, regulating the handling of that information.

(3) If the assessment determines that the relevant activity under the agreement will primarily or especially affect Aboriginal people, the proposed parties must take all reasonable steps to —

(a) identify and consult with relevant Aboriginal stakeholders in relation to the activity before entering into the information sharing agreement; and

(b) ensure that the agreement includes an Aboriginal information use plan developed in consultation with relevant Aboriginal stakeholders.

(4) An ***Aboriginal information use plan*** is a plan that —

(a) provides for opportunities for relevant Aboriginal stakeholders to participate in and engage with the relevant activity, including decision-making in connection with the relevant activity; and

(b) meets the requirements of subsection (5).

(5) An Aboriginal information use plan must —

(a) identify the Aboriginal stakeholders in consultation with whom the plan was developed; and

(b) describe the processes already undertaken to engage with those stakeholders; and

(c) describe the level of initial support from those stakeholders for the handling of the information for the relevant activity; and

(d) outline any benefits to Aboriginal people that are likely to result from the relevant activity; and

(e) set out processes for ongoing engagement with relevant Aboriginal stakeholders.

(6) In complying with the requirements of this section, the proposed parties must have regard to any Chief Data Officer guidelines in relation to the following —

(a) the identification of sensitive Aboriginal family history information or sensitive Aboriginal traditional information;

(b) the conduct of Aboriginal information assessments;

(c) the identification of relevant Aboriginal stakeholders;

(d) the development of sensitive Aboriginal information safeguards or Aboriginal information use plans;

(e) any other matters relevant to this section.

Subdivision 3 — Other provisions about information sharing agreements

178. Duration of information sharing agreement

(1) An information sharing agreement comes into force when notice of the agreement is given to the Chief Data Officer under section 182(1).

(2) An information sharing agreement remains in force until either of the following occurs —

(a) the term provided for in the agreement ends;

(b) the agreement is terminated.

(3) Subsection (2) does not prevent provisions of an information sharing agreement of the following kinds from continuing or being enforced after the term of the agreement ends or the agreement is terminated —

(a) provisions of a kind referred to in section 170(e), (f) or (h)(i) or 171(3);

(b) provisions that are expressed to continue despite the agreement ceasing to be in force or to regulate any matter occurring after the agreement ceases to be in force.

179. Variation of information sharing agreement

(1) An information sharing agreement may be varied by agreement (a ***variation agreement***) between the parties.

(2) Without limiting subsection (1), an information sharing agreement may be varied to —

(a) add or remove a provider or recipient under the agreement; or

(b) make changes to the relevant activity under the agreement.

(3) Before entering into a variation agreement, the providers and recipients under the agreement must comply with the applicable requirements of Subdivision 2 in relation to the agreement as proposed to be varied.

(4) Subsection (3) does not apply if the variation agreement is for a minor variation that does not materially affect the substance of the information sharing agreement.

(5) For the purposes of subsection (3), Subdivision 2 applies, with any appropriate modifications, as if —

(a) a reference in that Subdivision to entering into an information sharing agreement were a reference to entering into the variation agreement; and

(b) any other reference in that Subdivision to the information sharing agreement were a reference to the agreement as proposed to be varied.

(6) A variation agreement comes into force when notice of the agreement is given to the Chief Data Officer under section 182(2) or at a later time provided for under the variation agreement.

180. Withdrawal from and termination of information sharing agreement

(1) A party to an information sharing agreement may at any time withdraw from the agreement.

(2) An information sharing agreement may be terminated —

(a) under terms of the agreement dealing with termination; or

(b) at any time by agreement between the providers and recipients.

(3) An information sharing agreement is terminated if 1 or more parties to the agreement withdraw from the agreement with the result that there are no providers, or no recipients, under the agreement.

181. Enforcement of information sharing agreement

(1) An information sharing agreement may be enforced as a contract.

(2) This section does not limit section 189.

182. Notification of Chief Data Officer

(1) A provider under an information sharing agreement must ensure that written notice of the agreement, and a copy of the agreement, are given to the Chief Data Officer within 30 days after the day on which the agreement is entered into.

(2) If a variation agreement is entered into, a provider under the relevant information sharing agreement must ensure that written notice of the variation agreement, and a copy of the variation agreement, are given to the Chief Data Officer within 30 days after the day on which the variation agreement is entered into.

(3) If a party to an information sharing agreement withdraws from the agreement, a provider under the agreement must ensure that written notice of the withdrawal is given to the Chief Data Officer within 30 days after the day on which the party withdraws.

(4) If an information sharing agreement is terminated under section 180, a former provider under the agreement must ensure that written notice of the termination is given to the Chief Data Officer within 30 days after the day on which the agreement is terminated.

183. Register of information sharing agreements

(1) The Chief Data Officer must establish and maintain a register of information sharing agreements.

(2) The register must include the following information in relation to each information sharing agreement that is in force —

(a) the parties to the agreement;

(b) the general nature of the information to which the agreement relates and whether it includes personal information;

(c) the permitted purpose for which information may be handled under the agreement;

(d) the relevant activity to be carried out using the information;

(e) whether the agreement provides for further disclosure of information to a person who is not a party to the agreement under section 172;

(f) any other information prescribed by the regulations.

(3) Despite subsection (2), the register is not required to include the information referred to in subsection (2)(c) and (d) in relation to an information sharing agreement —

(a) if the Chief Data Officer considers that making that information publicly available would be likely to prejudice any law enforcement function of a law enforcement agency; or

(b) in circumstances prescribed by the regulations.

(4) The Chief Data Officer must make the register publicly available.

(5) Without limiting subsection (4), the Chief Data Officer must make the register available for public inspection during business hours.

Division 5 — Authorisations to share information and related matters

184. Authorisation to disclose information under information sharing agreement

A public entity (the ***disclosing entity***) is authorised to disclose government information it holds to another public entity, or an external entity, if —

(a) an information sharing agreement is in force in relation to the information under which —

(i) the disclosing entity is a provider; and

(ii) the entity to which the information is disclosed is a recipient;

and

(b) the information is disclosed —

(i) for the permitted purpose described in the agreement; and

(ii) for the purposes of the relevant activity described in the agreement; and

(iii) in accordance with the provisions of the agreement; and

(iv) in accordance with any applicable requirements of regulations made under section 190.

185. Authorisation to collect, hold, manage and use information under information sharing agreement

A public entity or an external entity (the ***receiving entity***) is authorised to collect, hold, manage and use information disclosed to it by a public entity if —

(a) an information sharing agreement is in force in relation to the information under which —

(i) the receiving entity is a recipient; and

(ii) the entity disclosing the information is a provider;

and

(b) the information is collected, held, managed and used —

(i) for the permitted purpose described in the agreement; and

(ii) for the purposes of the relevant activity described in the agreement; and

(iii) in accordance with the provisions of the agreement; and

(iv) in accordance with any applicable requirements of regulations made under section 190.

186. Authorisation to further disclose information disclosed under information sharing agreement in certain circumstances

A public entity, or external entity, to which information is disclosed under an information sharing agreement is authorised to further disclose that information to a person who is not a recipient under the agreement if —

(a) the further disclosure of the information to the other person is —

(i) expressly permitted by the agreement; and

(ii) carried out in accordance with the provisions of the agreement;

and

(b) for a further disclosure to which a secrecy provision applies — the further disclosure has been approved by the responsible Minister for the secrecy provision; and

(c) the entity complies with any applicable requirements of regulations made under section 190 in relation to the further disclosure.

187. Authorisations override secrecy provisions

(1) If the handling of information is authorised under this Division —

(a) the information may be handled despite any secrecy provision that applies to the information; and

(b) the handling of the information does not contravene any secrecy provision that applies to the information.

(2) Subsection (1) applies to a secrecy provision, whether the provision is enacted before, on or after the day on which this section comes into operation.

(3) However, subsection (1) does not apply to —

(a) a secrecy provision that is expressly stated to have effect despite this section; or

(b) any other secrecy provision prescribed by the regulations.

188. Protection from liability for authorised information sharing

(1) If a person handles information believing in good faith that the handling of the information is authorised under this Division —

(a) no civil or criminal liability is incurred in respect of the handling of the information; and

(b) the handling of the information is not to be regarded as a breach of any duty of confidentiality or secrecy imposed by law; and

(c) the handling of the information is not to be regarded as a breach of professional ethics or standards or as unprofessional conduct.

(2) Subsection (1) does not apply in relation to any civil or criminal liability, any breach of a duty of confidentiality or secrecy, or any breach of professional ethics or standards or unprofessional conduct, that arises under or in connection with a secrecy provision to which section 187(1) does not apply because of section 187(3).

189. Offences for unauthorised further disclosure or use of information

(1) A person commits an offence if the person, without reasonable excuse, discloses or uses information obtained under an information sharing agreement otherwise than —

(a) as authorised under this Division; or

(b) in connection with the performance of functions under this Part.

Penalty for this subsection: imprisonment for 12 months and a fine of $12 000.

(2) A person commits a crime if —

(a) the person, without reasonable excuse, discloses or uses information obtained under an information sharing agreement otherwise than —

(i) as authorised under this Division; or

(ii) in connection with the performance of functions under this Part;

and

(b) the person knows, or ought reasonably to know, that the information may be used by another person to —

(i) endanger the life, health, safety or welfare of any individual; or

(ii) commit, or assist in the commission of, an indictable offence; or

(iii) impede or interfere with the administration of justice.

Alternative offence for this subsection: subsection (1).

Penalty for this subsection: imprisonment for 3 years.

190. Regulations may prescribe safeguards

The regulations may make provision for requirements that must be complied with in relation to any of the following —

(a) the disclosure of information by a provider under an information sharing agreement;

(b) the collection, holding, management or use of information disclosed to a recipient under an information sharing agreement;

(c) the further disclosure of information disclosed to a recipient under an information sharing agreement as permitted by the agreement.

[Division 6 (s. 191-195) has not come into operation.]

Division 7 — Information holdings requests

196. Information holdings request

(1) The Chief Data Officer may, by written notice, request a public entity (other than a special information sharing entity) to disclose to the Chief Data Officer specified information about the government information held by the public entity.

(2) A request under subsection (1) is an ***information holdings request***.

(3) Without limiting subsection (1), the information that may be requested includes the following —

(a) the kinds of data sets held by the public entity;

(b) the number of data sets held by the public entity;

(c) the kinds of information contained in the data sets held by the public entity;

(d) the accuracy, currency and completeness of the data sets held by the public entity.

(4) An information holdings request must be given to the principal officer of the public entity and must specify —

(a) the information requested; and

(b) the reasons for the request.

197. Response to information holdings request

(1) If an information holdings request is made under section 196, the public entity given the request must give the Chief Data Officer a written notice responding to the request in accordance with subsection (2) within —

(a) 45 days after the day on which the request is made; or

(b) a longer period agreed with the Chief Data Officer.

(2) The response to an information holdings request must either —

(a) disclose the requested information about the government information held by the public entity to the Chief Data Officer; or

(b) state —

(i) that the public entity refuses to disclose the requested information about the government information held by the public entity; and

(ii) the reasons for the refusal.

(3) A public entity to which an information holdings request is made may refuse to provide the requested information about the government information held by the public entity if, for any reason, the public entity considers that the requested information should not be disclosed to the Chief Data Officer (including, without limitation, for a reason referred to in section 162(2)).

(4) If a public entity discloses information to the Chief Data Officer in accordance with an information holdings request —

(a) no civil or criminal liability is incurred in respect of the disclosure; and

(b) the disclosure is not to be regarded as a breach of any duty of confidentiality or secrecy imposed by law; and

(c) the disclosure is not to be regarded as a breach of professional ethics or standards or as unprofessional conduct.

Division 8 — Administration

Subdivision 1 — Chief Data Officer

198. Chief Data Officer

A Chief Data Officer must be appointed under the *Public Sector Management Act 1994* Part 3 as a senior executive officer in the information sharing Department.

199. Chief Data Officer is separate public entity for information sharing purposes

(1) For the purposes of a reference to a public entity in this Part —

(a) the Chief Data Officer is to be treated as a separate public entity and not as part of the information sharing Department; and

(b) the Chief Data Officer is to be treated as the principal officer of that public entity.

(2) Without limiting subsection (1), the Chief Data Officer may, on the Chief Data Officer's own initiative, make information sharing requests and enter into information sharing agreements as a public entity under this Part.

(3) Subsection (1) does not affect —

(a) the power under section 207 for the Chief Data Officer to delegate to an officer of the information sharing Department; or

(b) the requirement under section 211 for matters relating to the Chief Data Officer to be included in the annual report in respect of the information sharing Department referred to in that section.

200. Functions of Chief Data Officer

(1) The Chief Data Officer has the following functions —

(a) on request by a public entity or Minister or on the Chief Data Officer's own initiative, to undertake data analytics work, data integration and data linkage on information disclosed to the Chief Data Officer under this Part;

(b) to disclose or make publicly available information generated from undertaking data analytics work, data integration or data linkage if the Chief Data Officer considers it appropriate to do so;

(c) to do anything the Chief Data Officer may do as a public entity under this Part (including as referred to in section 199(2));

(d) to promote the objects of this Act;

(e) to build the capability of public entities to share information in accordance with this Part;

(f) to prepare and make available information and material in relation to the sharing of information in accordance with this Part;

(g) to provide assistance to public entities and external entities in relation to the sharing of information in accordance with this Part;

(h) to provide advice to the Information Sharing Minister or to any other person or body about any matters relating to the sharing of information held by public entities;

(i) to oversee and monitor the use of information sharing agreements;

(j) to promote and support the responsible sharing of information between public entities in the State and agencies and instrumentalities in other jurisdictions;

(k) any other functions given to the Chief Data Officer under this Act or another written law.

(2) The Chief Data Officer has all the powers that are needed for the performance of the Chief Data Officer's functions.

201. Power to issue guidelines

(1) The Chief Data Officer may issue guidelines —

(a) in relation to any matter required or permitted by this Part to be the subject of Chief Data Officer guidelines; or

(b) to provide information and guidance in relation to matters relating to this Part and the responsible sharing principles.

(2) Without limiting subsection (1)(b), guidelines may be issued in relation to any of the following —

(a) the form and contents of information sharing agreements, including template provisions for inclusion in information sharing agreements;

(b) processes to be followed before entering into information sharing agreements;

(c) processes and safeguards relating to the handling of information shared under this Part, including for the purposes of protecting —

(i) the privacy of individuals; and

(ii) the confidentiality and security of information;

(d) the management of risks relating to the sharing of information under this Part;

(e) the use of information shared under this Part for activities involving data analytics work, data integration or data linkage, including in relation to the design and governance of those activities.

(3) The Chief Data Officer may amend or revoke Chief Data Officer guidelines.

(4) The Chief Data Officer must ensure that Chief Data Officer guidelines are made publicly available.

Note for this section:

Section 221 makes provision for the status and effect of Chief Data Officer guidelines.

202. Consultation on guidelines

(1) The Chief Data Officer may consult with any person or body the Chief Data Officer considers appropriate before issuing, amending or revoking any guidelines under section 201.

(2) The Chief Data Officer must consult with the Information Commissioner before issuing, amending or revoking under section 201 any guidelines that relate to the handling of personal information or the privacy of individuals.

(3) The Chief Data Officer must consult with the Privacy and Responsible Information Sharing Advisory Committee before issuing, amending or revoking under section 201 any guidelines for the purpose of section 177(6).

203. Chief Data Officer must have regard to objects of Act

In performing functions under this Act, the Chief Data Officer must have regard to the objects of this Act.

Subdivision 2 — Privacy and Responsible Information Sharing Advisory Committee

204. Privacy and Responsible Information Sharing Advisory Committee

(1) A committee called the Privacy and Responsible Information Sharing Advisory Committee is established.

(2) The committee consists of the following members —

(a) the Chief Data Officer;

(b) the Information Commissioner;

(c) at least 2, and no more than 5, other members appointed by the Information Sharing Minister.

(3) The Information Sharing Minister must ensure that each person appointed under subsection (2)(c) has appropriate qualifications, skills or experience relevant to the functions of the committee.

(4) Before appointing a person under subsection (2)(c), the Information Sharing Minister must consult with the Privacy Minister.

(5) A person may be appointed under subsection (2)(c) —

(a) for a period not exceeding 3 years; and

(b) on a full-time basis or part-time basis.

(6) A person who has been appointed under subsection (2)(c) is eligible for reappointment.

205. Functions of Privacy and Responsible Information Sharing Advisory Committee

(1) The Privacy and Responsible Information Sharing Advisory Committee has the function of advising the Chief Data Officer in relation to the performance of the Chief Data Officer's functions.

(2) Without limiting subsection (1), the Privacy and Responsible Information Sharing Advisory Committee may give the Chief Data Officer advice in relation to the following —

(a) balancing the public interest in the protection of privacy with the public interest in the free flow of information;

(b) community expectations in relation to the matters referred to in section 177(6)(a) to (e);

(c) technical best practices in relation to the handling of information;

(d) developments in industry or other jurisdictions relevant to the handling of information.

(3) The Privacy and Responsible Information Sharing Advisory Committee may consult with any person or body for the purposes of providing advice to the Chief Data Officer.

206. Regulations about Privacy and Responsible Information Sharing Advisory Committee

(1) The regulations may make provision for or in relation to the Privacy and Responsible Information Sharing Advisory Committee.

(2) Without limiting subsection (1), regulations made under that subsection may make provision for or in relation to any of the following —

(a) the appointment of a chairperson and deputy chairperson of the committee;

(b) the conditions of appointment of members of the committee appointed under section 204(2)(c), including remuneration, allowances and leave;

(c) the resignation or removal of members of the committee appointed under section 204(2)(c);

(d) meetings and procedures of the committee, including the management of any conflicts of interest relating to the committee.

(3) Subject to any regulations made under subsection (1), the committee may determine its own procedures.

Subdivision 3 — Delegation and secrecy

207. Delegation by Chief Data Officer

(1) The Chief Data Officer may delegate to a person employed or engaged in the information sharing Department any power or duty of the Chief Data Officer under another provision of this Act.

(2) The delegation must be in writing signed by the Chief Data Officer.

(3) A person to whom a power or duty is delegated under this section cannot delegate that power or duty.

(4) A person exercising or performing a power or duty that has been delegated to the person under this section is taken to do so in accordance with the terms of the delegation unless the contrary is shown.

(5) Nothing in this section limits the ability of the Chief Data Officer to perform a function through an officer or agent.

208. Secrecy and authorised disclosure and use of information

(1) In this section —

relevant official means a person who is or has been —

(a) the Chief Data Officer; or

(b) a member of the Privacy and Responsible Information Sharing Advisory Committee; or

(c) a person employed or engaged in the information sharing Department.

(2) A relevant official must not, directly or indirectly, record, disclose or use information obtained in the administration of this Act.

Penalty for this subsection: a fine of $6 000.

(3) Subsection (2) does not apply to the recording, disclosure or use of statistical or other information that is not personal information.

(4) A relevant official does not commit an offence under subsection (2) if the recording, disclosure or use of the information is authorised under subsection (5).

(5) The recording, disclosure or use of information to which subsection (2) applies is authorised if the information is recorded, disclosed or used —

(a) for the purpose of, or in connection with, performing a function under this Act; or

(b) as permitted or required by this Act or another written law; or

(c) for the purposes of legal proceedings arising out of the administration of this Act or another written law; or

(d) with the written consent of the person to whom the information relates; or

(e) in circumstances prescribed by the regulations.

Subdivision 4 — Making documents publicly available

209. Making documents publicly available

(1) The regulations may make provision for how documents are to be made publicly available by the Chief Data Officer or an entity for the purposes of any provision of this Part.

(2) If a provision of this Part requires or permits the Chief Data Officer to make a document publicly available, the Chief Data Officer must comply with that requirement or exercise that power —

(a) if regulations under subsection (1) apply — in accordance with those regulations; or

(b) otherwise — by making the document publicly available in the manner the Chief Data Officer considers appropriate.

Division 9 — General

210. Information sharing officers of public entities

(1) The principal officer of a public entity must ensure that the principal officer, or another senior officer, of the entity is designated as the information sharing officer for the public entity.

(2) An information sharing officer of a public entity is responsible for the following —

(a) promoting the public entity's compliance with this Part;

(b) assisting in relation to —

(i) information sharing requests made by or to the public entity; and

(ii) information sharing agreements entered into or proposed to be entered into by the public entity;

(c) assisting in the conduct by the public entity of the following assessments —

(i) assessments of the responsible sharing principles under section 175;

(ii) privacy impact assessments under section 176;

(iii) Aboriginal information assessments under section 177;

(d) coordinating the public entity's dealings with the Chief Data Officer in relation to —

(i) notifications relating to information sharing agreements under section 182; and

(ii) information holdings requests made to the public entity.

(3) The principal officer of a public entity must ensure that the Chief Data Officer is notified of —

(a) the name and contact details of the information sharing officer; and

(b) any change to the individual designated as information sharing officer or to the information sharing officer's contact details.

211. Matters to be included in annual report

Without limiting the *Financial Management Act 2006* section 61(1), the annual report for a financial year required

under Part 5 of that Act in respect of the information sharing Department must include the following information for the financial year —

(a) the number of information sharing agreements entered into;

(b) the number of information sharing agreements in force as at 30 June;

(c) a list of the information sharing agreements in force as at 30 June, setting out in relation to each agreement the information referred to in section 183(2)(a) to (d) that is required to be included in the register of information sharing agreements;

(d) the number of information sharing requests made, and information sharing agreements entered into, by the Chief Data Officer;

(e) the number of shared information breaches notified to the Chief Data Officer under section 193 and how many of those breaches involved personal information;

(f) the number of information holdings requests made by the Chief Data Officer and the response to those requests;

(g) the number of information sharing directions given under section 163;

(h) a description of the data analytics work, data integration and data linkage undertaken by the Chief Data Officer;

(i) an assessment of the effectiveness of this Part and the responsible sharing principles in facilitating information sharing;

(j) an assessment of the issues and challenges that have arisen in relation to the operation of this Part and the responsible sharing principles.

212. Interaction with other laws

This Part does not limit the operation of any other written law that authorises the disclosure, collection, holding, management or use of information.

213. Application of *Freedom of Information Act 1992* to shared information

(1) In this section —

agency, ***document*** and ***exempt agency*** have the meanings given in the *Freedom of Information Act 1992* Glossary clause 1.

(2) Despite any provision of the *Freedom of Information Act 1992*, a person does not have a right under that Act to access a document of an agency if the document was —

(a) obtained by the agency under an information sharing agreement; or

(b) otherwise obtained by the Chief Data Officer in the performance of a function under this Act.

(3) Subsection (2) does not affect any right of the person under the *Freedom of Information Act 1992* to be given access to the document by the agency that disclosed the document under the information sharing agreement.

(4) If an agency to which an access application is made under the *Freedom of Information Act 1992* Part 2 holds the requested documents, but the documents were obtained from another agency (other than an exempt agency) under an information sharing agreement, the agency must transfer the access application to that other agency under section 15(2) of that Act.

214. Review of information sharing provisions of Act

(1) In this section —

information sharing provisions means the following —

(a) this Part;

(b) Schedule 2;

(c) the provisions of Parts 1, 4 and 5, to the extent that those provisions are relevant to this Part and Schedule 2;

(d) regulations made for the purposes of provisions referred to in paragraphs (a) to (c).

(2) The Information Sharing Minister must review the operation and effectiveness of the information sharing provisions, and prepare a report based on the review —

(a) as soon as practicable after the 3rd anniversary of the day on which section 160 comes into operation; and

(b) after that, at intervals of not more than 5 years.

(3) The Information Sharing Minister must cause the report to be laid before each House of Parliament as soon as practicable after it is prepared, but not later than 12 months after the 3rd anniversary or the expiry of the period of 5 years, as the case may be.

Part 4 — Miscellaneous

215. False or misleading information

A person commits an offence if the person gives to the Information Commissioner or Chief Data Officer a document or information that the person knows to be false or misleading in a material particular.

Penalty: a fine of $6 000.

216. Acts and practices of public entities and other IPP entities

(1) The following actions by a public entity or other IPP entity must be taken for the entity by the principal officer or by an officer authorised by the principal officer for that purpose (either generally or in a particular case) —

(a) making any application or submission, or giving any notice or other document, to the Information Commissioner under this Act;

(b) giving any notice or other document to the Chief Data Officer under this Act (subject to subsection (2));

(c) conducting, or preparing a report on, any assessment required under this Act.

(2) The following actions by a public entity must be taken for the entity by the principal officer or by a senior officer authorised by the principal officer for that purpose (either generally or in a particular case) —

(a) making an information sharing request;

(b) responding to an information sharing request;

(c) entering into an information sharing agreement;

(d) responding to an information holdings request.

(3) Subject to subsections (1) and (2), any act done or practice engaged in by an officer of a public entity or other IPP entity, acting in their capacity as officer and within the scope of their

actual or apparent authority, is taken for the purposes of this Act to have been done or engaged in by the entity.

217. States of mind of public entities and other IPP entities

(1) In this section —

state of mind includes —

(a) knowledge, intention, opinion, belief, suspicion or purpose; and

(b) reasons for an intention, opinion, belief, suspicion or purpose.

(2) If this Act refers to a state of mind of a public entity or other IPP entity, the entity is considered to have that state of mind if an officer of the entity, acting in their capacity as officer and within the scope of their actual or apparent authority, has that state of mind.

218. Protection from personal liability

(1) In this section —

relevant official means a person who is or has been —

(a) the Privacy Minister; or

(b) the Information Sharing Minister; or

(c) the Chief Data Officer; or

(d) a member of the Privacy and Responsible Information Sharing Advisory Committee; or

(e) a person employed or engaged in the information sharing Department.

(2) No civil liability is incurred by a relevant official for anything that the relevant official has done, in good faith, in the performance or purported performance of a function under this Act.

(3) The protection given by this section applies even though the thing done as described in subsection (2) may have been capable of being done whether or not this Act had been enacted.

(4) Despite subsection (2), the State is not relieved of any liability that it might have for a relevant official having done anything as described in that subsection.

(5) Subsection (2) does not affect the operation of section 181.

(6) In this section, a reference to the doing of anything includes a reference to an omission to do anything.

219. Giving documents

(1) The regulations may make provision for or in relation to the following —

(a) the giving of a document required or permitted to be given under this Act (including the giving of the document by electronic means);

(b) the time at which the document is taken to have been given;

(c) the means of satisfying a requirement under this Act in relation to a document in writing (for example, a requirement that the original of a document be given or that a document be signed) if the document is given by electronic means.

(2) This section applies to a requirement or permission to give a document whether the term "give", "issue", "send" or "serve", or any other similar term, is used.

220. Laying documents before House of Parliament not sitting

(1) This section applies if —

(a) a provision of this Act requires a Minister (the ***relevant Minister***) to cause a document to be laid before each

House of Parliament, or dealt with under this section, within a specified period; and

(b) at the beginning of the period, a House of Parliament is not sitting; and

(c) in the relevant Minister's opinion, the House will not sit before the end of the period.

(2) The relevant Minister must send the document to the Clerk of the House before the end of the period.

(3) When the document is sent to the Clerk of the House it is taken to have been laid before the House.

(4) The laying of the document that is taken to have occurred under subsection (3) must be recorded in the Minutes, or Votes and Proceedings, of the House on the first sitting day of the House after the Clerk receives the document.

221. General provisions about guidelines

(1) Privacy guidelines and Chief Data Officer guidelines are not subsidiary legislation for the purposes of the *Interpretation Act 1984*.

(2) If there is a conflict or inconsistency between a provision of this Act and a provision of privacy guidelines or Chief Data Officer guidelines, the provision of this Act prevails.

(3) A requirement under this Act to have regard to privacy guidelines or Chief Data Officer guidelines does not —

(a) derogate from a duty to exercise discretion in a particular case; or

(b) prevent a person from having regard to matters not set out in the guidelines; or

(c) require the entity to have regard to guidelines that are inconsistent with a provision of this Act.

222. Regulations

(1) The Governor may make regulations prescribing matters —

(a) required or permitted by this Act to be prescribed; or

(b) necessary or convenient for giving effect to the purposes of this Act.

(2) Without limiting any other provision of this Act, regulations may make provision for or in relation to the following —

(a) applications under this Act;

(b) forms for the purposes of this Act;

(c) fees or charges in relation to any matter under this Act.

(3) Regulations for the purposes of section 6(1)(h) or (4) or 9(2)(f)(i) can only be made on the recommendation of the Privacy Minister and the Information Sharing Minister.

Part 5 — Transitional provisions

223. Application of information privacy principles

(1) In this section —

commencement day means the day on which section 20 comes into operation.

(2) The following information privacy principles apply only in relation to personal information collected on or after commencement day —

(a) IPP 1;

(b) IPP 7;

(c) IPP 8;

(d) IPP 10.

(3) The following information privacy principles apply in relation to personal information whether collected before, on or after commencement day —

(a) IPP 2;

(b) IPP 3;

(c) IPP 4;

(d) IPP 5;

(e) IPP 6;

(f) IPP 9.1.

(4) The following information privacy principles apply to de-identified information whether collected before, on or after commencement day —

(a) IPP 9.2;

(b) IPP 11.

224. Application of approved privacy codes of practice

(1) In this section —

commencement day means the day on which section 33 comes into operation.

(2) To the extent that an approved privacy code of practice modifies the application of an IPP referred to in section 223(2), or provides for how an IPP referred to in section 223(2) is to be applied or complied with, the approved privacy code of practice applies only in relation to personal information collected on or after commencement day.

(3) Any other provision of an approved privacy code of practice applies in relation to personal information or de-identified information whether collected before, on or after commencement day.

(4) Subsections (2) and (3) apply subject to any provision of the approved privacy code of practice that provides for the approved privacy code of practice, or any provision of it, to apply only in relation to information collected on or after a day that is later than commencement day.

225. Notifiable information breach may involve personal information collected before commencement day

(1) In this section —

commencement day means the day on which section 61 comes into operation.

(2) For the purposes of section 57, a notifiable information breach may occur in relation to personal information held by an IPP entity whether the personal information was collected before, on or after commencement day.

226. Public register obligations apply to personal information collected before commencement day

(1) In this section —

commencement day means the day on which section 76 comes into operation.

(2) Part 2 Division 7 applies to personal information contained, or proposed to be contained, in a public register whether the personal information was collected before, on or after commencement day.

227. Privacy impact assessments not required for functions or activities performed before commencement day

(1) In this section —

commencement day means the day on which section 79 comes into operation.

(2) The requirement under section 79(2) for an IPP entity to conduct a privacy impact assessment before first performing a high privacy impact function or activity does not apply in relation to a function or activity that the IPP entity started to perform before commencement day.

(3) Subsection (2) does not limit —

(a) any requirement under section 79(2) for an IPP entity to conduct a privacy impact assessment before making a significant change to the way in which personal information is handled as part of a high privacy impact function or activity that the IPP entity started to perform before commencement day; or

(b) any requirement under section 79(2) for an IPP entity to conduct a privacy impact assessment in relation to an activity that the IPP entity first performs on or after commencement day, even if the activity is performed in connection with a function that the IPP entity started to perform before commencement day; or

(c) the Information Commissioner's power to issue a direction under section 80 in relation to a function or activity that an IPP entity started to perform before commencement day.

228. State services contracts entered into before commencement day

(1) In this section —

commencement day means the day on which section 129 comes into operation.

(2) This Act applies in relation to a provision of a State services contract of the kind referred to in section 129 even if that provision was included in the contract before commencement day.

(3) Section 140(2) does not apply in relation to a State services contract entered into before commencement day.

229. Transitional regulations

(1) In this section —

specified means specified or described in regulations;

transitional matter —

(a) means a matter or issue of a transitional nature that arises as a result of the enactment of this Act or the coming into operation of any provisions of this Act or regulations made under it; and

(b) includes a savings or application matter.

(2) If there is not sufficient provision in this Part for dealing with a transitional matter, regulations may prescribe anything required, necessary or convenient to be prescribed in relation to the matter.

(3) Without limiting subsection (2), regulations made for the purposes of that subsection may provide that specified provisions of this Act —

(a) do not apply to, or in relation to, a specified matter or thing; or

(b) apply with specified modifications to, or in relation to, a specified matter or thing.

(4) If regulations made for the purposes of subsection (2) provide that a specified state of affairs is taken to have existed, or not to have existed, on and from a day that is earlier than the day on which the regulations are published in accordance with the *Interpretation Act 1984* section 41(1)(a) but not earlier than the day on which this section comes into operation, the regulations have effect according to their terms.

(5) If regulations made for the purposes of subsection (2) contain a provision of a kind described in subsection (4), the provision does not operate so as —

(a) to affect in a manner prejudicial to any person (other than the State or an authority of the State) the rights of that person existing before the day of publication of those regulations; or

(b) to impose liabilities on any person (other than the State or an authority of the State) in respect of anything done or omitted to be done before the day of publication of those regulations.

Part 6 — Other Acts amended

[Part 6 Division 1 will not come into operation [1].]

Division 2 — *Freedom of Information Act 1992* amended

232. Act amended

This Division amends the *Freedom of Information Act 1992*.

233. Section 23 amended

In section 23(5) delete "is an intellectually handicapped person," and insert:

has a cognitive impairment,

234. Section 32 amended

(1) Delete section 32(2)(b) and insert:

(b) if the third party is dead, the third party's nearest relative,

(2) In section 32(3):

(a) delete "party, or the closest relative of a dead third party," and insert:

party

(b) delete "subsection (2)." and insert:

subsection (2)(a).

(3) In section 32(4) delete "closest relative of a dead third party, is an intellectually handicapped person, the views of the person's closest" and insert:

nearest relative of a dead third party, has a cognitive impairment, the views of the person's nearest

235. Section 45 amended

In section 45(2) delete "closest" (each occurrence) and insert:

nearest

236. Section 67A inserted

After section 67 insert:

67A. Commissioner may deal with complaint under *Privacy and Responsible Information Sharing Act 2024*

(1) If the Information Commissioner considers that the matter about which a complaint is made could be the subject of a complaint under the *Privacy and Responsible Information Sharing Act 2024* Part 2 Division 9 —

(a) the Commissioner may decide that the complaint should be dealt with under that Act; and

(b) if the Commissioner so decides, the complaint is taken to be a privacy complaint made under section 82 of that Act.

(2) If the Information Commissioner makes a decision that a complaint should be dealt with under the *Privacy and Responsible Information Sharing Act 2024*, the Commissioner must inform the complainant and agency, in writing, of the decision.

237. Section 98 replaced

Delete section 98 and insert:

98. Application on behalf of child or person with disability

(1) An access application or application for amendment may be made to an agency on behalf of a child by the child's guardian or a person who has custody or care and control of the child.

(2) An access application or application for amendment may be made to an agency on behalf of a person who is incapable of making the application because of a disability (as defined in the *Disability Services Act 1993* section 3) by —

(a) another person chosen by the person to make the application on their behalf; or

(b) if the person is incapable of choosing another person to make the application on their behalf —

(i) a guardian (as defined in the *Guardianship and Administration Act 1990* section 3(1)) of the person; or

(ii) another person who is related to the person by blood or marriage or is a de facto partner of the person; or

(iii) another person who, in the opinion of the principal officer of the agency, has a sufficient interest in the subject matter of the application.

(3) Subsections (1) and (2) do not limit the ability of persons to make applications on behalf of other persons generally.

98A. Certain requests under *Privacy and Responsible Information Sharing Act 2024* taken to be applications for access or amendment

(1) In this section —

IPP means an information privacy principle set out in the *Privacy and Responsible Information Sharing Act 2024* Schedule 1.

(2) A reference in this section to an IPP followed by a designation is a reference to the provision with that designation in the *Privacy and Responsible Information Sharing Act 2024* Schedule 1.

(3) If a request made by an individual to an agency (other than an exempt agency) purports to be a request for access to personal information that relates to the individual under IPP 6.1, and the request complies with the requirements of the *Privacy and Responsible Information Sharing Act 2024* section 40 —

(a) the request is taken to be an access application under this Act that complies with the requirements of section 12; and

(b) the agency must deal with the request accordingly under this Act.

(4) If a request made by an individual to an agency purports to be a request for correction of personal information that relates to the individual under IPP 6.5,

and the request complies with the requirements of the *Privacy and Responsible Information Sharing Act 2024* section 41 —

(a) the request is taken to be an application for amendment under this Act that complies with the requirements of section 46; and

(b) the agency must deal with the request accordingly under this Act.

(5) If a request made by an individual to an agency purports to be an application for access to or correction of personal information under IPP 6.1 or IPP 6.5, but does not comply with the requirements of the *Privacy and Responsible Information Sharing Act 2024* section 40 or 41 (as the case requires), the agency must comply with its obligations under section 11 or 45 to help the individual to make an access application or application for amendment under this Act.

Note for this section:

Under the *Privacy and Responsible Information Sharing Act 2024* section 27, IPP 6 does not apply to an agency.

238. Glossary clause 1 amended

(1) In the Glossary clause 1 delete the definition of ***personal information***.

(2) In the Glossary clause 1 insert in alphabetical order:

nearest relative, in relation to a person, has the meaning given in the *Guardianship and Administration Act 1990* section 3(1);

personal information —

(a) means information or an opinion, whether true or not, and whether recorded in a material form or not, that relates to an individual, whether living or dead,

whose identity is apparent or can reasonably be ascertained from the information or opinion; and

(b) includes information of the following kinds to which paragraph (a) applies —

(i) a name, date of birth or address;

(ii) a unique identifier, online identifier or pseudonym;

(iii) contact information;

(iv) information that relates to an individual's location;

(v) technical or behavioural information in relation to an individual's activities, preferences or identity;

(vi) inferred information that relates to an individual, including predictions in relation to an individual's behaviour or preferences and profiles generated from aggregated information;

(vii) information that relates to 1 or more features specific to the physical, physiological, genetic, mental, behavioural, economic, cultural or social identity of an individual;

239. Various references to personal information "about" an individual amended

In the provisions listed in the Table delete "about" (each occurrence" and insert:

that relates to

Table

s. 16(1)(d)	s. 21
s. 29	s. 32(1)
s. 45(1) and (2)	s. 109(a)
s. 112(3)(b)	Sch. 1 cl. 3(1) and (2)

Note: The heading to the amended sections listed in the Table are to read as set out in the Table:

Table

Amended section	Section heading
s. 21	**Consideration of application for personal information that relates to applicant**
s. 29	**Agency's duties when giving access to personal information that relates to applicant**
s. 32	**When access may be given to personal information that relates to third party**

Division 3 — *Government Trading Enterprises Act 2023* amended

240. Act amended

This Division amends the *Government Trading Enterprises Act 2023*.

241. Section 86 amended

In section 86 delete the definition of ***personal information*** and insert:

> ***personal information*** has the meaning given in the *Privacy and Responsible Information Sharing Act 2024* section 4;

Division 4 — *Health Practitioner Regulation National Law Application Act 2024* amended

242. Act amended

This Division amends the *Health Practitioner Regulation National Law Application Act 2024*.

243. Section 22 amended

In section 22(2):

(a) delete "Acts" and insert:

enactments

(b) after paragraph (d) insert:

(da) the *Privacy and Responsible Information Sharing Act 2024* Part 2 and Schedule 1;

Division 5 — *National Health Funding Pool Act 2012* amended

244. Act amended

This Division amends the *National Health Funding Pool Act 2012*.

245. Section 25 amended

In section 25:

(a) delete "Acts" and insert:

enactments

(b) after paragraph (b) insert:

(ba) the *Privacy and Responsible Information Sharing Act 2024* Part 2 and Schedule 1;

Part 7 — Amendment to this Act linked to commencement of *Criminal Law (Mental Impairment) Act 2023*

246. Act amended

This Part amends this Act.

247. Section 4 amended

In section 4 in the definition of ***law enforcement agency*** delete paragraph (e) and insert:

(e) the Mental Impairment Review Tribunal established under the *Criminal Law (Mental Impairment) Act 2023* section 156; or

Schedule 1 — Information privacy principles

[s. 4, 5 and 19]

1. Principle 1: Collection

1.1 An IPP entity must not collect personal information (other than sensitive personal information) unless the information is necessary for 1 or more of the IPP entity's functions or activities.

1.2 An IPP entity must not collect sensitive personal information that relates to an individual unless the information is necessary for 1 or more of the IPP entity's functions or activities and —

(a) the individual consents to the collection of the information; or

(b) the collection of the information is required or authorised by or under law; or

(c) both of the following apply —

(i) the collection of the information is necessary to prevent or lessen a serious threat to the life, health, safety or welfare of any individual, or a threat to the life, health, safety or welfare of any individual due to family violence;

(ii) the individual to whom the information relates is incapable under section 154(4) of giving consent to the collection;

or

(d) the collection of the information is necessary for the establishment, exercise or defence of a legal or equitable claim; or

(e) the collection of the information is permitted under subclause 1.3.

1.3 For the purposes of subclause 1.2(e), collecting sensitive personal information is permitted if —

(a) the collection —

(i) is necessary for research, or the compilation or analysis of statistics, relevant to government-funded targeted welfare or educational services; or

(ii) is of information relating to an individual's racial or ethnic origin and is collected for the purpose of providing government-funded targeted welfare or educational services;

and

(b) there is no reasonably practicable alternative to collecting the information for that purpose; and

(c) it is impracticable for the IPP entity to seek the individual's consent to the collection.

1.4 An IPP entity must not collect personal information that relates to an individual unless the collection is fair and reasonable in the circumstances, taking into account the following matters —

(a) whether the individual would reasonably expect the information to be collected in the circumstances;

(b) the kind of personal information collected, including whether any of that information is sensitive personal information;

(c) the amount of personal information collected;

(d) whether the collection of the information is necessary for 1 or more of the IPP entity's functions or activities;

(e) whether there is a risk of loss, harm or other detriment to any individual as a result of the collection of the information;

(f) whether the collection of the information for 1 or more of the IPP entity's functions or activities is, on balance, in the public interest;

(g) in the case of personal information that relates to a child — whether the collection of the information is in the best interests of the child;

(h) the objects of this Act.

1.5 Subclause 1.4 does not apply to the collection of personal information if —

(a) the collection is required or authorised by or under law; or

(b) the IPP entity reasonably believes that the collection is necessary to prevent or lessen —

(i) a serious threat to the life, health, safety or welfare of any individual; or

(ii) a threat to the life, health, safety or welfare of any individual due to family violence;

or

(c) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

1.6 An IPP entity must not collect personal information in an unreasonably intrusive way.

1.7 Before collecting personal information, an IPP entity must make a written record of the purposes for which the information will be collected and used or disclosed.

1.8 An IPP entity must collect personal information that relates to an individual only from the individual unless —

(a) the individual consents to the collection of the information from someone other than the individual; or

(b) the collection of the information is required or authorised by or under law; or

(c) it is unreasonable or impracticable to do so.

1.9 At or before the time (or, if that is not practicable, as soon as practicable after) an IPP entity collects personal information that relates to an individual from the individual, it must take such steps (if any) as are reasonable in the circumstances to ensure that the individual is given, or made aware of, the following information —

(a) the identity of the IPP entity and how to contact it;

(b) how the individual may access the information (if applicable);

(c) the purposes for which the information is collected and will be used or disclosed;

(d) whether the IPP entity usually discloses information of that kind and, if so, the persons or bodies or kinds of persons or bodies to which the information is usually disclosed;

(e) any law that requires the particular information to be collected;

(f) the main consequences (if any) for the individual if all or part of the information is not provided.

1.10 If an IPP entity collects personal information that relates to an individual from someone other than the individual, the IPP entity must take such steps (if any) as are reasonable in the circumstances —

(a) to satisfy itself that the information was not originally collected from the individual in contravention of this clause; and

(b) to ensure that the individual is given, or made aware of, the information referred to in subclause 1.9(a) to (f), except to the extent that giving or making the individual aware of that information would pose —

(i) a serious threat to the life, health, safety or welfare of any individual; or

(ii) a threat to the life, health, safety or welfare of any individual due to family violence.

1.11 If an IPP entity collects personal information that relates to an individual from someone other than the individual in connection with a complaint made about the individual, the IPP entity is not required to comply with subclause 1.10 in relation to the collection of the information unless the IPP entity contacts the individual about the complaint.

1.12 An IPP entity must ensure that the information that an individual is given, or made aware of, under subclause 1.9 or 1.10(b) is up-to-date, clear, concise and expressed in plain language.

2. Principle 2: Use and disclosure

2.1 If an IPP entity holds personal information that relates to an individual that was collected to be used or disclosed for a particular purpose (the ***primary purpose***), the IPP entity must not use or disclose

the information for another purpose (the ***secondary purpose***) unless —

(a) the individual would reasonably expect the IPP entity to use or disclose the information for the secondary purpose and the secondary purpose is —

(i) if the information is not sensitive personal information — related to the primary purpose; or

(ii) if the information is sensitive personal information — directly related to the primary purpose;

or

(b) the individual consents to the use or disclosure; or

(c) all of the following apply —

(i) the use or disclosure is necessary for research, or the compilation or analysis of statistics, in the public interest;

(ii) the research or statistics are not to be published in a form that identifies any particular individual;

(iii) it is impracticable for the IPP entity to seek the individual's consent before the use or disclosure or, in the case of disclosure, the IPP entity reasonably believes that the recipient of the information will not further disclose the information;

or

(d) the IPP entity reasonably believes that the use or disclosure is necessary to prevent or lessen —

(i) a serious threat to the life, health, safety or welfare of any individual; or

(ii) a serious threat to public health, public safety or public welfare; or

(iii) a threat to the life, health, safety or welfare of any individual due to family violence;

or

(e) the IPP entity has reason to suspect that unlawful activity has been, is being, or may be, engaged in and uses or discloses the information as a necessary part of its investigation of the

matter or in reporting the matter to relevant persons or authorities; or

(f) the use or disclosure is required or authorised by or under law; or

(g) the IPP entity reasonably believes that the use or disclosure is necessary for —

(i) a law enforcement function to be performed by a law enforcement agency; or

(ii) proceedings before a court or tribunal.

2.2 An IPP entity must not use or disclose personal information unless the use or disclosure is fair and reasonable in the circumstances, taking into account the following matters —

(a) whether the individual would reasonably expect the information to be used or disclosed in the circumstances;

(b) the kind of personal information used or disclosed, including whether any of that information is sensitive personal information;

(c) the amount of personal information used or disclosed;

(d) whether the use or disclosure is necessary for 1 or more of the IPP entity's functions or activities;

(e) whether there is a risk of loss, harm or other detriment to any individual as a result of the use or disclosure of the information;

(f) whether the disclosure or use of the information for 1 or more of the IPP entity's functions or activities is, on balance, in the public interest;

(g) in the case of personal information that relates to a child — whether the use or disclosure of the information is in the best interests of the child;

(h) the objects of this Act.

2.3 Subclause 2.2 does not apply to the use or disclosure of personal information if —

(a) the use or disclosure is required or authorised by or under law; or

(b) the IPP entity reasonably believes that the use or disclosure is necessary to prevent or lessen —

(i) a serious threat to the life, health, safety or welfare of any individual; or

(ii) a serious threat to public health, public safety or public welfare; or

(iii) a threat to the life, health, safety or welfare of any individual due to family violence;

or

(c) the IPP entity has reason to suspect that unlawful activity has been, is being, or may be, engaged in and uses or discloses the information as a necessary part of its investigation of the matter or in reporting the matter to relevant persons or authorities; or

(d) the IPP entity reasonably believes that the use or disclosure is necessary for —

(i) a law enforcement function to be performed by a law enforcement agency; or

(ii) proceedings before a court or tribunal.

2.4 Before using or disclosing personal information for a secondary purpose, the IPP entity must make a written record of the secondary purpose.

2.5 If an IPP entity uses or discloses personal information in a manner permitted by subclause 2.1(g) or 2.3(d), the IPP entity must make a written record of the use or disclosure.

2.6 For the purposes of this clause, a disclosure of information that is covered by an express exception from a secrecy provision in a written law is taken to be authorised by law.

3. Principle 3: Information quality

An IPP entity must take such steps (if any) as are reasonable in the circumstances to ensure that personal information it collects, uses or discloses is accurate, complete and up-to-date.

4. Principle 4: Information security

4.1 An IPP entity must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

4.2 An IPP entity must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which it may be used or disclosed under this Schedule, unless the IPP entity is expressly required or authorised to retain the information by or under another law.

5. Principle 5: Openness and transparency

5.1 An IPP entity must develop a document setting out policies on its handling of personal information and must make the document available to anyone who requests it.

5.2 A document referred to in subclause 5.1 must be up-to-date, clear, concise and expressed in plain language.

5.3 On request by a person, an IPP entity must take reasonable steps to let the person know, generally —

(a) the kinds of personal information that the IPP entity collects and holds; and

(b) how the IPP entity handles personal information; and

(c) the purposes for which the IPP entity handles personal information; and

(d) whether any personal information held by the IPP entity is used for an automated decision-making process.

6. Principle 6: Access and correction

6.1 If an IPP entity holds personal information that relates to an individual, it must provide the individual with access to the information on a request made by the individual in accordance with section 40, except to the extent that —

(a) providing access would endanger the life or physical safety of any person; or

(b) there are reasonable grounds to believe that —

(i) the person requesting access is a perpetrator, or alleged perpetrator of family violence; and

(ii) denying access is necessary to prevent or lessen a threat to the life, health, safety or welfare of any individual due to family violence;

or

(c) providing access would enable the existence, non-existence or identity of any confidential source of information in relation to the enforcement or administration of the law to be discovered; or

(d) providing access would have an unreasonable impact on the privacy of other individuals; or

(e) the request for access is frivolous or vexatious; or

(f) the information relates to existing legal proceedings between the IPP entity and the individual, and the information would not be accessible by the process of discovery or subpoena in those proceedings; or

(g) providing access would reveal the intentions of the IPP entity in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

(h) providing access would be unlawful; or

(i) denying access is required or authorised by or under law; or

(j) providing access would be likely to prejudice an investigation of possible unlawful activity; or

(k) providing access would be likely to prejudice any of the law enforcement functions of a law enforcement agency; or

(l) providing access would be likely to reveal evaluative information generated within the IPP entity about a commercially sensitive decision-making process.

6.2 If the IPP entity denies access to the personal information because of subclause 6.1(l), the IPP entity may include in the reasons for the denial of access referred to in subclause 6.7 an explanation for the commercially sensitive decision.

6.3 If an IPP entity is not required to provide an individual with access to information because of any of subclause 6.1(a) to (l), the IPP entity must, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.

6.4 If a fee for making a request for access to personal information applies under regulations made for the purposes of section 40(2)(e), the IPP entity may refuse access to the personal information until the fee is paid.

6.5 If an individual makes a request to an IPP entity in accordance with section 41 for the correction of personal information that relates to the individual, and the individual establishes that the information is not accurate, complete and up-to-date, the IPP entity must take reasonable steps to correct the information so that it is accurate, complete and up-to-date.

6.6 If the individual and the IPP entity disagree about whether the information is accurate, complete and up-to-date, and the individual requests the IPP entity to associate with the information a statement claiming that the information is not accurate, complete or up-to-date, the IPP entity must take reasonable steps to do so.

6.7 An IPP entity must provide reasons for a denial of access to, or a refusal of a request for the correction of, personal information.

6.8 If an individual requests access to, or the correction of, personal information held by an IPP entity, the IPP entity must, as soon as practicable, but no later than 45 days after the day on which the request is made —

(a) provide access to the information or reasons for the denial of access; or

(b) correct the information or provide reasons for the refusal of the request for the correction of the information; or

(c) provide reasons for the delay in responding to the request.

7. Principle 7: Unique identifiers

7.1 An IPP entity must not assign unique identifiers to individuals unless the assignment of unique identifiers is necessary to enable the IPP entity to perform any of its functions or activities efficiently.

7.2 An IPP entity must not adopt as its own unique identifier of an individual a unique identifier of the individual that has been assigned by another IPP entity unless —

(a) the adoption of the unique identifier is necessary to enable the IPP entity to perform any of its functions efficiently; or

(b) the individual consents to the use of the unique identifier; or

(c) the IPP entity is an outsourcing entity under a State services contract and is adopting the unique identifier assigned by a contracted service provider in the provision of services under the contract; or

(d) the IPP entity is a contracted service provider under a State services contract and is adopting the unique identifier assigned by the relevant outsourcing entity.

7.3 An IPP entity must not use or disclose a unique identifier assigned to an individual by another IPP entity unless —

(a) the use or disclosure is necessary for the IPP entity to fulfil its obligations to the other IPP entity; or

(b) circumstances referred to in IPP 2.1(c), (e), (f) or (g) apply to the use or disclosure; or

(c) the individual consents to the use or disclosure.

7.4 An IPP entity must not require an individual to provide a unique identifier in order to obtain a service unless —

(a) the provision of the identifier is required or authorised by or under law; or

(b) the provision is in connection with the purpose for which the identifier was assigned or a directly related purpose.

8. Principle 8: Anonymity

8.1 Individuals must have the option of not identifying themselves when dealing with an IPP entity.

8.2 Subclause 8.1 does not apply to an IPP entity in relation to a matter if —

(a) the IPP entity is required or authorised by or under law to deal with individuals who have identified themselves in relation to that matter; or

(b) it is impracticable for the IPP entity to deal with individuals who have not identified themselves in relation to that matter.

9. Principle 9: Disclosures outside Australia

9.1 An IPP entity must not disclose personal information that relates to an individual to a person (other than the individual) outside Australia unless —

(a) the IPP entity reasonably believes that the person to whom the information is disclosed is subject to a law, binding administrative scheme, or contract, that requires the person to comply with principles for handling the information that are substantially similar to the information privacy principles; or

(b) the individual consents to the disclosure; or

(c) the disclosure is required or authorised by or under law; or

(d) the disclosure is necessary for the performance of a contract between the individual and the IPP entity or for the implementation of pre-contractual measures taken in response to the individual's request; or

(e) the disclosure is necessary for the conclusion or performance of a contract that is concluded in the interest of the individual between the IPP entity and a third party; or

(f) all of the following apply —

(i) the disclosure is for the benefit of the individual;

(ii) it is impracticable to obtain the consent of the individual to the disclosure;

(iii) if it were practicable to obtain that consent, the individual would be likely to give it;

or

(g) the IPP entity has taken reasonable steps to ensure that the information will not be held, used or disclosed by the

recipient inconsistently with the information privacy principles.

9.2 An IPP entity must not disclose de-identified information that relates to an individual to a person (other than the individual) outside Australia unless the IPP entity takes reasonable steps to ensure that the person to whom the de-identified information is disclosed —

(a) protects the de-identified information from misuse and loss and from unauthorised re-identification, access, modification or disclosure; and

(b) does not —

(i) re-identify the de-identified information (except in circumstances referred to in IPP 11.2(c) or (d)); or

(ii) further disclose the information in a manner that is likely to undermine the effectiveness of the de-identification of the information.

10. Principle 10: Automated decision-making

10.1 An IPP entity that employs an automated decision-making process involving the use of personal information in making significant decisions about individuals must —

(a) conduct an assessment of the impact of the automated decision-making process on those individuals, having regard to —

(i) the elimination or minimisation of harm, bias and discrimination; and

(ii) whether there is a process by which individuals about whom decisions are made can request human intervention; and

(iii) whether the handling of personal information in the process complies with any applicable requirements under this Act;

and

(b) periodically evaluate the operation and effectiveness of the automated decision-making process; and

(c) reassess the matter referred to in paragraph (a) when changes are made to the automated decision-making process.

10.2 If an IPP entity employs an automated decision-making process involving the use of personal information in making a significant decision about an individual, the IPP entity must —

(a) notify the individual that an automated decision-making process has been employed in making the decision; and

(b) on request, give the individual information about how the automated decision-making process is employed in making decisions; and

(c) provide a process by which the individual can request human intervention in relation to the decision.

10.3 A notification under subclause 10.2(a) —

(a) may be given with, or as part of, any notification of the significant decision required to be given under a written law; and

(b) subject to paragraph (a), must be given as soon as practicable.

10.4 Information provided under subclause 10.2(b) must be reasonably comprehensive and provided in a form that is capable of being understood by a person without specialist knowledge.

11. Principle 11: De-identified information

11.1 An IPP entity must take reasonable steps to protect the de-identified information it holds from misuse and loss and from unauthorised re-identification, access, modification or disclosure.

11.2 An IPP entity must not re-identify de-identified information that it holds unless —

(a) the de-identified information was de-identified by the IPP entity itself; or

(b) all of the following apply —

(i) the de-identified information was collected from another IPP entity;

(ii) that other IPP entity has given written authorisation for the IPP entity to re-identify the de-identified information for a specified purpose;

(iii) the re-identification is undertaken for the specified purpose;

or

(c) the re-identification is undertaken to test the effectiveness of de-identification processes or security measures protecting information; or

(d) the re-identification is required or authorised by or under law.

Schedule 2 — Responsible sharing principles

[s. 4 and 175]

1. Principle 1: Activities

The relevant activity to be carried out using the information to be disclosed must be appropriate, having regard to the following —

(a) whether there is a direct and identifiable connection between the relevant activity and a permitted purpose;

(b) whether it is necessary to disclose and use the information for the relevant activity in order to achieve the permitted purpose;

(c) whether the methods to be used in carrying out the relevant activity can reasonably be expected to result in the achievement of the permitted purpose;

(d) whether the relevant activity will be of benefit to the public;

(e) whether there is a risk of loss, harm or other detriment to the public if the disclosure and use of the information for the relevant activity does not occur;

(f) whether there is a risk of loss, harm or other detriment to the public as a result of the proposed disclosure and use of the information for the relevant activity (including whether there is a risk of an interference with the privacy of any individual) and, if so, whether the risk can be appropriately mitigated;

(g) whether the relevant activity will primarily or especially affect Aboriginal people;

(h) whether the proposed disclosure and use of the information for the relevant activity is, on balance, in the public interest.

2. Principle 2: Recipients

The proposed recipient of the information must be an entity to which it is appropriate to disclose the information, having regard to the following —

(a) whether the proposed recipient has the appropriate skills, experience and capability to use the information effectively in carrying out the relevant activity;

(b) whether the proposed recipient will restrict access to the information to appropriate persons (for example, persons with security clearances or other authorisations);

(c) whether the proposed recipient will require support from the proposed provider to use the information in carrying out the relevant activity and, if so, whether the proposed provider has capacity to provide that support;

(d) whether any person other than the proposed recipient has an interest in the relevant activity, or in any derived information to be generated as a result of the relevant activity, and if so, the nature of that interest;

(e) whether the systems, processes and governance arrangements of the proposed recipient are appropriate for carrying out the relevant activity using the information.

3. Principle 3: Information

3.1 The information must be information that it is appropriate to disclose and use for the relevant activity, having regard to the following —

(a) whether the information is limited to only such information as it is necessary to use to achieve the permitted purpose;

(b) whether the information is of sufficient quality for the proposed use;

(c) whether the information includes sensitive Aboriginal family history information or sensitive Aboriginal traditional information;

(d) whether circumstances affecting the appropriateness of disclosing or using the information are likely to change during the period in which the information is to be disclosed and used;

(e) if the information is or includes de-identified information —

(i) whether there is a risk that the de-identified information could be re-identified; and

(ii) if so, how that re-identification could occur.

3.2 The information to be disclosed and used for the relevant activity must not include personal information that relates to an individual unless —

(a) the individual consents to the disclosure of the personal information for the proposed use; or

(b) the individual would reasonably expect the personal information to be disclosed for the proposed use and the proposed use relates to the purpose for which the information was collected; or

(c) the personal information is to be used for the permitted purpose of informing or enabling emergency management (including prevention of, preparedness for, response to, and recovery from, emergencies); or

(d) the relevant activity consists only of data linkage, data integration or both; or

(e) all of the following apply —

(i) it is impracticable to seek the individual's consent to the disclosure of the personal information for the proposed use;

(ii) the permitted purpose cannot be achieved by the use of de-identified information;

(iii) the proposed disclosure and use of the personal information for the relevant activity is, on balance, in the public interest.

4. Principle 4: Settings

The environments in which, and manner in which, the information proposed to be disclosed will be collected, held, managed and used must be appropriate, having regard to the following —

(a) the physical locations where the information will be held, managed and used;

(b) the digital environments in which the information will be held, managed and used;

(c) the methods that will be used to transport or transmit the information;

(d) the period for which the information is proposed to be held by the proposed recipient;

(e) whether the proposed recipient has appropriate security systems and processes to protect the information from unauthorised access, use or disclosure;

(f) the likelihood that an information breach could occur in relation to the information and whether the proposed recipient's systems and processes are adequate to respond to an information breach;

(g) how the information will be dealt with after it has been used in carrying out the relevant activity.

5. Principle 5: Outputs

If the relevant activity to be carried out using the information to be disclosed will or may involve the disclosure of any derived information, that proposed disclosure must be appropriate, having regard to the following —

(a) the nature of the proposed disclosure;

(b) the persons to whom the proposed disclosure is to be made;

(c) the likelihood that the identity of any individual to whom the information relates could be ascertained as a result of the proposed disclosure;

(d) whether there will be an external audit or review prior to the disclosure and, if so, whether the proposed provider would be involved in that audit or review.

Notes

This is a compilation of the *Privacy and Responsible Information Sharing Act 2024* and includes amendments made by other written laws. For provisions that have come into operation see the compilation table. For provisions that have not yet come into operation see the uncommenced provisions table.

Compilation table

Short title	Number and year	Assent	Commencement
Privacy and Responsible Information Sharing Act 2024 Pt. 1, Pt. 2 (other than Div. 6, Div. 10 Subdiv. 4 and s. 134-136), Pt. 3 (other than Div. 6), Pt. 4, 5 and 6 (other than Div. 1 [1]) and 7 and Sch. 1 and 2	51 of 2024	6 Dec 2024	Pt. 1 and 7: 6 Dec 2024 (see s. 2(a) and (b)(i)); Pt. 2 Div. 12, Pt. 3 Div. 8, Pt. 4 and 5: 1 Jul 2025 (see s. 2(c) and SL 2025/102 cl. 2); Pt. 2 Div. 1-5 and 7-9, Div. 10 Subdiv. 1-3, 5 and 6, Div. 11 (other than s. 134-136), Div. 13, Pt. 3 Div. 1-5, 7 and 9, Pt. 6 (other than Div. 1) and Sch. 1 and 2: 1 Jul 2026 (see s. 2(c) and SL 2026/128 cl. 2)
Assisted Reproductive Technology and Surrogacy Act 2025 Pt. 17 Div. 13	19 of 2025	18 Dec 2025	1 Jul 2026 (see s. 2(b)(ii) and SL 2026/128 cl. 2(b)(i))
Education and Care Services National Law Application Act 2026 Pt. 6 Div. 4	2 of 2026	31 Mar 2026	1 May 2026 (see s. 2(1)(d) and SL 2026/50 cl. 2)

Uncommenced provisions table

To view the text of the uncommenced provisions see *Acts as passed* on the WA legislation website.

Short title	Number and year	Assent	Commencement
Privacy and Responsible Information Sharing Act 2024 Pt. 2 Div. 6, Div. 10 Subdiv. 4 and s. 134-136 and Pt. 3 Div. 6	51 of 2024	6 Dec 2024	1 Jan 2027 (see s. 2(c) and SL 2026/203 cl. 2)
Evidence Act 2025 Pt. 12 Div. 17	15 of 2025	25 Sep 2025	18 Sep 2027 (see s. 2(d)(i) and (e) and SL 2026/190 cl. 2)

Other notes

[1] The *Privacy and Responsible Information Sharing Act 2024* Pt. 6 Div. 1 was deleted by the *Education and Care Services National Law Application Act 2026* Pt. 6 Div. 4 before it purported to come into operation (see Act No. 2 of 2026 s. 2(1)(d) and (2) and SL 2026/50 cl. 2).

Defined terms

[This is a list of terms defined and the provisions where they are defined. The list is not part of the law.]

Defined term	Provision(s)
Aboriginal community controlled organisation	4
Aboriginal information assessment	4, 177(1)
Aboriginal information use plan	4, 177(4)
act	4
affected individual	4
affected individuals	107(1)
agency	213(1)
approved form	4
approved privacy code of practice	4
assessed notifiable information breach	4
assessed shared information breach	4
associated	169(2)
Australian Information Commissioner	4
authorised officer	4
authorised representative	154(1)
automated decision-making process	4, 16(2)
automated system	4, 16(1)
care leaver	4
Chief Data Officer	4
Chief Data Officer guidelines	4
child	4
child protection functions	4
collect	4
commencement day	223(1), 224(1), 225(1), 226(1), 227(1), 228(1)
community policing functions	4
compliance notice	4, 122(1)
conciliation agreement	98(1)
conciliator	4
confidential or commercially sensitive information	4
consent	4
contracted service provider	4, 8(2)
data analytics work	4
Data analytics work	12(2)
data integration	4
Data integration	12(4)
data linkage	4
Data linkage	12(3)
data linkage key	12(3)
data set	4, 12(1)

de-identified information ..... 4, 11(2)
de-identify ..... 4, 11(1)
derived information 4, 170
disability 4
disclose 4
disclosing 10
disclosing entity 184
document ..... 213(1)
draft determination ..... 47(2)
electronic means 4
emergency response functions 4
enforcement action ..... 140(1)
exempt agency ..... 213(1)
exempt information ..... 4, 158(1), (2) and (3)
external entity ..... 4, 156(2)
family violence 4
government information 4, 157
handle 4
Health and Disability Services Complaints Office Director 4
health information 4
health service 4
high privacy impact function or activity ..... 4, 79(1)
hold 4
holding entity ..... 4, 160(3)
information breach 4
Information Commissioner 4
information holdings request ..... 4, 196(2)
information privacy principle 4
information sharing agreement ..... 4, 168(1)
information sharing CEO 4
information sharing Department 4
information sharing direction ..... 4, 163(1)
Information Sharing Minister 4
information sharing provisions ..... 214(1)
information sharing request ..... 4, 160(3)
insolvent ..... 140(1)
instrument of extension ..... 55(1)
interference with the privacy 4, 15
IPP 4
IPP entity ..... 4, 14(1)
judicial body ..... 4, 7(1)
law enforcement agency 4
law enforcement functions 4
materially assisted ..... 4, 16(3)

member of Commissioner staff 4
notice to produce or attend ..... 4, 113(1)
notifiable information breach 4
officer 4
outsourcing entity ..... 4, 8(1)
Parliamentary Commissioner for Administrative Investigations 4
Parliamentary Secretary 4
permitted purpose ..... 4, 159(1)
personal information 4
Police Force of Western Australia 4
primary purpose ..... Sch. 1 cl. 22.1
principal officer ..... 4, 9(1), (2) and (3)
privacy code of practice ..... 4, 28(1)
privacy complaint 4
Privacy Deputy Commissioner 4
privacy functions ..... 4, 142(1)
privacy guidelines 4
privacy impact assessment ..... 4, 79(2), 80(2), 176(2)
Privacy Minister 4
privacy provisions ..... 155(1)
proposed provider 4
proposed recipient 4
provider ..... 4, 168(2)
public entity ..... 4, 6(1) and (2)
public interest determination ..... 4, 45(1)
public register 4
receiving entity 185
recipient ..... 4, 168(3)
re-identify ..... 4, 11(3)
relevant activity ..... 4, 168(1)
relevant act or practice ..... 90(1), 98(3), 140(1)
relevant Minister ..... 220(1)
relevant official ..... 208(1), 218(1)
relevant outsourcing entity ..... 130(1), 131(2), 132(2), 133(3), 138(2), 139(3), 140(1)
requesting entity ..... 4, 160(3)
respondent ..... 4, 82(2)
responsible Minister 4
responsible sharing principle 4
responsible sharing safeguards ..... 175(3)
scheme ombudsman ..... 93(6)
secondary purpose ..... Sch. 1 cl. 22.1
secrecy provision 4
senior executive officer 4
senior officer 4

sensitive Aboriginal family history information 4
sensitive Aboriginal information safeguards ..... 177(2)
sensitive Aboriginal traditional information 4
sensitive personal information 4
shared information 4
shared information breach 4
significant decision ..... 4, 16(4)
special information sharing entity ..... 4, 156(1)
specified ..... 229(1)
state of mind ..... 217(1)
State services contract ..... 4, 8(1)
temporary public interest determination ..... 4, 49(1)
transitional matter ..... 229(1)
unique identifier 4
variation agreement ..... 4, 179(1)

© State of Western Australia 2026.
This work is licensed under a Creative Commons Attribution 4.0 International Licence (CC BY 4.0).
To view relevant information and for a link to a copy of the licence, visit www.legislation.wa.gov.au.
Attribute work as: © State of Western Australia 2026.
By Authority: ANDREW JONES, Government Printer